ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ КН МОН РК

30 YEARS OF INDEPENDENCE KAZAKHSTAN

VI - МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА»

МАТЕРИАЛЫ

29 сентября - 02 октября 2021 года

Институт информационных и вычислительных технологий МОН РК

МАТЕРИАЛЫ

VI международной научно-практической конференции "Информатика и прикладная математика", 29 сентября - 2 октября 2021, Алматы, Казахстан

Алматы 2021

УДК 378 (063)
ББК 74.58
И74

Главный редактор:
Калимолдаев М.Н. - академик НАН РК, д.ф.-м.н., профессор, советник генерального директора ИИВТ МОН РК

Ответственные редакторы:
Мамырбаев О.Ж. - заместитель генерального директора ИИВТ, доктор PhD
Айнакулов С.Ж. - заместитель генерального директора ИИВТ
Усатова О.А. – главный ученый секретарь ИИВТ МОН РК, PhD

И 74 **Информатика и прикладная математика:** Мат. VI Межд. науч. конф. (29 сентября -2 октября 2021 г.). Алматы, 2021. – с. 490

ISBN 978-601-332-384-8

В сборнике опубликованы доклады, представленные от Республики Казахстан, Российской Федерации, США, Латвии, Польши, Республики Беларусь, Украины, Азербайджана, Узбекистана, Японии, Кореи, Ирана, Португалии, Испании, Великобритании, Греции, Кыргызской Республики и других.

Рассмотрены актуальные вопросы в области математики, информатики и управления: математического моделирования сложных систем и бизнес-процессов, исследования и разработки защищенных и интеллектуальных информационных и телекоммуникационных технологий, математической теории управления, технологий искусственного интеллекта.

Материалы сборника предназначены для научных работников, докторантов и магистрантов, а также студентов старших курсов.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-384-8

© Институт информационных и вычислительных технологий МОН РК, 2021

Программный комитет

Почетный председатель:

- Мутанов Г.М., академик НАН РК, Казахстан

Сопредседатели Международного Программного комитета:

- Калимолдаев М.Н., академик НАН РК, д.ф.-м.н., советник генерального директора ИИВТ МОН РК, Казахстан
- Wójcik Waldemar, professor, Poland

Члены международного программного комитета:

- Абдыкаппар Ашимович Ашимов, доктор технических наук, профессор, академик НАН РК, основатель ИИВТ
- Andrzej Smolarz, professor, Poland
- Aijaz A. Shaikh, professor, Finland
- Arwa Sami Falazi, UAE -DUBAI
- Kisala Piotr, professor, Poland
- Erol Kurt, professor, Turkey
- Mohamed Othman, professor, Malaysia
- Keylan Alimhan, professor, Japan
- Marat Ahmet, professor, Turkey
- Müslüm Arici, professor, Turkey
- Nenad Mladenovich, professor, France
- Ravil Muhamediev, professor, Latvia
- Айда-заде К.Р., член кор., д.ф.-м.н., профессор, Азербайджан;
- Барахнин В.Б., д.т.н., профессор, Россия
- Бериков В.Б., д.т.н., профессор, Россия
- Евтушенко Ю.Г., академик РАН, Россия
- Исмаилов Б.И., д.т.н., профессор, Кыргызстан
- Родионов А.С., д.т.н., профессор, Россия
- Тузиков А.В., член кор., д.т.н., профессор, Беларусь
- Шаронова Н.В., д.т.н., профессор, Украина

Ученые секретари конференции:

- PhD, Усатова О.А.
- PhD, Шаяхметова А.С.

Организационный комитет

- Председатель - PhD, Мамырбаев О.Ж.
- Зам.председателя - Айнакулов С.Ж.

Соорганизаторы конференции

Место проведения

Республика Казахстан, г. Алматы, ул. Шевченко 28,
Ғылым ордасы, с 29 сентября по 2 октября 2021 г.

Тел.: **+7 727 272 37 11; +7 727 272 73 27; +7 727 272 39 13**

Вступительное слово

Дорогие друзья, уважаемые коллеги, организаторы и участники VI Международной научной конференции «Информатика и прикладная математика», посвященной 30-летию Института информационных и вычислительных технологий! Мы гордимся тем, что наш институт является ровесником Независимости Республики Казахстан.

Приветствую Вас и поздравляю с началом работы конференции, посвященной юбилею нашего Института! В работе международной конференции принимают участие видные ученые из ближнего и дальнего зарубежья, отечественные ученые, представители международных общественных организаций, ведущих ВУЗов РК и научно-исследовательских институтов. К сожалению, пандемия вносит свои коррективы и поэтому, в связи со сложившейся ситуацией, конференция будет проводиться в оффлайн и онлайн-режиме.

Институт является единственной профильной организацией Казахстана в области информационных технологий и вносит свой вклад в цифровую трансформацию нашей страны успешно выполняя фундаментальные и прикладные научные исследования.

Результаты НИР ИИВТ получили заслуженное признание в республике, о чем свидетельствуют полученные авторские свидетельства, отечественные и международные патенты, публикации в зарубежных рейтинговых журналах. Многие результаты научных исследований, выполненных в Институте, нашли свое практическое применение в развитии информационной инфраструктуры Республики Казахстан.

Институт выражает благодарность руководству Министерства образования и науки РК, Министерства цифрового развития, инноваций и аэрокосмической промышленности РК, Люблинскому техническому университету, организаторам, участникам и гостям конференции за активное участие в подготовке данного мероприятия.

Юбилей — это прекрасная возможность вспомнить о славной истории института, о многочисленных именах выдающихся учёных, инженеров и их достижениях, наметить планы на будущее. В этот день отдельные слова благодарности хочется адресовать ветеранам нашего коллектива, внесшим неоценимый вклад в его развитие. Многие из вас продолжают работать, передавая свои поистине бесценные знания и навыки молодым специалистам.

Желаю всем участникам конференции плодотворной работы, творческой результативной дискуссии, активности, оптимизма и приобретения дружеских контактов. Уверен, что результаты конференции будут полезны всем участникам данной конференции, а предложенные рекомендации найдут свое применение в дальнейшей практической деятельности каждого из вас.

ВРИО генерального директора
ИИВТ МОН РК, Мутанов Г.М.

СЕКЦИЯ 1

Қолданбалы математика, информатика және басқару теориясының қазіргі заманғы мәселелері. Бизнес процесстер мен күрделі жүйелерді оңтайландыру мен модельдеу. Есептеу математикасы, сандық талдау және программалау, математикалық логика. Статистика теориясы. Статистикалық әдістер

Современные проблемы прикладной математики, информатики и теории управления. Моделирование и оптимизация сложных систем и бизнес процессов. Вычислительная математика, численный анализ и программирование, математическая логика. Теория статистики. Статистические методы

Current issues of applied mathematics, computer science and control theory. Modeling and optimization of complex systems and business processes. Computational mathematics, numerical analysis and programming, mathematical logic. Theory of statistics. Statistical methods

РАЗРАБОТКА БИОРЕАКТОРА ГОРИЗОНТАЛЬНОГО ТИПА ДЛЯ ФЕРМЕРОВ КАЗАХСТАНА С УЧЕТОМ КЛИМАТИЧЕСКИХ И ЭКОНОМИЧЕСКИХ УСЛОВИЙ И МАТ.МОДЕЛИ ДЛЯ УПРАВЛЕНИЯ ПРОЦЕССАМИ

Шакерхан К.О., Сагындыков К.М., Мешечкин В.В., Анибаев С.К., Абильмажинов Е.Т., Конырханова А.А.
e-mail: kapan-shakerkhan@mail.ru
Казахский гуманитарно-юридический инновационный университет, Казахстан

Аннотация. *В данной статье приводится сравнение биогазовых установок по переработке отходов различной модификации, преимущества и их недостатки, а также описание биогазовой установки собственной разработки горизонтального типа, учитывающая местные климатические и экономические условия развития фермерских хозяйств Казахстана. В статье рассмотрены применение запатентованного нами пневмороторного двигателя для перемешивания биоотходов, биореактора собственного производства и описывается анализ развития биогазовых технологий в странах дальнего и ближнего зарубежья. Проводится анализ математической модели. Рассмотрены несколько направлений математического моделирования процессов анаэробного сбраживания. Такие модели, основанные на уравнениях химических реакции, научные работы Басвелла, Мюллера, Бойля и др. Модели, основанные на эмпирических зависимостях, работы Сэфили, Вестермана. Модели, основанные на кинетических зависимостях, от концентрации субстрата и клеток, от процесса ингибирования, например работы Моно, Конто, Мозера, Чена и Хашимото*.

Ключевые слова: *биометан, биогазовая установка, биореактор, биоотходы, биоудобрения*

Во многих странах к проблеме получения и использования биогаза уделяется большое внимание. За короткий срок во многих странах мира возникла целая индустрия по производству биогаза. Лидером в развитии биогазовой промышленности является Китай. С середины 70-х годов XX века в этой стране действует Национальная программа по получению биогаза из отходов животноводства. В настоящее время действует 10 миллионов фермерских метантенков. Кроме того, в Китае работает 40000 биогазовых станций, 24000 очистных сооружений, производящих биогаз, что обеспечивает работу 190 электростанций. Китай является экспортером биогаза и двигателей на его основе.

Европейская комиссия выделила биоэнергетику в самостоятельное направление общей энергетики, что было подтверждено на Всеевропейской конференции по биоэнергетике в октябре 2003 года в Будапеште.

Главными преимуществами биогаза являются его возобновляемость, наличие местных источников сырья для получения топлива, снижение парникового эффекта и экологического ущерба от систем сбора органических отходов, обеспечение экологически замкнутой энергетической системы. В таблице 1 приведены данные по производству биогаза в мире. [1, 2, 12]

Таблица 1. Производство биогаза в мире

Страна	**Объем производства биогаза в год, млн. м^3**	**Суммарная мощность биоЭС на биогазе, МВт**
США	500	200
Великобритания	200	80
Франция	40	16
Россия	58	-
Казахстан (потенциальные возможности)	15	-

Из таблицы видно, что в США в настоящее время годовой объем выработки биогаза составляет 500 млн. м^3. Значительная часть его поступает на электростанции. Суммарная электрическая мощность установок, работающих на биогазе, составляет около 200 МВт.

В США работает более десяти крупных биогазовых заводов, один из которых (при трех откормочных комплексах на 110 тыс. голов) подает вырабатываемый биогаз в газораспределительную сеть Чикаго. Кроме этого, в США получили широкое распространение установки для использования отходов на небольших скотоводческих фермах с поголовьем крупного рогатого скота до 150 голов.

В Великобритании добывается в год около 200 млн. м^3 биогаза. Суммарная мощность биоЭС Великобритании составляет около 80 МВт.

Во Франции добывается в год около 40 млн. м^3 биогаза. На одной из свалок вблизи Парижа была построена биоТЭС, использующая биогаз, эмиссия которого составляет 1,5 тыс. м^3 в сутки.

Германия является лидером в производстве биогаза в Европе. Страна стремиться сократить выбросы углекислого газа на 40% и поэтапно отказывается от ядерной энергии к 2020 году. Акты правительства, в котором излагаются стратегии, о сокращение выбросов, включают национальные цели для производства биометана – 6 миллиардов кубометров газа в год до 2020 и 10 млрд. кубометров в год к 2030 году. В связи с этим ожидается дальнейшее значительное расширение немецкого производства биогаза.

Правительство Дании предоставляет значительные налоговые льготы для производителей биогаза: около 20% капитальных инвестиций для централизованного биогаза и 30% для индивидуальных станций или установок. Суммарная годовая энергетическая мощность производителей биогаза Дании, получаемого из всех источников, в настоящее время составляет до 4ПДж. Планируется дальнейшее увеличение его производства до 6ПДж. В настоящее время в Дании эксплуатируются 18 биогазовых заводов, способных ежегодно обрабатывать 1,2 млн. т биомассы (75% отходов животноводства и 25% других органических отходов), давая до 45 млн. м^3 биогаза, что эквивалентно 24 млн. м^3 природного газа. [1, 2, 11]

В России нет национальной программы поддержки строительства биогазовых установок, ни одного централизованного биогазового завода. Вместе с тем на внутреннем рынке имеются модели малых биогазовых установок отечественного производства, предназначенные для использования в личных подсобных и фермерских хозяйствах.

Компания «Фактор Лтд» (Москва) разработала и внедрила на Балахнинской птицефабрике (Нижегородская обл.) опытный образец биогазовой установки. При вместимости реактора 5 м^3 она способна перерабатывать 1 тонну помета в сутки и

производить до 60 м^3 биогаза. В ближайшее время компания готова приступить к серийному производству биогазовых установок с реакторами вместимостью до 500 м^3.

АО «Центр «ЭкоРос» в 1994 г. при животноводческом комплексе КРС «Поярково», АО «Агрофирма «Искра» Солнечногорского района Московской области ввели в эксплуатацию автономный энергетический блок-модуль БИОЭН-1 по переработке отходов 20-25 голов КРС (рисунок 1).

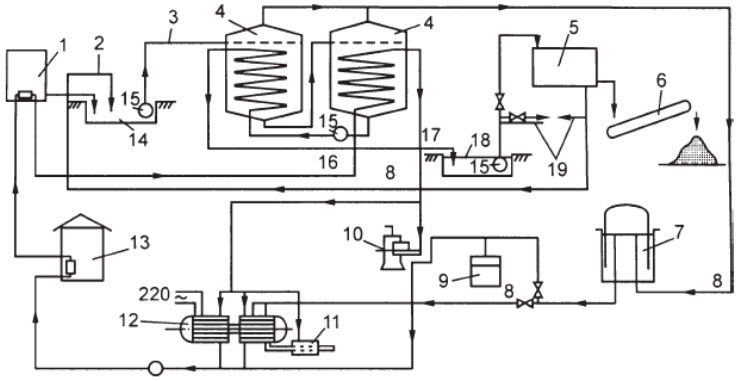


Рис. 1. Технологическая схема автономного биоэнергетического блок - модуля БИОЭН – 1: 1 – ферма; 2 – линия подачи жидкой фракции удобрений (после разделения); 3 – линия подачи сырья в биореактор; 4 – биореакторы; 5 – центрифуга; 6 – транспортер твердой фракции удобрений; 7 – газгольдер; 8 – линия подачи биогаза; 9– газовая плита; 10 – отопительный аппарат; 11 – рекуператор тепла выхлопных газов; 12 –электрогенератор; 13 – отопление помещений; 14 – емкость для хранения и подготовки сырья; 15– насосы; 16 – линия подачи горячей воды в рубашки биореакторов; 17–линия вывода охлажденной воды из биореакторов; 18–емкость для хранения жидких удобрений; 19 – линия выгрузки жидких удобрений.

В Казахстане также развивается энергетика ВИЭ, в том числе и биогазовая энергетика. 18 млн кВт/ч или 0,75% всей электроэнергии ВИЭ было выработано в 2019 году тремя биогазовыми станциями (БГС) общей мощностью 2,42 МВт, за которыми Минэнерго РК ежеквартально осуществляет мониторинг. С текущего года в этот перечень включена еще одна БГС – ТОО «Водные ресурсы-Маркетинг» с установленной мощностью 0,4 МВт на канализационных очистных сооружениях г. Шымкента. Таким образом, по данным Минэнерго, в 2020 году под мониторинг попадают 2,82 МВт биогазовых мощностей. Одна из включенных в перечень – биогазовая станция на 1 МВт, смонтированная из железнодорожных цистерн, – принадлежит карагандинскому ТОО АПК «Волынский». Сырье для ее работы – отходы свиноводческой фермы; выработанная электроэнергия поддерживает работу рыбного цеха комплекса. Биогазовая станция на 0,35 МВт ТОО «Караман-К» расположена в Костанайской области и работает на отходах животноводческой фермы КРС; выработанная электроэнергия направляется на собственные нужды. Разработкой проекта и доставкой оборудования этой станции занималось ООО «Зорг Биогаз Украина». Этот же поставщик оказал аналогичные услуги карагандинскому ТОО «Агрофирма Курма» для возведения БГС мощностью 1,07 МВт. [2, 3, 10]

В настоящее время разработаны биогазовые установки с различными конструктивными и технологическими особенностями. Существуют промышленные и кустарные установки. Промышленные установки отличаются от кустарных наличием механизации, систем подогрева, гомогенизации, автоматики. Типы биогазовых установок классифицируются по методам загрузки сырья, методам сбора биогаза, по используемым для их сооружения материалам, использованию дополнительных устройств, горизонтальному или вертикальному расположению реактора, подземной или наземной конструкции. Применяются двухстадийные и одностадийные биогазовые комплексы. Одностадийная технология используется для большинства субстратов и такую технологию можно считать базовой. По количеству ступеней процесса установки бывают одноступенчатыми, двухступенчатыми и многоступенчатыми. Одноступенчатые установки состоят из одного биореактора, в котором происходит полное сбраживание биомассы. В двухступенчатых системах процесс проходит в главном биореакторе брожения и в реакторе окончательного сбраживания и осаждения шлама. Многоступенчатые системы включают различное количество основных бродильных биореакторов и реакторов дображивания.

По режиму работы можно выделить непрерывные, полунепрерывные и периодические установки.

Установки периодического действия состоят из одного биореактора, который полностью загружается исходным субстратом, а затем после определенного времени процесса полностью опорожняется. В установках полунепрерывного режима процесс получения биогаза протекает в двух и более реакторах, которые работают по очереди.

При непрерывном режиме субстрат подается в биореактор непрерывно или через короткие промежутки времени, при этом соответствующий объем перебродившего субстрата удаляется. Установки, работающие в непрерывном режиме, отличаются стабильностью и высокой производительностью по сравнению с другими режимами.

По положению биореакторы бывают вертикального, горизонтального и наклонного расположения. Выбор расположения реактора зависит от режима работы и наличия свободной территории. В нашем случае мы используем биореактор горизонтального типа, полуподземного расположения с непрерывным режимом работы. Такой биореактор позволяет экономить энергию на перемешивания и сохранять тепло в холодных погодных условиях.

В биогазовых установках используют биореакторы овальной, цилиндрической и кубической формы. Наш предлагаемый биореактор представляет собой одноступенчатый, цилиндрической формы резервуар. Резервуары цилиндрической формы намного эффективнее сокращают расход энергии на перемешивание, в отличие от овального и кубического, что подтверждается большинством лабораторных исследований.

Также биогазовые установки различают по способу подвода тепла и способу перемешивания. Подвод тепла необходимого для протекания процесса может осуществляться прямым и непрямым способами. Для нашего биореактора мы используем непрямой способ. Т.к. прямой метод производится непосредственно подачей горячей воды или пара под давлением в бродильную массу. Для подогрева биомассы данным способом требуется установка парогенерирующей системы, что ведет к дополнительным затратам. Кроме того, при подаче пара или воды

происходит неравномерное распределение температуры в реакторе, в результате чего происходит перегрев биомассы [8, 9, 10].

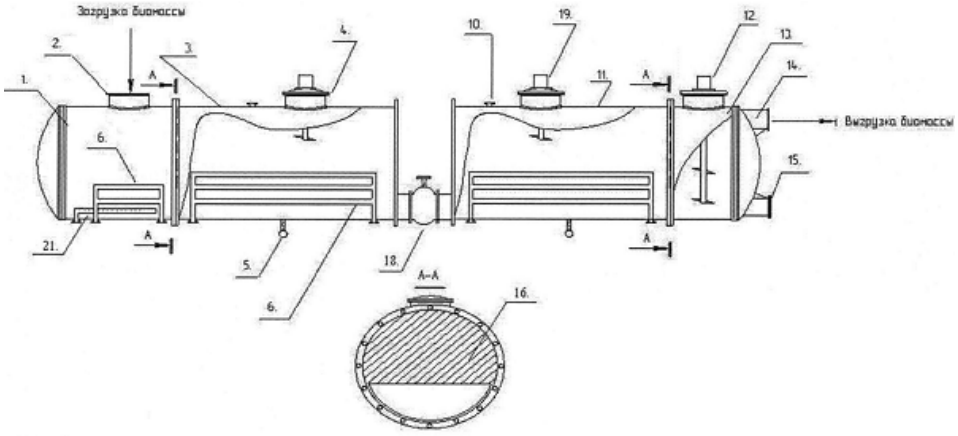


Рис. 2. Схема простейшей биогазовой горизонтальной установки

Биогазовая установка (см. рис. 2) предлагаемая нами для небольших фермерских хозяйств. Объем реактора от 16 м^3, рассчитанный на переработку 500-1000 кг навоза в сутки. Установка содержит несколько составных частей для обеспечения процесса переработки навоза и получения биоудобрений и биогаза. И работает она в мезофильном температурном режиме от 20 ºС до 35 ºС. Вырабатываемый установкой биогаз сразу направляется на использование в энергетических установках. Переработанная масса удаляется из реактора через выгрузочную трубу в момент загрузки очередной порции сырья или за счет давления биогаза. Выгружаемая сброженная масса попадает в емкость для временного хранения, которая по объему должна быть не менее объема реактора [9, 11].

Для реалии Казахстана, учитывая экономические и климатические факторы нами изобретено биореактор отечественного образца. Биореактор, выполнен трубчатой формой, расположен горизонтально и разделен на три секции: загрузочную, рабочую и выгрузочную, рабочая секция состоит из одного или нескольких модулей, в каждом модуле рабочей секции смонтированы мешалки с приводом и теплообменник, ***отличающийся тем, что*** каждый модуль снабжен поплавковым устройством, в котором монтируется мешалка с приводом с возможностью поворота относительно горизонтальной оси, причем в верхней части каждого модуля на горизонтальных направляющих установлена тележка с приводом, к которой посредством вертикальных штанг подсоединено (встроено) поплавковое устройство (см. рис. 3).

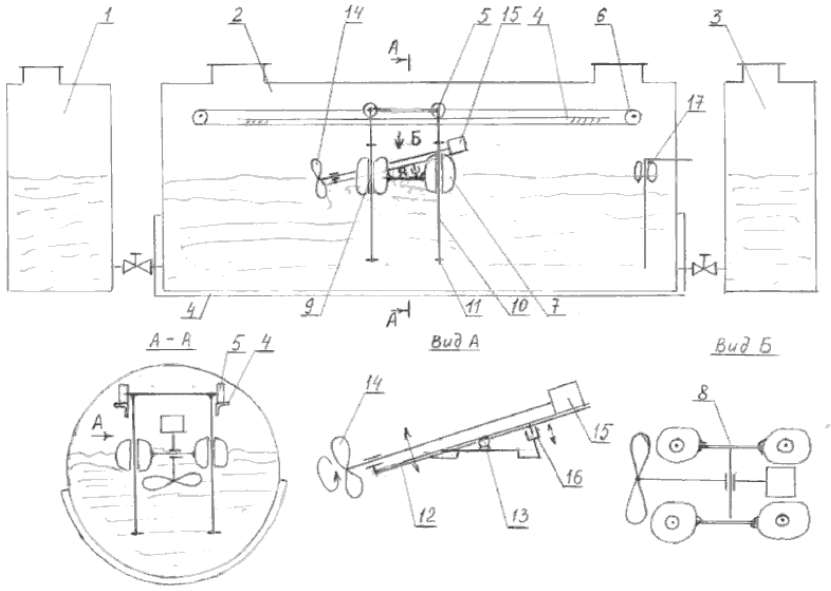


Рис. 3. Биореактор горизонтального типа с поплавковым перемешивающим устройством на пневмодвигателе, работающего на сжатом воздухе.

Технический результат достигается за счет того, что в конструкцию биореактора вводится дополнительный элемент в виде поплавкового устройства, в которое монтируется мешалка с приводом, с возможностью перемещения вдоль биореактора и поворота относительно горизонтальной оси в вертикальной плоскости [4, 6].

На рисунке 5 изображен биореактор с одним модулем:
1 - загрузочный сектор;
2 – рабочий сектор (модуль);
3 – разгрузочный сектор;
4 – теплообменная рубашка;
5 – тележка;
6 - привод тележки;
7 - поплавок;
8 – горизонтальные тяги;
9 – втулки;
10 – штанга вертикальная;
11 – ограничители;
12 – рычаг;
13 – ось рычага;
14 – мешалка;
15 – привод мешалки;
16 – гидро (пневмо) цилиндр;
17 – датчик уровня.

Биореактор состоит из трех секций: загрузочной 1, рабочей 2 и разгрузочной 3 (рисунок 5).

Рабочая секция может состоять из нескольких модулей. Модуль в нижней части имеет теплообменную рубашку 4.

В каждом модуле в ее верхней внутренней части смонтированы тележка 5 с приводом 6. Внутри каждого модуля на поверхности биомассы располагается поплавковое устройство, состоящее из поплавков 7 жестко скрепленных между собой горизонтальными тягами 8, при этом каждый поплавок 7 посредством втулок 9 подвижно встроен в вертикальную штангу 10. Вертикальные штанги 10 снабжены ограничителями 11перемещения поплавков 7 вдоль штанг.

На горизонтальных тягах 8 поплавкового устройства на рычаге 12 с осью 13 смонтирована мешалка 14 с приводом 15. Рычаг 12 снабжен гидро (пневмо) цилиндром 16. Для контроля уровня биомассы внутри каждого модуля имеется датчик уровня 17 электрически связанный с системой управления гидро (пневмо) цилиндром 16.

Перемешивание биомассы в каждом модуле происходит следующим образом.

Мешалка 14 с приводом 15, установленная на поплавковом устройстве, перемешивает биомассу по всей длине модуля, перемещаясь вдоль нее посредством тележки 5, которая может двигаться, например, с помощью трособлочного привода 6. Вертикальные штанги 10 обеспечивают устойчивое перемещение поплавкового устройства вдоль модуля. Ограничители 11 не позволяют поплавковому устройству опуститься ниже критической отметки, при которой мешалка могла бы задевать стенки модуля.

Мешалка 14 с приводом 15, проворачиваясь с помощью гидро (пневмо) цилиндра 16 относительно горизонтальной оси 13 позволяет перемешивать биомассу по всей высоте модуля.

Угол поворота рычага 12 с размещенной на ней мешалкой 14 с приводом 15 относительно горизонтальной оси 13 координируется в зависимости от уровня биомассы в рабочей секции 2 с помощью датчика уровня 17.

Таким образом, изобретение позволяет повысить качество перемешивания биомассы по всему объему модуля биореактора, сократить энергозатраты на его работу. А подземное расположение предусматривает горизонтальную конструкцию биореактора из-за очевидно меньших материальных затрат по сравнению с малой надежностью и неэффективностью маловысотной вертикальной конструкции. Кроме того, по нашим предварительным расчетам, железобетонная конструкция в условиях Казахстана оказывается в 1,5-2 раза дешевле стальной.

В результате анализа рынка биогазовых установок нами были установлено следующее: в Казахстане на сегодняшний день нет предприятий, выпускающих биогазовое оборудование (а тем более комплексы). Зарубежное оборудование очень дорогое, его не могут позволить себе купить даже относительно крупные фермерские хозяйства (около 1000 голов КРС). Например, стоимость биогазового комплекса в Костанайской области составила 400 млн. тенге [14], то есть более 1 млн. долларов США для фермерского хозяйства, где в наличии порядка 1000 голов к.р.с. Важно заметить, большинство поставщиков БГУ за рубежом, включая РФ [15], как и индивидуальные предприниматели в РК [19], широко рекламируют и продают БГУ (причём дорого, около 1300 долларов США за 1 $м^3$ биореактора), не включая в комплект такое важное и необходимое для нормального осуществления технологического процесса оборудование как измельчитель сырья. Измельчители нашей разработки [3] эффективны, практичны и недороги в сравнении с зарубежными аналогами (например, германский измельчитель средней производительности имеет стоимость порядка 13000 евро). Также не включаются в

комплект в большинстве случаев система очистки биогаза и другое оборудование. Кроме того, часто встречаются БГУ с неэффективным энергопотреблением перемешивающего устройства (до 3,4 кВт на 1 м^3 объёма биореактора).

На этом фоне предлагаемая разработка биореактора представляется действительно эффективной и максимально учитывающей экономические и климатические особенности региона.

Наличие оптимальной и адекватной математической модели позволяет оценить анаэробный процесс переработки отходов со всех его сторон, без проведения полномасштабных экспериментов, где соблюдаются пределы указанных и принятых ограничений. Актуальной задачей математического моделирования процесса метаногенеза является разработка универсальной модели, которая могла бы учитывать все параметры и факторы, связанные с процессом анаэробного брожения субстрата.

К настоящему времени математическое моделирование процесса анаэробного сбраживания рассматривается в нескольких направлениях.

Основой первого направления являются модели, основанные на уравнениях химических реакций. К ним относятся работы Басвелла, Мюллера, Бойля и других. Например, Басуэлл и Мюллер берут модель в качестве основы для определения количества произведенного биогаза в зависимости от исходного субстрата, а именно от химического состава:

$$C_nH_aO_b + (n - \frac{a}{4} - \frac{b}{8})H_2O \leftrightarrow \left(\frac{n}{2} - \frac{a}{8} - \frac{b}{4}\right)CO_2 + \left(\frac{n}{2} + \frac{a}{8} - \frac{b}{4}\right)CH_4 \quad (1)$$

где, $C_nH_aO_b$ - органическое вещество, H_2O - вода, CO_2 - углекислый газ, CH_4 - метан, a, b, n – безразмерные коэффициенты

Второе направление состоит из моделей, основанных на эмпирических зависимостях. В тоже время эти модели не учитывают параметры, которые влияют на конечный выход биогаза, и поэтому не раскрывают подробно процесс разложения органического вещества. Работы Сэфили и Вестермана предлагают эмпирическую зависимость выхода метана от температуры анаэробного сбраживания отходов в психофильном режиме:

$CH_4 = 0{,}216 + 0{,}00934 * T$ (2),

где CH_4 – выход метана, м^3/кг, Т – температура процесса сбраживания, ^{0}С.

Третье направление включает модели, основанные на кинетических зависимостях моделей Моно и Конто. Моно описывает процесс анаэробного разрушения ферментированного субстрата в зависимости от удельной скорости роста микроорганизмов:

$$\mu = \mu_M \frac{S}{K_s + S} \quad (3)$$

где, $\mu_м$ – максимальный удельный темп роста микроорганизмов, сут$^{-1}$; K_S – константа Моно, при которой темп роста составляет 0,5 от максимума.

На основе модели Моно Эндрюс, Мозер и другие разработали свои модели. В их работе также описывается выход биогаза в зависимости от концентрации субстрата, но с введением дополнительной функции в формулу как ингибирование у Эндрюса и с введением сигмоидального фактора в Мозер. Вышеприведенные формулы являются лишь частью, которая характеризует биологическую фазу:

$$\frac{dx_1}{dt} = \frac{F}{V}(X_0 - X_1) + \mu * X_1 - k_T * T_{x1} (4)$$

$$\frac{dS_1}{dt} = \frac{F}{V}(S_0 - S_1) - \frac{\mu}{Y_{\frac{X}{S}}} * X_1 (5)$$

$$\mu = \frac{\mu_{XX}}{1 + \frac{K_S}{HS} + \frac{HS}{K_1}} (6)$$

где X_0, X_1 – концентрация микробной популяции на входе и на выходе соответственно, кг/м^3; F,V – скорость подачи субстрата и объем субстрата в реакторе, м^3/с; μ - удельный темп роста микроорганизмов, сут$^{-1}$; k_T – коэффициент токсичности, сут$^{-1}$; T_{x1} – концентрация токсического вещества, кг/м^3; S_0, S_1 – концентрация ацетата на входе и на выходе, соответственно, кг/м^3; $Y_{x/s}$ – экономический коэффициент, характеризующий рост микробной популяции по мере потребления субстрата; HS – концентрация уксусной кислоты, кг/м^3; K_1 – константа ингибирования роста микроорганизмов уксусной кислоты, кг/м^3.

Модель Конто описывает скорость роста микроорганизмов в зависимости от концентрации субстрата и клеток бактерий. Отличительной особенностью модели Моно является учет процесса ингибирования:

$$\mu = \mu_м \frac{S}{K_S X + S} (7)$$

где X – концентрация клеток бактерий.

На основе модели Конто была разработана модель Чена и Хашимото. Чтобы определить скорость выхода биогаза в математической модели, основные параметры процесса анаэробной ферментации были введены как отдельные функции:

$$V = \frac{B_0 S}{\tau} * (1 - \frac{k}{\mu_m \tau - 1 + K}) (8)$$

где B_0 – максимальный выход метана за сутки из 1 кг органического вещества, м^3 CH_4/кг;

S – концентрация субстрата, кг/м^3; τ – продолжительность сбраживания, сут; К – кинетический параметр. Здесь параметр $\mu_м$ = 0,013 Т – 0,129.

Все приведенные выше модели учитывают выход биогаза (качество анаэробного процесса) на основе химического состава и массы исходного сырья, количества и скорости роста микроорганизмов или продолжительности ферментации. [16]

Также имеются предложенные модели Друзьяновой В.П., которая описывает среднюю скорость всплытия пузырьков газа из биореактора при психрофильном режиме:

Уравнение скорости всплытия биогазового пузыря

$$\vartheta_n = \frac{e^{\frac{t(\sqrt{l^2-4ac})}{b}(l-\sqrt{l^2-4ac})-l-\sqrt{l^2-4ac}}}{2a(1-e^{\frac{t(\sqrt{l^2-4ac})}{b}})} \quad (9)$$

Тем самым определяя, скорость всплытия пузырьков газа и их количества, и образующиеся осадки, можно определить мощность при спонтанном перемешивания и далее спрогнозировать объем ожидаемого биометана в ферментаторе:

Мощность спонтанного перемешивания

$$N_{сп} = m_{суб} g(\vartheta_n + \sqrt{\frac{4gd(\rho_T - \rho_{ж})}{\xi \rho_{ж}}}) \quad (10)$$

$m_{суб}$ - масса субстрата, ϑ_n - скорость всплытия пузырька, ξ - коэффициент лобового сопротивления, ρ_T - плотность твердой частицы, $\rho_{ж}$ - плотность жидкости, d – диаметр пузырька, g – ускорение свободного падения.

Существует модель Егоровой Е.Н., которая учитывает зависимость образования продукта метаболизма от скорости массообмена субстрата и скорости продуктов метаболизма, как основные факторы, интенсивно воздействующие на процесс эффективной деструкции органического навоза. Таким образом можно говорить, что выход биогаза определяется перемешиванием субстрата:

$$\nu_б = \int(N_{перем}) \text{, (10) где}$$

$N_{перем}$ – мощность перемешивания в метантенке

Мощность перемешивания $N_{перем}$, по матмодели Егоровой Е.Н. необходимую на перемешивание субстрата внутри метантенка, определяется с учетом необходимого количества лопастей, крутящего момента на валу мешалки, коэффициента лобового сопротивления, плотности субстрата и т.п.:

$$N_n = (M_{кр} * \omega) * Z_л = \left(\frac{C_x \rho \omega^3 a b^4}{8}\right) * Z_л \text{, (11)}$$

где

$M_{кр}$ – крутящий момент, возникающий на валу мешалки, Н*м;

C_x – коэффициент лобового сопротивления лопастей;

ρ – плотность перемешиваемой среды, кг/м^3;

ω - угловая скорость вращения мешалки, с$^{-1}$;

$Z_л$ – количество лопастей, ед;

a – высота лопасти, м;

b - высота лопасти, м.

В моделях Друзьяновой В.П. и Егоровой Е.Н. описаны обобщающие модели, полученные в лабораторных установках. В первом случае для определения выхода биогаза в зависимости от мощности биореактора при психрофильном режиме, а во втором случае в зависимости от мощности перемешивания в метантенке. Но все эти математические модели, сложно применяемые в промышленных масштабах для точного прогнозирования выхода биогаза с учетом различных параметров. [17, 18]

В нашей исследовательской работе по анализу оптимальной математической модели для более точного прогнозирования выхода биогаза при анаэробном брожении были использованы статические данные из биогазовой станции с. Курма, Карагандинской области и аналитические данные получены на примере биогазовой станции в провинции Манитоба, Канада. В предложенную нами в математическую модель, для ее широкого использования в промышленных масштабах и практического применения, использованы от 20 и до 26 различных параметров, существенно влияющих на качество анаэробного брожения, и соответственно на высокий результат выхода биогаза. Предлагается включить такие параметры в математическую модель, как показатели макро и микроэлементов (K-калий, Na-натрий, Ca-кальций, Mg-магний, Fe-железо, Cu-медь, Zn-цинк, Ni-никель, Co-кобальт, Mo-молибден, Cr-хром, Cd-кадмий), показатели C-углерода, N-азота, P-фосфор, C/N-соотношение углерода к азоту, L-концентрация питательных веществ, n-степень измельчения, VFA-содержание жирных кислот, τ-период брожения, m-масса субстрата, t-температура, pH-показатель кислотности, φ-влажность, S-сера, H_4N+ - аммоний.

Из полученных стат. данных сформировали свою математическую модель с учетом предложенных параметров, оказывающих влияние на анаэробное брожение. Из всех изученных моделей для анаэробного брожения, нами предложена линейная регрессионная модель. Т.к. в ходе экспериментальных и математических исследований выяснилось, что данная модель является более практичным и эффективным при широком промышленном производстве биогаза. Выделяют несколько разновидностей регрессий: линейная, гиперболическая, множественная, логарифмически линейная, нелинейная, обратная, парная. Экспериментальные исследования показывают, что влияние различных параметров на выход биогаза имеет линейную зависимость.

Предложенная нами математическая модель представляет собой линейное дифференциальное уравнение эмпирических соотношений каждого параметра, полученное путем регрессионного анализа. Модель линейной регрессии имеет следующий вид (см. формула 12):

$$\mathbf{y = a_0+a_1x_1+a_2x_2+\dots a_nx_n \quad (12)}$$

В данном уравнении:

- *Y* – переменная, влияние на которую нужно найти;
- X – факторы, влияющие на переменную;
- A – коэффициенты регрессии, определяющие значимости факторов;
- N – общее количество факторов.

Литература

1 Барбара Эдери, Хайнц Шульц. Биогазовые установки. Практическое пособие. 1996 - 268 стр.

2 Веденев А.Г., Веденева Т.А.-Б.: Руководство по биогазовым технологиям. - "ДЭМИ", 2011 - 84с.

3 Искаков С.К. Мобильная биогазовая установка. // Энергосовет – 2015. – №4 – С.

4 Биомасса как возобновляемый источник энергии. https://esa-conference.ru/wp-content/uploads/files/pdf/Kozlov-YUrij-Pavlovich.pdf

5 Перспективы производства биогаза в Казахстане. https://cyberleninka.ru/article/n/perspektivy-proizvodstva-biogaza-v-kazahstane/viewer

6 Биогазовая установка https://kazpatent.kz/images/bulleten/2018/gazette/ru201819/html/b0025684.htm

7 Казахстанская биогазовая энергетика https://eenergy.media/2020/03/11/kak-razvivaetsya-kazahstanskaya-biogazovaya-energetika/

8 Китайская система стимулирования биогазовой энергетики. http://aenergy.ru/1766

9 Классификация биогазовых установок по конструктивным и технологическим признакам. https://cyberleninka.ru/article/n/klassifikatsiya-biogazovyh-ustanovok-po-konstruktivnym-i-tehnologicheskim-priznakam/viewer

10 Строительство биогазовых установок. https://docviewer.yandex.kz/view

11 Digitalization and Innovative Development of Mining Processes.https://www.scopus.com/freelookup/form/author.uri?st1=Sagindikov

12 Совершенствование электроимпульсной технологии при получении биогаза из органических отходов. http://www.dslib.net/agroprom-elektrotex/sovershenstvovanie-jelektroimpulsnoj-tehnologii-pri-poluchenii-biogaza-iz.html

13 Энергосберегающая технология переработки навоза крупного рогатого скота. https://www.dissercat.com/content/energosberegayushchaya-tekhnologiya-pererabotki-navoza-krupnogo-rogatogo-skota

14 Где еще в Казахстане работают биогазовые установки // Inbusiness [Электронный ресурс]. – 2019. – URL: https://inbusiness.kz/ru/post/gde-eshe-v-kazahstane-rabotayut-biogazovye-ustanovki.

15 Биогазовые установки для производства газа // GreenDem [Электронный ресурс]. – 2019. – URL: https://greda.kz/p59616395-biogazovye-ustanovki-dlya.html.

16 Review of the mathematical description of the process of methanogenesis in a bioreactor. M.B. Tlebaev, N.K. Kalinchun, D.U. Mamataeva. International scientific journal (ISSN 2072-0297) № 4.1(138.1)/2017. http://www.rusnauka.com/pdf/246610.pdf

17 Energy-saving technology for processing cattle manure. Dissertation work / Ulan-Ude / 2016, V.P. Druzyanova. https://www.esstu.ru/uportal/dissertation/downloadFile.htm?type=dissertation&typeId=499

18 Substantiation of the parameters of a small-volume digester with a stirring device for the conditions of the Republic of Sakha (Yakutia). Dissertation work / Blagoveshchensk / 2017, E.N. Egorova. https://www.dissercat.com/content/obosnovanie-parametrov-metantenka-malogo-obema-s-peremeshivayushchim-ustroistvom-dlya-uslovi

КОМПАНЬОНЫ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Хисамиев З.Г.
KhisamievZ@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Описаны компаньоны поля рациональных чисел. Каждый компаньон, условно говоря, состоит из трансцендентной части и последующего его специального алгебраического расширения Это исследование предворяет описание экзистенциально закмнутых компаньонов поля рациональных чисел. В свою очередь описание экзистенциально замкнутых компаньонов поля рациональных чисел относится к иследованию классическиих алгебраических структур методами общей теории экзистенцильно замкнутых компаньонов, построенной в работах А.Т.Нуртазина на основе классов Фрэсе, и относящейся к классической области экзистециально замкнутых теорий в теории моделей.*

Пусть: $\mathbf{Q}$ – поле рациональных чисел; $\mathbf{Q}[\overline{x}]$, $\mathbf{Q}(\overline{x})$ – соответственно кольцо многочленов и поле частных над полем $\mathbf{Q}$ от независимых переменных $\overline{x}=(x_1,...,x_n)$. Все используемые и неприведенные определения и обозначения взяты из монографии [1]. Класс компаньонов поля $\mathbf{Q}$ обозначаем $C(\mathbf{Q})$**|**. Опишем некоторые базовые компаньоны поля $\mathbf{Q}$.

Очевидно, чисто алгебраические расширения поля $\mathbf{Q}$ не являются его компаньонами. В свою очередь, следующая теорема посвящена первым базовым компаньонам поля $\mathbf{Q}$ и которые есть его чисто трансцендентные расширения.

ТЕОРЕМА 1. Поле частных $\mathbf{Q}(\overline{x})$ является компаньоном поля $\mathbf{Q}$ т.е.. $\mathbf{Q}(\overline{x})$**|**$\models C(\mathbf{Q})$**|**

Доказательство. Каждая конечная подмодель кольца $\mathbf{Q}$ является подмоделью поля $\mathbf{Q}(\overline{x})$. Обратно пусть имеется конечная подмодель $\mathbf{F}$ поля $\mathbf{Q}(\overline{x})$, можно считать что $\mathbf{F}$ задается конечной системой равенств и неравенств $(\neq)$, правые и левые части которых содержат элементы $\mathbf{F}$ и операции сложения и умножения поля $\mathbf{Q}(\overline{x})$. Такая конечная система равенств и неравенств преобазуем в эквивалентную в $\mathbf{Q}(\overline{x})$ систему $\&R_i(\overline{x})=0 \,\&\&\, S_j(\overline{x})\neq 0$, где $R_i = f_i(\overline{x})\big/g_i(\overline{x})$, $S_j = u_j(\overline{x})\big/v_j(\overline{x})$, $f_i(\overline{x}), g_i(\overline{x}), u_j(\overline{x}), v_j(\overline{x}) \in \mathbf{Q}$**[**$\overline{x}$**]**, $g_i(\overline{x}), v_j(\overline{x}) \neq 0$.

Последняя система эквивалентна в $\mathbf{Q}[\overline{x}]$ системе с одним равенством и одним неравенством $P_1(\overline{x})=0 \,\&\, P_2(\overline{x})\neq 0$, где $P_1(\overline{x})=\sum f_i^2(\overline{x})$, $P_2(\overline{x})=\prod g_i(\overline{x})u_j(\overline{x})v_j(\overline{x})$. Докажем существование набора $\overline{a}=(a_1,...,a_n)\in\mathbf{Z}$ целых чисел, такого что в $\mathbf{Q}$ выполнено $P_1(\overline{x})=0 \,\&\, P_2(\overline{x})\neq 0$. При $n=1$ выберем положительное число a_1 настолько большим, чтобы модуль произведения a_1 на старший коэффициент по x_1 был больше модуля произведения числа $\deg(P_2(x_1))+1$ на максимальный модуль

коэффициентов $P_2(x_1)$. Тогда очевидно, что $P_2(a_1) \neq 0$. Индукционный шаг $n>1$. Будем считать, что переменная x_n присутствует в $P_2(\overline{x})$, иначе утверждение следует из предположения индукции. Запишем $P_2(\overline{x})$ как многочлен от переменной x_n и выберем набор $(a_1,...,a_{n-1}) \in \mathbf{Z}$ такой, что значение старшего коэффициента при x_n от этого набора отлично от нуля. Рассмотрим отличный от нуля многочлен $P_2(a_1,...,a_{n-1},x_n)$ одной переменной x_n, тогда осуществив выбор a_n как это сделано в при $n=1$ получим набор $P_2(a_1,...,a_{n-1},a_n) \neq 0$. Так как $P_1(\overline{x}) = 0$, то $P_1(a_1,...,a_{n-1},a_n)=0$. Теорема доказана.

Эквивалентность конечной системы уравнений и неравенств в $\mathbf{Q}(\overline{x})$ системе из не более чем одного уравнения и не более чем одного неравенства, целесообразно сформулировать в виде

ПРЕДЛОЖЕНИЕ 1. Пусть $R_i(\overline{x}), S_j(\overline{x}) \in \square(\overline{x})$. Система $\&R_i(\overline{x}) = 0 \&\& S_j(\overline{x}) \neq 0$, эквивалентна в $\mathbf{Q}[\overline{x})$ системе из одного уравнения и одного неравенства $P_1(\overline{x}) = 0 \& P_2(\overline{x}) \neq 0$, где $P_1(\overline{x}), P_2(\overline{x}) \in \mathbf{Q}[\overline{x}]$.

Пусть $A_f = \{ (\overline{a},a) | f(\overline{a},a) = 0,\ \overline{a},a \in \mathbf{Q}\}$ – аннулятор f, где $f(\overline{x},x) \in \mathbf{Q}(\overline{x})[x]$.

ТЕОРЕМА 2. Пусть $I(A_f) = \{ g | g \in \mathbf{Q}(\overline{x})[x],\ A_f \subseteq A_g \}$, где $f \in \mathbf{Q}(\overline{x})[x] \setminus \mathbf{Q}(\overline{x})$ неприводим над полем $\mathbf{Q}[\overline{x})$. Тогда, $I(A_f)$ является главным идеалом в кольце $\mathbf{Q}(\overline{x})[x]$ и $I(A_f) = (f)$.

Доказательство. Очевидно, множество $I(A_f) \subseteq \mathbf{Q}(\overline{x})[x]$ является кольцом. Кольцо многочленов $\mathbf{Q}(\overline{x})[x]$ над полем $\mathbf{Q}(\overline{x})$ является является евклидовым кольцом т.е. в нем выполняется деление многочленов с остатком. Поэтому многочлен наименьшей степени по x в $I(\square A_f)$ делит любой из многочленв из $I(\square A_f)$. Следовательно, ввиду неприводимости многочлена f имеем $I(A_f) = (f)$. Теорема доказана.

Укажем базовый не являющийся чисто трансцендентным компаньон $\mathbf{Q}$

ТЕОРЕМА 3. Пусть $f(\overline{x},x)$ – неприводимый многочлен над полем $\mathbf{Q}(\overline{x})$. Тогда, алгебраическое расширение $\mathbf{Q}(\overline{x})[x]/f$ поля $\mathbf{Q}(\overline{x})$ является компаньоном $\mathbf{Q}$ если и только если каждая проекция аннулятора A_f является бесконечным множеством.

Доказательство. Необходимость. Допустим противное – $A_f = \{(\overline{b}_1,c_1),...,(\overline{b}_k,c_k) | \overline{b}_i = (b_{1i},...,b_{ni}), b_{ji},c_i \in \mathbf{Q},\}$. Тогда выполнено: $\mathbf{Q}[\overline{x})[x]/f \models \exists \overline{u} \exists v (f(\overline{u},v) = 0 \&\&_i (\overline{u},v) \neq (\overline{b}_i,c_i))$ здесь $\overline{u} = (u_1,...,u_n)$. Используя различные переменные для каждого рационального числа из множества $\{b_{ji},c_i | j = 1,...,n, i = 1,...,k\}$, нетрудно указать экзистенциальное предложение не содержащее параметров b_{ji},c_i выполняющееся в $\mathbf{Q}(\overline{x})[x]/f$ но не в $\mathbf{Q}$. Противоречие. Необходимость даказана.

Достаточность. Докажем, что в моделях $\mathbf{Q}$ и $\mathbf{Q}(\overline{x})[x]/f$ выполняются одни и те же экзистенциальные предложения. Очевидно, что экзистенциальное предложение истинное в $\mathbf{Q}$ также истинно в $\mathbf{Q}(\overline{x})[x]/f$. Докажем, что каждое экзистенциальное предложение φ выполненное в $\mathbf{Q}(\overline{x})[x]/f$ выполняется в $\mathbf{Q}$. Так как для любых $(\overline{a},a)\in A_f$ выполнено $\mathbf{Q}[= g(\overline{a},a)=0$. Достаточно доказать, что если $\mathbf{Q}(\overline{x})[x]/f \mid= g(\overline{x},x_f)=0 \& h(\overline{x},x_f)\neq 0$, то $\mathbf{Q}[= h(\overline{a},a)\neq 0$ для подходящего набора $(\overline{a},a)\in A_f$, здесь $x_f = x+(f)$ – смежный класс в $\mathbf{Q}(\overline{x})[x]/f$, $f,g,h\in \mathbf{Q}(\overline{x})[x]$. Из теоремы 2 вытекает существование набора $(\overline{a},a)\in A_f \setminus A_h$. Действительно, если бы $A_f \subseteq A_h$, то $h\in(f)$ и $\mathbf{Q}(\overline{x})[x]/f \mid= h(\overline{x},x_f)=0$. Противоречие, достаточность а вместе с ней теорема доказаны.

ТЕОРЕМА 4. Пусть $\mathbf{Q}(\overline{x})[y]/f$ и $\mathbf{Q}(\overline{x})[y]/f/g$ (здесь $\mathbf{Q}(\overline{x})[y]/f/g=(\mathbf{Q}(\overline{x})[y]/f)[z]/g$ – простые алгебраические расширения полей $\mathbf{Q}(\overline{x})$ и $\mathbf{Q}(\overline{x})[y]/f$ соответственно, $f(\overline{x},y), g(\overline{x},y,z)$ – неприводимые многочлены над полями $\mathbf{Q}(\overline{x})$ и $\mathbf{Q}(\overline{x})[y]/f$ соответственно. Тогда, алгебраическое расширение $\mathbf{Q}(\overline{x})[y]/f/g$ поля $\mathbf{Q}(\overline{x})[y]/f$ является компаньоном $\mathbf{Q}$ если и только если множество $A_f \times Z \cap A_g$ бесконечно.

Доказательство. Для $\mathbf{Q}(\overline{x})[y]/f/g$ выполняется следующее предложение

ПРЕДЛОЖЕНИЕ 1^0. Система $\&_i g_i(\overline{x},y_f,z_g)=0 \& \&_j h_j(\overline{x},y_f,z_g)\neq 0$, где $g_i(\overline{x},y_f,z_g), h_j(\overline{x},y_f,z_g)\in \mathbf{Q}(\overline{x})[y]/f/g$, y_f, z_g – корни многочленов $f(\overline{x},y), g(\overline{x},y_f,z)$ соответственно, эквивалентна в $\mathbf{Q}(\overline{x})[y]/f/g$ системе из одного уравнения и одного неравенства $h_1(\overline{x},y_f,z_g)=0 \& h_2(\overline{x},y_f,z_g)\neq 0$.

Доказательство. Положим $h_1(\overline{x},y_f,z)=(g_i(\overline{x},y_f,z))$ – наибольший общий делитель многочленов $\{g_i(\overline{x},y_f,z)\}$ над полем $\mathbf{Q}(\overline{x})[y]/f$ и положим $h_2(\overline{x},y,z)=\prod_j h_j(\overline{x},y,z)$. Имеем $\mathbf{Q}(\overline{x})[y]/f/g \mid= \&_i g_i(\overline{x},y_f,z_g)=0 \& \&_j h_j(\overline{x},y_f,z_g)\neq 0$ тогда и толко тогда, когда $\mathbf{Q}(\overline{x})[y]/f/g \mid= h_1(\overline{x},y_f,z_g)=0 \& h_2(\overline{x},y_f,z_g)\neq 0$. Предложение доказано.

Перейдем к доказательству теоремы. Необходимость. Опираясь на предложение 1^0 будем рассматривать бескванторную часть *E*-предложения φ истинного, как состоящую из одного равенств и одного неравенства т.е. выполнено $\mathbf{Q}(\overline{x})[y]/f/g \mid= h_1(\overline{x},y_f,z_g)=0 \& h_2(\overline{x},y_f,z_g)\neq 0$. Допустим противное $A_f \times Z \cap A_g = \{(\overline{a}_1,b_1,c_1),,...,(\overline{a}_s,b_s,c_s) \mid \overline{a}_i=(a_{1i},...,a_{ni}), b_i,c_i\in \mathrm{Q}\}$ конечно.Тогда выполнено

$\mathbf{Q}(\overline{x})[y]/f/g \mid= h_1(\overline{x},y_f,z_g)=0 \& h_2(\overline{x},y_f,z_g)\neq 0 \& \&_i(\overline{x}\neq \overline{a}_i \,\&\, y_f\neq b_i, z_g\neq c_i)$, тогда

выполнено
$\mathbf{Q}(\overline{x})[y]/f/g|=\exists\overline{u}vw(h_1(\overline{u},v,w)=0\,\&\,h_2(\overline{u},v,w)\neq 0\,\&\,\&_i(\overline{u}\neq\overline{a}_i\,\&\,v\neq b_i, v\neq c_i)$, но это экзистенциальное предложение ложно в $\mathbf{Q}$. Так как рациональные числа *E*-выразимы в компаньон–полях $\mathbf{Q}$, то получим *E*-предложение истинное в $\mathbf{Q}(\overline{x})[y]/f/g$, но ложное в $\mathbf{Q}$. Противоречие, необходимость доказана.

Достаточность. Доказательству предпошлем предложении и две теоремы.

ТЕОРЕМА 5. Пусть в $\mathbf{Q}(\overline{x})[y]/f/g=(\mathbf{Q}(\overline{x})[y]/f)[z]/g$ выполнено $\mathbf{Q}(\overline{x})[y]/f/g|=h(\overline{x},y_f,z_g)=0$, тогда выполняется $\Box(\overline{x})[y,z]|=h(\overline{x},y_f,z_g)=g(\overline{x},y,z)q_1(\overline{x},y,z)+f(\overline{x},y)q_2(\overline{x},y,z)$ для подходящих $q_1(\overline{x},y,z),q_2(\overline{x},y,z)\in\Box(\overline{x})[y,z]$.

Доказательство. Из $\mathbf{Q}(\overline{x})[y]/f/g|=h(\overline{x},y_f,z_g)=0$ следует что $h(\overline{x},y_f,z)$ делится на $g(\overline{x},y_f,z)$ в $\mathbf{Q}(\overline{x})[y]/f[z]$, при делении второй делитель равен искомому $q_1(\overline{x},y,z)\in\Box(\overline{x})[y,z]$. В свою очередь $q_2(\overline{x},y,z)\in\Box(\overline{x})[y,z]$ определится из равенства $h(\overline{x},y_f,z)=g(\overline{x},y+(f),z)q_1(\overline{x},y+(f),z)$.

ТЕОРЕМА 6. Пусть $\mathbf{Q}(\overline{x})[y]/f/g=(\mathbf{Q}(\overline{x})[y]/f)[z]/g$, $I(A_{fg})=\{h|h\in\mathbf{Q}(\overline{x})[y,z],\ A_{fg}\subseteq A_h\}$, $A_{fg}=\{(\overline{a},b,c)\in\mathbf{Q}\,|(\overline{a},b)\in A_f,(\overline{a},b,c)\in A_g\}$, где $f\in\mathbf{Q}(\overline{x})[y]\setminus\mathbf{Q}(\overline{x})$, $g\in(\mathbf{Q}(\overline{x})[y]/f)[z]\setminus\mathbf{Q}(\overline{x})[y]/f$ неприводимы над соответствующими полями $\mathbf{Q}[\overline{x})[y],\mathbf{Q}(\overline{x})[y]/f)[z]$. Тогда, $I(A_{fg})$ является идеалом в кольце $\mathbf{Q}(\overline{x})[y,z]$, порожденным многочленами $f(\overline{x},y)$ и $g(\overline{x},y,z)$ т.е. $I(A_{fg})=(f,g)$

Доказательство. В условиях теоремы как и в предыдущем предложении выполнено $\Box(\overline{x})[y,z]|=h_1(\overline{x},y,z)=g(\overline{x},y,z)q_1(\overline{x},y,z)+f(\overline{x},y)q_2(\overline{x},y,z)$ для подходящих $q_1(\overline{x},y,z),q_2(\overline{x},y,z)\in\Box(\overline{x})[y,z]$. Теорма доказана.

ТЕОРЕМА 7. Любое экзистенциальное предложение истинное $\mathbf{Q}(\overline{x})[y]/f/g=(\mathbf{Q}(\overline{x})[y]/f)[z]/g$ истинно в $\mathbf{Q}$ для .

Доказательство. Как установлено выше достаточно из выполнимости $\Box(\overline{x})[y,z]|=h_1(\overline{x},y,z)=g(\overline{x},y,z)q_1(\overline{x},y,z)+f(\overline{x},y)q_2(\overline{x},y,z)$ для подходящих $q_1(\overline{x},y,z),q_2(\overline{x},y,z)\in\Box(\overline{x})[y,z]$ и $\Box(\overline{x})[y,z]\not|=h_2(\overline{x},y,z)=g(\overline{x},y,z)p_1(\overline{x},y,z)+f(\overline{x},y)p_2(\overline{x},y,z)$ для любых $p_1(\overline{x},y,z),p_2(\overline{x},y,z)\in\Box(\overline{x})[y,z]$. Укажем рациональные $(\overline{a},b,c)\in A_{fg},\overline{a}=(a_1,...,a_n),b,c\in\mathrm{Q}$ для которых выполнено $\Box|=h_2(\overline{a},b,c)\neq 0$. Если таких не существует тогда, $h_2\in A_{fg}$. Противоречие, теорема доказана.

Достаточность следует из предыдущей теоремы . Теорема даказана.

2.2. Описание компаньонов поля рациональных чисел

Пусть $B=\{\beta_1,\beta_2,....\}$, $X=\{x_1,x_2,....\}$ – счетные множества независимых переменных, $\overline{\beta}=(\beta_1,...,\beta_m)$, $\overline{x}_n=(x_1,...,x_n)$, $\overline{f}_n=(f_1,...,f_n)$, где $f_i(\overline{\beta},\overline{x}_{i-1}^{\overline{f}_{i-1}},x_i)$ неприводим в кольце $\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}][x_i]$, где $\overline{x}_i^{\overline{f}_i}=(x_1^{f_1},...,x_i^{f_i})$, $x_i^{f_i}$ – корень многочлена

$f_i(\overline{\beta},\overline{x}_{i-1}^{\overline{f}_{i-1}},x_i)\in\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}][x_i]$ над полем $f_i(\overline{\beta},\overline{x}_{i-1}^{\overline{f}_{i-1}},x_i)\in\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}]$. Поле $\mathbf{Q}(\overline{\beta})[\overline{x}_i^{\overline{f}_i}]$ определяется следующим образом. Положим $\mathbf{Q}(\overline{\beta})[\overline{x}_1^{\overline{f}_1}]=\mathbf{Q}(\overline{\beta})[x_1]/f_1(\overline{\beta},x_1)$, $\mathbf{Q}(\overline{\beta})[\overline{x}_2^{\overline{f}_2}]=\mathbf{Q}[\overline{\beta}][\overline{x}_1^{\overline{f}_1}][x_2]/f_2(\overline{\beta},\overline{x}_1^{\overline{f}_1},x_2)$. По индукции определим $\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]=\mathbf{Q}(\overline{\beta})[\overline{x}_{n-1}^{\overline{f}_{n-1}}][x_n]/f_n(\overline{\beta},\overline{x}_{n-1}^{\overline{f}_{n-1}},x_n)$. Таким образом, в последовательности $\mathbf{Q}(\overline{\beta})[\overline{x}_1^{\overline{f}_1}],\mathbf{Q}(\overline{\beta})[\overline{x}_2^{\overline{f}_2}],...,\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]$ – каждое последующее поле $\mathbf{Q}(\overline{\beta})[\overline{x}_{i+1}^{\overline{f}_{i+1}}]$ есть простое алгебраическое расширение предыдущего поля посредством неприводимого многочлена $f_{i+1}(\overline{\beta},\overline{x}_i^{\overline{f}_i},x_{i+1})$.

ТЕОРЕМА 8. Пусть в $g(\overline{\beta},\overline{x}_n^{\overline{f}_n})=h(\overline{\beta},\overline{x}_n^{\overline{f}_n})$ выполнено в поле $\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]$, полученном посредством последовательных присоединений корней $x_1^{f_1},...,x_n^{f_n}$ неприводимых многочленов $f_1,...,f_n$ над соответствующими полями $\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}]$, $\mathbf{Q}(\overline{\beta})\subseteq\mathbf{Q}(\overline{\beta})[x_1^{f_1}]\subseteq\mathbf{Q}(\overline{\beta})[\overline{x}_2^{\overline{f}_2}]\subseteq...\subseteq\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]$.

Тогда, в кольце $\mathbf{Q}(\overline{\beta})[\overline{x}_n]$ выполняется соотношение $g(\overline{\beta},\overline{x}_n)=h(\overline{\beta},\overline{x}_n)+q_1(\overline{\beta},\overline{x}_n)f_1(\overline{\beta},\overline{x}_1)+q_n(\overline{\beta},\overline{x}_n)f_2(\overline{\beta},\overline{x}_2)+...+q_n(\overline{\beta},\overline{x}_n)f_n(\overline{\beta},\overline{x}_n)$ для подходящих $q_1(\overline{\beta},\overline{x}_n),...,q_n(\overline{\beta},\overline{x}_n)\in\mathbf{Q}(\overline{\beta})[\overline{x}_n]$.

Доказательство. Теорема является обобщением теоремы 5 и докательство проводится повторением доказательства последней.

ТЕОРЕМА 9. Пусть в поле $\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]$ $I(A_{\overline{f}_n})=\{h\in\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]\,|\,A_{\overline{f}_n}\subseteq A_h\}$, $A_{\overline{f}_n}=\{(\overline{a},\overline{b}_n)\in\mathbf{Q}\,|(\overline{a},b_{,1})\in A_{f_1},...,(\overline{a},b_1,...,b_n)\in A_{f_n},\overline{b}_n=(b_1,...,b_n)\}$ где $f_i\in\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}][x_i]$, $i=1,...,n$ неприводим над соответствующим полем $\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}]$. Тогда, $I(A_{\overline{f}_n})$ является идеалом в кольце $\mathbf{Q}(\overline{\beta})[\overline{x}_n]$, порожденным многочленами $f_i(\overline{\beta},\overline{x}_i)$ т.е. $I(A_{\overline{f}_n})=(f_1,...,f_n)$.

Доказательство. Из предыдущей теоремы следует, что в $\mathbf{Q}(\overline{\beta})[\overline{x}_n]$выполнено $h\in I(A_{\overline{f}_n})$тогда и только тогда, когда $h(\overline{\beta},\overline{x}_n)=q_1(\overline{\beta},\overline{x}_n)f_1(\overline{\beta},\overline{x}_1)+q_n(\overline{\beta},\overline{x}_n)f_2(\overline{\beta},\overline{x}_2)+...+q_n(\overline{\beta},\overline{x}_n)f_n(\overline{\beta},\overline{x}_n)$ для подходящих $q_1(\overline{\beta},\overline{x}_n),...,q_n(\overline{\beta},\overline{x}_n)\in\mathbf{Q}(\overline{\beta})[\overline{x}_n]$. Теорема доказана.

ТЕОРЕМА 10. Пусть в поле $\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]$ $I(A_{\overline{f}_n})=\{h\in\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]\,|\,A_{\overline{f}_n}\subseteq A_h\}$, $A_{\overline{f}_n}=\{(\overline{a},\overline{b}_n)\in\mathbf{Q}\,|(\overline{a},b_{,1})\in A_{f_1},...,(\overline{a},b_1,...,b_n)\in A_{f_n},\overline{b}_n=(b_1,...,b_n)\}$ где $f_i\in\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}][x_i]$, $i=1,...,n$ неприводим над соответствующим полем $\mathbf{Q}(\overline{\beta})[\overline{x}_{i-1}^{\overline{f}_{i-1}}]$. Поле $\mathbf{Q}(\overline{\beta})[\overline{x}_n^{\overline{f}_n}]$ является компаньоном кольца $\mathbf{Z}$ тогда и только тогда, каждая проекция аннулятора $A_{\overline{f}_n}=\{(\overline{a},\overline{b}_n)\in\mathbf{Q}\,|(\overline{a},b_{,1})\in A_{f_1},...,(\overline{a},b_1,...,b_n)\in A_{f_n},\overline{b}_n=(b_1,...,b_n)\}$ является бесконечным множеством.

Доказательство. Доказательство повторяет схему доказательства теоремы 4 для случая $n=2$, при этом вместо теорем которые в доказательстве теоремы 4

использованы нужно использовать их обобщение теорема 8, теорема 9, теорема 10. Теорема доказана.

Работа выполнена по гранту КН МОН РК №AP08856114 по теме: Теория компаньонов (2020-2022 гг.).

Литература

1. Нуртазин А.Т. Введение в теорию моделей, элиминация кванторов и экзистенциальная замкнутость. – Алматы: НЦ ГНТЭ, 2017.– 187 с.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЧИСЛЕННОГО И АНАЛИТИЧЕСКОГО МЕТОДОВ РЕШЕНИЙ ЗАДАЧИ РАСПРЕДЕЛЕНИЯ ТЕМПЕРАТУРЫ ПО ДЛИНЕ СТЕРЖНЯ ПЕРЕМЕННОГО СЕЧЕНИЯ.

Ташев А.А., Аршидинова М.Т.
e-mail: mukaddas_arshidi@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В современных технологических линиях производства, ракетных и авиационных двигателях, двигателях внутреннего сгорания, атомных и тепловых электростанциях, для крепления солнечных батарей к космическим станциям применяются стержни переменного сечения. Но они работают при одновременном наличии разнородных видов источников тепла. В связи с этим в стержнях переменного сечения возникает сложное термо-напряженное деформируемое состояние. Надежная работа несущих элементов в виде стержней переменного сечения зависит от их термопрочности. Поэтому разработка методов исследования термо-напряженно-деформированного состояния стержней переменного сечения, находящихся под воздействием разнородных источников тепла, а также решения соответствующих задач являются актуальной. В данной работе исследуется установившееся термо-напряженно – деформированное состояние горизонтального стержня переменного сечения, образующая которого является прямая. Радиус сечения стержня по его длине меняется линейно, а площадь поперечного сечения – нелинейно. При этом на поперечного сечения левого конца стержня подводится тепловой поток с постоянной интенсивностью. Через площадь боковой поверхности и площадь поперечного сечения правого конца стержня происходит теплообмен с окружающей средой. При этом численно и аналитически решаются задачи определения поля распределения температуры. Полученные численные решения сравниваются с аналитическими решениями. При исследовании выявлены соответствующие закономерности.*

Ключевые слова: *Стержень переменного сечения, аналитическое, численное решение, деформация, напряжение, перемещение, удлинение, усилие.*

Как известно, в атомных и тепловых электростанциях, реактивных и водородных, а также двигателях внутреннего сгорания, космических станциях широко применяются несущие стержневые элементы в виде стержней переменного поперечного сечения. Эти стержневые элементы находятся под воздействием разнородных источников тепла. В связи с этим в стержнях переменного сечения возникают сложные термо-напряженно-деформированное состояние. Надежная работа конструкций в целом будет зависить от термопрочности имеющихся в них стержневых элементов [1-11].

Определение закона распределения температуры для стержня под воздействием теплового потока на одном торце, и теплообмена на другом торце рассмотрены во многих работах [15-18]. Осуществлено сравнение решений, полученных энергетическим и аналитическим методами. Вариационный подход

рассмотрен в [12]. В [15] стержень переменного сечения разбивается на три части. На средней части поддерживаются постоянная температура, а первые и третий дискретные элементы не теплоизолированы. При этом на боковой поверхности не теплоизолированных частей и на торцах происходит теплообмен с окружающей средой.

В данной работе рассматривается не теплоизолированный, ограниченный стержень переменного сечения, с левого торца которой подается тепловой поток. Определяется закон распределения температуры методом конечных элементов и аналитическим способом, после осуществляется сравнительный анализ.

1. Постановка задачи

Рассмотрим горизонтальный стержень переменного сечения ограниченной длины $L[см]$. Горизонтальная ось OX направлена слева на право и совпадает с осью стержня. Радиус поперечного сечения левого конца стержня $r_1[см]$, а правого конца $r_2[см]$, кроме того $r_1 > r_2$. Радиус сечения стержня по оси OX меняется линейно.

$$r(x) = ax + b, \;\; 0 \le x \le L\,, \tag{1}$$

где a и b – некоторые постоянные. Тогда $r(x=0) = a \cdot 0 + b = r_1$ или

$$b = r_1, \tag{2}$$

а $r(x = L) = a \cdot L + b = r_2$ или

$$a = \frac{r_2 - r_1}{L}. \tag{3}$$

Подставляя (2-3) в (1) определим закон изменения радиуса по длине исследуемого стержня.

$$r(x) = \left(\frac{r_2 - r_1}{L}\right) \cdot x + r_1, \;\; 0 \le x \le L. \tag{4}$$

Тогда площадь поперечного сечения исследуемого стержня по ее длине меняется следующим образом

$$F = \pi r^2 = \pi \left[\left(\frac{r_2 - r_1}{L}\right) \cdot x + r_1\right]^2 =$$
$$\pi \left[\left(\frac{{r_2}^2 - 2r_2r_1 + {r_1}^2}{L^2}\right) \cdot x^2 + 2\left(\frac{r_2 - r_1}{L}\right) r_1 x + {r_1}^2\right], \;\; 0 \le x \le L. \tag{5}$$

На площадь поперечного сечения левого конца исследуемого стержня подводится тепловой поток с постоянной интенсивностью $q\left[\frac{\text{Вт}}{\text{см}^2}\right]$.

Через площадь боковой поверхности и поперечного сечения правого конца происходит теплообмен с окружающей средой. При этом температура $T_{ос}[^oC]$ окружающей среды постоянна. Коэффициент теплообмена $h\left[\frac{\text{Вт}}{\text{см}^2{}^\circ\text{C}}\right]$. Физико-механические свойства материала стержня характеризуется коэффициентами теплопроводности $K_{xx}\left[\frac{\text{Вт}}{\text{см}^\circ\text{C}}\right]$,теплового расширения $\alpha[\frac{1}{^\circ\text{C}}]$ и модуля упругости $\text{E}\left[\frac{\text{кГ}}{\text{см}^2}\right]$.

Следует отметить, что наибольший радиус исследуемого стержня r_1 гораздо меньше по сравнению с значением коэффициента теплопроводности материала стержня K_{xx}.

Считая, что линейные размеры поперечного сечения малы по сравнению с его длиной, можно предположить, что внутри стержня поток тепла распространяется лишь вдоль его оси.

Поэтому с приемлемой точностью можно сказать, что процесс теплопроводности по длине исследуемого стержня будет одномерной и будет зависит только от переменной x, то есть $T = T(x)$. Расчетная схема рассматриваемой задачи показана на рисунке – 1.

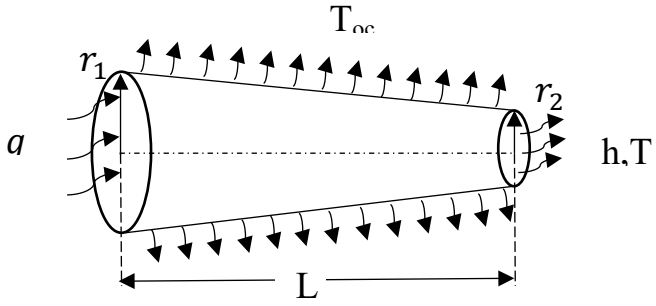


Рисунок – 1 . Расчетная схема рассматриваемой задачи.

На рисунке 1 представлен горизонтальный не теплоизолированный стержень переменного сечения ограниченной длины $L[см]$. Горизонтальная ось OX направлена слева на право и совпадает с осью стержня. $q\left[\frac{Вт}{см^2}\right]$ – тепловой поток с постоянной интенсивностью, который подводится на левый конец исследуемого стержня. $T_{ос}[^oC]$ - температура окружающей среды. $h\left[\frac{Вт}{см^2 °C}\right]$ - коэффициент теплообмена. $r_1[см]$ –радиус поперечного сечения левого конца стержня, а $r_2[см]$ - правого конца.

При этом решается задача определения закона распределения температуры по длине исследуемого стержня.

С точки зрения вариационного исчисления искомая функция $T=T(x)$ дает минимум функционалу полной тепловой энергии (для рассматриваемого стержня переменного сечения ограниченной длины с учетом его геометрических размеров, физико-механических свойств его материала и наличия теплового потока и теплообмена)[12]:

$$J = \int_{S(x=0)} qTds + \int_V \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv + \int_{S_{пбп}} \frac{h}{2}(T(x) - T_{ос})^2 ds + \int_{S(x=L)} \frac{h}{2}(T(x) - T_{ос})^2 ds, \quad (6)$$

где $S(x = 0)$ - площадь поперечного сечения левого конца исследуемого стержня переменного сечения:

$$S(x = 0) = \pi r_1^2; \quad (7)$$

$S_{пбп}$- площадь боковой поверхности исследуемого стержня;

$S(x = L)$- площадь поперечного сечения правого конца стержня:

$$S(x = L) = \pi r_2^2; \quad (8)$$

V - Объем исследуемого стержня.

3. Построение квадратичной сплайн функции в локальной системе координат

Исследуемый стержень переменного сечения и ограниченной длины дискретизируем n-дискретными элементами одинаковой длины $l = \frac{L}{n}$ [см]. Тогда в пределах длины одного произвольного элемента поле распределения температуры аппроксимируется полным полиномом второго порядка [17]:

$$T(x) = ax^2 + bx + c, \ \ 0 \le x \le l, \quad (9)$$

где a, b и $c -$ постоянные.

В пределах длины каждого дискретного элемента введем следующие обозначения:

$$T(x = 0) = T_i; T\left(x = \frac{l}{2}\right) = T_j; \qquad T(x = l) = T_k. \quad (10)$$

Расчетная схема для одного дискретного элемента и поле распределения температуры показана на рисунке -2.

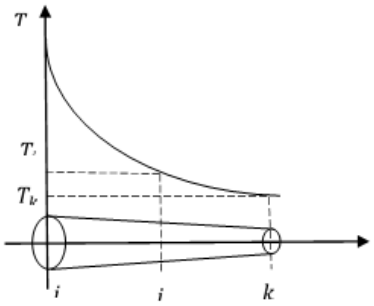


Рисунок – 2. Расчетная схема одного дискретного элемента

На рисунке 2 показан один дискретный элемент в локальной системе координат. Разбиваем область на два элемента с тремя узловыми точками T_i, T_j, T_k, для представления функции элемента в виде полинома второй степени.

Пользуясь выражениями (9) и (10) составим следующую систему уравнений:

$$\begin{cases} a \cdot 0 + b \cdot 0 + c = T_i \\ a \cdot \dfrac{l^2}{4} + b \cdot \dfrac{l}{2} + c = T_j \\ a \cdot l^2 + b \cdot l + c = T_k \end{cases} \quad (11)$$

Отсюда определим значения постоянных:

$$c = T_i, \quad b = \frac{4T_j - 3T_i - T_k}{l}, \ a = \frac{2T_k - 4T_j + 2T_i}{l^2}. \quad (12)$$

Далее подставляя найденные значения в (9) получим

$$T(x) = \left(\frac{2T_k - 4T_j + 2T_i}{l^2} \right) x^2 + \left(\frac{4T_j - 3T_i - T_k}{l} \right) x + T_i$$

или

$$T(x) = (\frac{2x^2 - 3xl + l^2}{l^2}) T_i + (\frac{4lx - 4x^2}{l^2}) T_j \quad + (\frac{2x^2 - lx}{l^2}) T_k, 0 \le x \le l \qquad (13)$$

Это согласуется с результатом, полученным в [17]

В (13) введем следующие обозначения

$$\begin{cases} \varphi_i(x) = \dfrac{2x^2 - 3lx + l^2}{l^2}; \\ \varphi_j(x) = \dfrac{4lx - 4x^2}{l^2}; \\ \varphi_k(x) = \dfrac{2x^2 - lx}{l^2}. \end{cases} \qquad (14)$$

Функции $\varphi_i(x), \varphi_j(x), \varphi_k(x)$ называются квадратичными сплайн функциями в локальной системе координат $x \in [0, l]$.

Эти функции имеют следующие свойства:

$$\varphi_i(x) = \begin{cases} 1, при_x = 0; \\ 0, при_x = \dfrac{l}{2}; \\ 0, при_x = l; \end{cases} \quad \varphi_j(x) = \begin{cases} 0, при_x = 0; \\ 1, при_x = \dfrac{l}{2}; \\ 0, при_x = l; \end{cases} \quad \varphi_k(x) = \begin{cases} 0, при_x = 0; \\ 0, при_x = \dfrac{l}{2}; \\ 1, при_x = l. \end{cases} \qquad (15)$$

$$\varphi_i(x) + \varphi_j(x) + \varphi_k(x) = 1. \qquad (16)$$

Из (13) можно найти выражение для градиента температуры в пределах длины одного дискретного элемента

$$\frac{\partial T}{\partial x} = \frac{4x - 3l}{l^2} T_i + \frac{4l - 8x}{l^2} T_j + \frac{4x - l}{l^2} T_k. \qquad (17)$$

Кроме того, из (14) можно показать, что

$$\frac{\partial \varphi_i}{\partial x} + \frac{\partial \varphi_j}{\partial x} + \frac{\partial \varphi_k}{\partial x} = 0. \qquad (18)$$

Если исследуемый стержень дискретизируем n элементами, то в первом дискретном элементе участвуют узловые температуры $T_i = T_1$, $T_j = T_2$, $T_k = T_3$. Во

втором дискретном элементе $T_i = T_3$, $T_j = T_4$, $T_k = T_5$. В третьем дискретном элементе $T_i = T_5$, $T_j = T_6$, $T_k = T_7$ и так далее. На в *n*-м дискретном элементе будут участвовать температуры $T_i = T_{2n-1}$, $T_j = T_{2n}$, $T_k = T_{2n+1}$. В общем случае, если число дискретных элементов в исследуемом стержне переменного сечения будет равно *n*, то число узлов будет равно $(2n+1)$.

4.Определение функционала тепловой энергии

Для понимания предлагаемого вычислительного алгоритма исследуемый стержень переменного сечения дискретизуем тремя дискретными элементами одинаковой длины $l = \frac{L}{3}$ [см] .

Рассмотрим первый дискретный элемент

Для этого элемента $T_1 = T(x=0); T_2 = T(x=\frac{l}{2}); T_1 = T(x=l)$. Радиус сечения меняется по длине этого дискретного элемента линейно: $r(x) = ax + b,\ 0 \le x \le l.$

Тогда поле распределения температуры по длине этого дискретного элемента имеет вид:

$$T^{(1)}(x) = \frac{2x^2 - 3lx + l^2}{l^2} T_1 + \frac{4lx - 4x^2}{l^2} T_2 + \frac{2x^2 - lx}{l^2} T_3,\ 0 \le x \le l\ . \quad (19)$$

Градиент температуры по длине этого дискретного элемента равен:

$$\frac{\partial T^{(1)}}{\partial x} = \frac{4x - 3l}{l^2} T_1 + \frac{4l - 8x}{l^2} T_2 + \frac{4x - l}{l^2} T_3\ ,0 \le x \le l\ . \quad (20)$$

Тогда функционал тепловой энергии для первого дискретного элемента равен:

$$J_1 = \int\limits_{S(x=0)} qTds + \int\limits_{S_{ПбП1}} \frac{h}{2}(T - T_{ос})^2 ds + \int\limits_{V_1} \frac{K_{xx}}{2}(\frac{\partial T}{\partial x})^2 dv = J_{11} + J_{12} + J_{13} \quad (21)$$

где $S_{ПбП1}$ -площадь боковой поверхности 1-го элемента; V_1 - объем первого элемента;

$s(x=0)$ – площадь поперечного сечения левого конца стержня.

Радиус левого конца первого дискретного элемента будет равно:

$r(x=0) = a \cdot 0 + b = b$[см].

Тогда площадь этого поперечного сечения будет равна:

$$F = \pi r^2(x=0) = \pi b^2.$$

Введем следующие обозначения:

$b_1 = b$- радиус самого левого конца стержня,

$b_2 = a\frac{L}{3} + b$ – радиус правого конца первого элемента.

Теперь вычислим первый интеграл функционала J_1:

$$J_{11} = \int\limits_{S(x=0)} qTds = \pi b_1^2 qT_1\ . \quad (22)$$

Второй интеграл функционала J_1 вычисляется следующим образом:

$$J_{12} = \int\limits_{S_{ПБП1}} \frac{h}{2}(T - T_{ос})^2\, ds = \pi \int\limits_0^l (ax+b)^2 (\varphi_i(x)T_1 + \varphi_j(x)T_2 + \varphi_k(x)T_3 - T_{ос})^2 =$$

$$h\pi\left[\left(\frac{al^2}{60} + \frac{2b_1 l}{15}\right)T_1^2 + \left(\frac{4al^2}{15} + \frac{8b_1 l}{15}\right)T_2^2 + \left(\frac{7al^2}{60} + \frac{2b_1 l}{15}\right)T_3^2 + \frac{2b_1 l}{15}T_1T_2 - \right.$$

$$\left(\frac{al^2}{30} + \frac{b_1 l}{15}\right)T_1T_3 + \left(\frac{2al^2}{15} + \frac{2b_1 l}{15}\right)T_2T_3 + \left(\frac{al^2}{15} + b_1 l\right)T_{ос}^2 - \frac{b_1 l}{3}T_1T_{ос} - \qquad (23)$$

$$\left.\left(\frac{2al^2}{3} + \frac{4b_1 l}{3}\right)T_2T_{ос} - \left(\frac{al^2}{3} + \frac{b_1 l}{3}\right)T_3T_{ос}\right]$$

Последний интеграл функционала J_1 равен:

$$\mathrm{J}_{13} = \int\limits_{V_1} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv = \frac{\pi K_{xx}}{2}\int\limits_0^l (ax+b)^2\left[\frac{4x-3l}{l^2}T_1 + \frac{4l-8x}{l^2}T_2 + \frac{4x-l}{l^2}T_3\right]^2 dx =$$

$$\frac{\pi K_{xx}}{2}\left[\left(\frac{a^2 l}{5} + ab_1 + \frac{7b_1^2}{3l}\right)T_1^2 + \left(\frac{32a^2 l}{15} + \frac{16ab_1}{3} + \frac{16b_1^2}{3l}\right)T_2^2 + \left(\frac{23a^2 l}{15} + \frac{11ab_1}{3} + \frac{7b_1^2}{3l}\right)T_3^2 - \right. \qquad (24)$$

$$\left.\left(\frac{4a^2 l}{5} + \frac{8ab_1}{3} + \frac{16b_1^2}{3l}\right)T_1T_2 + \left(\frac{2a^2 l}{5} + \frac{2ab_1}{3} + \frac{2b_1^2}{3l}\right)T_1T_3 - \left(\frac{52a^2 l}{15} + 8ab_1 + \frac{16b_1^2}{3l}\right)T_2T_3\right]$$

.

Тогда для первого дискретного элемента функционал тепловой энергии энергии J_1 будет равен:

$$J_1 = J_{11} + J_{12} + J_{13} \qquad (25)$$

Рассмотрим второй дискретный элемент исследуемого стержня.

Радиус поперечного сечения левого конца второго дискретного элемента, как уже упоминалось, равна:

$$b_2 = a \cdot \frac{L}{3} + b \qquad (26)$$

Функционал полной тепловой энергии для этого дискретного элемента равен:

$$J_2 = \int\limits_{S_{ПБП2}} \frac{h}{2}(T - T_{ос})^2\, ds + \int\limits_{V_2} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv = J_{21} + J_{22} \qquad (27)$$

где $S_{ПБП2}$ -площадь боковой поверхности 2-го элемента;

V_2 - объем второго элемента.

Значения температур для второго дискретного элемента равны $T_3 = T(x=0); T_4 = T(x=\frac{l}{2}); T_5 = T(x=l);$

По аналогии (25) и (24) находим функционалы J_{21} и J_{22}:

$$J_{21} = \int_{S_{ПБП2}} \frac{h}{2}(T - T_{ос})^2 ds =$$

$$h\pi\left[\left(\frac{al^2}{60} + \frac{2b_2 l}{15}\right)T_3^2 + \left(\frac{4al^2}{15} + \frac{8b_2 l}{15}\right)T_4^2 + \left(\frac{7al^2}{60} + \frac{2b_2 l}{15}\right)T_5^2 + \frac{2b_2 l}{15}T_3T_4 - \right. \quad (28)$$

$$\left(\frac{al^2}{30} + \frac{b_2 l}{15}\right)T_3T_5 + \left(\frac{2al^2}{15} + \frac{2b_2 l}{15}\right)T_4T_5 + \left(\frac{al^2}{15} + b_2 l\right)T_{ос}^2 - \frac{b_2 l}{3}T_3T_{ос} -$$

$$\left.\left(\frac{2al^2}{3} + \frac{4b_2 l}{3}\right)T_4T_{ос} - \left(\frac{al^2}{3} + \frac{b_2 l}{3}\right)T_5T_{ос},\right.$$

$$\mathrm{J}_{22} = \int_{V_2} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv =$$

$$\frac{\pi K_{xx}}{2}\left[\left(\frac{a^2 l}{5} + ab_2 + \frac{7b_2^2}{3l}\right)T_3^2 + \left(\frac{32a^2 l}{15} + \frac{16ab_2}{3} + \frac{16b_2^2}{3l}\right)T_4^2 + \left(\frac{23a^2 l}{15} + \frac{11ab_2}{3} + \frac{7b_2^2}{3l}\right)T_5^2 - \right. \quad (29)$$

$$\left.\left(\frac{4a^2 l}{5} + \frac{8ab_2}{3} + \frac{16b_2^2}{3l}\right)T_3T_4 + \left(\frac{2a^2 l}{5} + \frac{2ab_2}{3} + \frac{2b_2^2}{3l}\right)T_3T_5 - \left(\frac{52a^2 l}{15} + 8ab_2 + \frac{16b_2^2}{3l}\right)T_4T_5\right].$$

Тогда функционала тепловой энергии для второго дискретного элемента будет равен:

$$J_2 = J_{21} + J_{22} \quad (30)$$

Рассмотрим третий дискретный элемент стержня.

В этом элементе $b_3 = r(x = 2l) = 2 \cdot a \cdot l + b;$

Функционал полной тепловой энергии для третьего элемента рассматриваемого стержня имеет следующий вид:

$$J_3 = \int_{S_{ПбП3}} \frac{h}{2}(T - T_{ос})^2 ds + \int_{S(x=L)} \frac{h}{2}(T - T_{ос})^2 ds + \int_{V_3} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv = J_{31} + J_{32} + J_{33} \quad (31)$$

где $S_{ПбП3}$ -площадь боковой поверхности 3-го дискретного элемента;

$S(x = L)$ - площадь поперечного сечения правого конца исследуемого стержня;

V_3 - объем третьего (последнего) дискретного элемента стержня.

По аналогии (28) и (29) находим каждый член функционала J_3.

$$J_{31} = \int\limits_{S_{ПБП3}} \frac{h}{2}(T - T_{ос})^2 ds =$$

$$h\pi\left[\left(\frac{al^2}{60} + \frac{2b_3 l}{15}\right)T_5^2 + \left(\frac{4al^2}{15} + \frac{8b_3 l}{15}\right)T_6^2 + \left(\frac{7al^2}{60} + \frac{2b_3 l}{15}\right)T_7^2 + \frac{2b_3 l}{15}T_5T_6 - \right. \tag{32}$$

$$\left(\frac{al^2}{30} + \frac{b_3 l}{15}\right)T_5T_7 + \left(\frac{2al^2}{15} + \frac{2b_3 l}{15}\right)T_6T_7 + \left(\frac{al^2}{15} + b_3 l\right)T_{ос}^2 - \frac{b_3 l}{3}T_5T_{ос} -$$

$$\left.\left(\frac{2al^2}{3} + \frac{4b_3 l}{3}\right)T_6T_{ос} - \left(\frac{al^2}{3} + \frac{b_3 l}{3}\right)T_7T_{ос}\right],$$

$$J_{32} = \int\limits_{S(x=L)} \frac{h}{2}(T - T_{ос})^2 ds = \frac{\pi(aL+b)^2 h}{2}(T_7 - T_{ос})^2, \tag{33}$$

$$\mathrm{J}_{33} = \int\limits_{V_3} \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv =$$

$$\frac{\pi K_{xx}}{2}\left[\left(\frac{a^2 l}{5} + ab_3 + \frac{7b_3^2}{3l}\right)T_5^2 + \left(\frac{32a^2 l}{15} + \frac{16ab_3}{3} + \frac{16b_3^2}{3l}\right)T_6^2 + \left(\frac{23a^2 l}{15} + \frac{11ab_3}{3} + \frac{7b_3^2}{3l}\right)T_7^2 - \right. \tag{34}$$

$$\left.\left(\frac{4a^2 l}{5} + \frac{8ab_3}{3} + \frac{16b_3^2}{3l}\right)T_5T_6 + \left(\frac{2a^2 l}{5} + \frac{2ab_3}{3} + \frac{2b_3^2}{3l}\right)T_5T_7 - \left(\frac{52a^2 l}{15} + 8ab_3 + \frac{16b_3^2}{3l}\right)T_6T_7\right]$$

.

Тогда функционал тепловой энергии для третьего дискретного элемента J_3 будет равен:

$$J_3 = J_{31} + J_{32} + J_{33} \tag{35}$$

В целом для исследуемого стержня переменного сечения функционал тепловой энергии имеет вид:

$$J = J_1 + J_2 + J_3\,. \tag{36}$$

5. Построение разрешающих систем линейных алгебраических уравнений с учетом естественных граничных условий

Для определения поля температуры по длине исследуемого стержня переменного сечения с учетом наличия разнородных видов источников тепла

необходимо найти узловые температуры $T_i (i = 1 \div 7)$. С этой целью минимизируем функционал тепловой энергии J из (36) по $T_i (i = 1 \div 7)$:

$$1) \frac{\partial J}{\partial T_1} = 0; \Rightarrow \left[2h\left(\frac{al^2}{60} + \frac{2b_1 l}{15} \right) + K_{xx}\left(\frac{al^2}{5} + ab_1 + \frac{7b_1^2}{3l} \right) \right] T_1 +$$

$$\left[\frac{2hb_1 l}{15} - K_{xx}\left(\frac{4a^2 l}{5} + \frac{8ab_1}{3} + \frac{16b_1^2}{3l} \right) \right] T_2 +$$

$$\left[K_{xx}\left(\frac{a^2 l}{5} + \frac{ab_1}{3} + \frac{b_1^2}{3l} \right) - h\left(\frac{al^2}{30} + \frac{b_1 l}{15} \right) \right] T_3 = \frac{hb_1 l}{3} T_{oc} - b_1^2 q;$$

$$2) \frac{\partial J}{\partial T_2} = 0; \Rightarrow \left[\frac{2hb_1 l}{15} - 2K_{xx}\left(\frac{a^2 l}{5} + \frac{2ab_1}{3} + \frac{4b_1^2}{3l} \right) \right] T_1 +$$

$$\left[8h\left(\frac{al^2}{15} + \frac{2b_1 l}{15} \right) + K_{xx}\left(\frac{32a^2 l}{15} + \frac{11ab_1}{3} + \frac{16b_1^2}{3l} \right) \right] T_2 +$$

$$\left[2h\left(\frac{al^2}{15} + \frac{b_1 l}{15} \right) - \frac{K_{xx}}{2}\left(\frac{52a^2 l}{15} + 8ab_1 + \frac{16b_1^2}{3l} \right) \right] T_3 = h\left(\frac{2al^2}{3} + \frac{4b_1 l}{3} \right) T_{oc};$$

$$3) \frac{\partial J}{\partial T_3} = 0; \Rightarrow \left[-h\left(\frac{al^2}{30} + \frac{b_1 l}{15} \right) + K_{xx}\left(\frac{a^2 l}{5} + \frac{ab_1}{3} + \frac{b_1^2}{3l} \right) \right] T_1 +$$

$$\left[2h\left(\frac{al^2}{15} + \frac{b_1 l}{15} \right) - 2K_{xx}\left(\frac{13a^2 l}{15} + 2ab_1 + \frac{4b_1^2}{3l} \right) \right] T_2 + \left[2h\left(\frac{7al^2}{60} + \frac{2b_1 l}{15} \right) + 2h\left(\frac{al^2}{60} + \frac{2b_2 l}{15} \right) + \right.$$

$$\left. K_{xx}\left(\frac{23a^2 l}{15} + \frac{11ab_1}{3} + \frac{7b_1^2}{3l} \right) + K_{xx}\left(\frac{a^2 l}{5} + ab_2 + \frac{7b_2^2}{3l} \right) \right] T_3 +$$

$$\left[\frac{2hb_2 l}{15} - K_{xx}\left(\frac{2a^2 l}{5} + \frac{4ab_2}{3} + \frac{8b_2^2}{3l} \right) \right] T_4 +$$

$$\left[-h\left(\frac{al^2}{30} + \frac{b_2 l}{15} \right) + K_{xx}\left(\frac{a^2 l}{5} + \frac{ab_2}{3} + \frac{b_2^2}{3l} \right) \right] T_5 =$$

$$h\left(\frac{al^2}{3} + \frac{b_1 l}{3} + \frac{b_2 l}{3} \right) T_{oc};$$

$$4) \frac{\partial J}{\partial T_4} = 0; \Rightarrow \left[\frac{2hb_2 l}{15} - K_{xx}\left(\frac{2a^2 l}{5} + \frac{4ab_2}{3} + \frac{8b_2^2}{3l} \right) \right] T_3 +$$

$$\left[2h\left(\frac{4al^2}{15} + \frac{8b_2 l}{15} \right) + 16K_{xx}\left(\frac{2a^2 l}{15} + \frac{ab_2}{3} + \frac{b_2^2}{3l} \right) \right] T_4 +$$

$$\left[2h\left(\frac{al^2}{15} + \frac{b_2 l}{15} \right) - 2K_{xx}\left(\frac{13a^2 l}{15} + 2ab_2 + \frac{8b_2^2}{3l} \right) \right] T_5 = 2h\left(\frac{al^2}{3} + \frac{2b_2 l}{3} \right) T_{oc};$$

(37)

$$5)\frac{\partial J}{\partial T_5}=0;\Rightarrow\left[-h\left(\frac{al^2}{30}+\frac{b_2l}{15}\right)+K_{xx}\left(\frac{a^2l}{5}+\frac{ab_2}{3}+\frac{b_2^2}{3l}\right)\right]T_3+$$

$$\left[2h\left(\frac{al^2}{15}+\frac{b_2l}{15}\right)-2K_{xx}\left(\frac{13a^2l}{15}+2ab_2+\frac{4b_2^2}{3l}\right)\right]T_4+\left[2h\left(\frac{8al^2}{60}+\frac{2b_2l}{15}+\frac{2b_3l}{15}\right)+\right.$$

$$\left.K_{xx}\left(\frac{23a^2l}{15}+\frac{11ab_2}{3}+\frac{7b_2^2}{3l}\right)+K_{xx}\left(\frac{al^2}{5}+ab_3+\frac{7b_3^2}{3l}\right)\right]T_5+$$

$$\left[\frac{2hb_3l}{15}-2K_{xx}\left(\frac{a^2l}{5}+\frac{2ab_3}{3}+\frac{4b_3^2}{3l}\right)\right]T_6+$$

$$\left[-h\left(\frac{al^2}{30}+\frac{b_3l}{15}\right)+K_{xx}\left(\frac{a^2l}{5}+\frac{ab_3}{3}+\frac{b_3^2}{3l}\right)\right]T_7=h\left(\frac{al^2}{3}+\frac{b_2l}{3}+\frac{b_3l}{3}\right)T_{oc};$$

$$6)\frac{\partial J}{\partial T_6}=0;\Rightarrow\left[\frac{2hb_3l}{15}-2K_{xx}\left(\frac{a^2l}{5}+\frac{2ab_3}{3}+\frac{4b_3^2}{3l}\right)\right]T_5+$$

$$\left[8h\left(\frac{al^2}{15}+\frac{b_3l}{15}\right)+16K_{xx}\left(\frac{2a^2l}{15}+\frac{ab_3}{3}+\frac{b_3^2}{3l}\right)\right]T_6+$$

$$\left[2h\left(\frac{al^2}{15}+\frac{b_3l}{15}\right)-K_{xx}\left(\frac{26a^2l}{15}+4ab_3+\frac{8b_3^2}{3l}\right)\right]T_7=2h\left(\frac{al^2}{3}+\frac{2b_3l}{3}\right)T_{oc};$$

$$7)\frac{\partial J}{\partial T_7}=0;\Rightarrow\left[-h\left(\frac{al^2}{30}+\frac{b_3l}{15}\right)+K_{xx}\left(\frac{a^2l}{5}+\frac{2ab_3}{3}+\frac{2b_3^2}{3l}\right)\right]T_5+$$

$$\left[2h\left(\frac{al^2}{15}+\frac{b_3l}{15}\right)-2K_{xx}\left(\frac{13a^2l}{15}+2ab_3+\frac{4b_3^2}{3l}\right)\right]T_6+$$

$$\left[2h\left(\frac{7al^2}{60}+\frac{2b_3l}{15}\right)+K_{xx}\left(\frac{23a^2l}{15}+\frac{11ab_3}{3}+\frac{7b_3^2}{3l}\right)\right]T_7=h\left(\frac{al^2}{3}+\frac{b_3l}{3}\right)T_{oc}-h(al+b)^2;$$

(37) представляет собой систему линейных алгебраических уравнений с учетом существующих естественных граничных условий:

Эту систему определяем узловые значения температуры $T_i(i=1\div 7)$. По этим значениям строим закон распределения температуры по длине стержня переменного сечения. По дискретным элементам стержня поле температуры выражается следующим образом:

$$\begin{cases} T^{(1)}(x)=\varphi_i(x)\,T_1+\varphi_j(x)\,T_2+\varphi_k(x)\,T_3,\ 0<x<l;, \\ T^{(2)}(x)=\varphi_i(x)\,T_3+\varphi_j(x)\,T_4+\varphi_k(x)\,T_5,\ l<x<2l;, \\ T^{(3)}(x)=\varphi_i(x)\,T_5+\varphi_j(x)\,T_6+\varphi_k(x)\,T_7,\ 2l<x<3l. \end{cases} \quad (38)$$

А поле температур по всему стержню переменного сечения определяется как:

$$T(x) = T^{(1)}(x) + T^{(2)}(x) + T^{(3)}(x)\,. \tag{39}$$

6. Аналитическое определение поля температуры по длине стержня переменного сечения

Пользуясь (22) и (33) и учитывая

$$\int_V \frac{K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 dv = \frac{\pi}{2}\int_0^l (ax+b)^2\left(\frac{\partial T}{\partial x}\right)^2 dx \tag{40}$$

Перепишем (6) в следующем виде:

$$J = \pi b^2 q T_l + \frac{\pi L^2 h}{2}(T_r - T_{oc})^2 + \pi h\int_0^L (ax+b)(T - T_{oc})^2 dx + \frac{\pi K_{xx}}{2}\int_0^L (ax+b)^2\left(\frac{\partial T}{\partial x}\right)^2 dx. \tag{41}$$

Здесь $T_l = T(x=0)$ *и* $T_r = T(x=l)$ пока неизвестные.

В (41) введем следующие обозначения:

$$F(x) = \frac{(ax+b)^2 K_{xx}}{2}\left(\frac{\partial T}{\partial x}\right)^2 + (ax+b)h(T - T_{oc})^2. \tag{42}$$

Тогда:

$$J = \pi b^2 q T_l + \frac{\pi L^2 h}{2}(T_r - T_{oc})^2 + \pi h\int_0^L F(x)dx = const + \pi\int_0^L F(x)dx.$$

Как известно из курса вариационного исчисления, что для достижения минимума функционала (41) по Эйлеру необходимо выполнение следующих условий:

$$\begin{gathered}\frac{dF}{dT} - \frac{d}{dx}\left(\frac{\partial F}{\left(\frac{\partial T}{\partial x}\right)}\right) = 0,\\ \left.\frac{\partial F}{\left(\frac{\partial T}{\partial x}\right)}\right|_0^l = 0.\end{gathered} \tag{43}$$

Из (42) определим, что :

$$\begin{gathered}\frac{\mathrm{d}F}{\mathrm{d}T} = 2(ax+b)h(T - T_{oc}),\\ \frac{\partial \mathrm{F}}{\frac{\partial \mathrm{T}}{\partial \mathrm{x}}} = (ax+b)^2 K_{xx}\frac{\partial \mathrm{T}}{\partial \mathrm{x}},\\ \frac{\mathrm{d}}{\mathrm{d}x}\left(\frac{\partial \mathrm{F}}{\frac{\partial \mathrm{T}}{\partial \mathrm{x}}}\right) = 2a(ax+b)K_{xx}\frac{\partial \mathrm{T}}{\partial \mathrm{x}} + (ax+b)^2 K_{xx}\frac{\mathrm{d}^2 T}{\mathrm{d}x^2}.\end{gathered} \tag{44}$$

Подставляя (44) в (43) получим:

$$\frac{\mathrm{d}F}{\mathrm{dT}} - \frac{\mathrm{d}}{\mathrm{dx}}\left(\frac{\partial \mathrm{F}}{\partial \mathrm{T}}\right) = 2(ax+b)h(T-T_{oc}) - 2a(ax+b)K_{xx}\frac{\partial \mathrm{T}}{\partial \mathrm{x}}$$

$$+(ax+b)^2 K_{xx}\frac{\mathrm{d}^2T}{\mathrm{d}x^2} = 0,$$

или

$$(ax+b)^2 K_{xx}\frac{\mathrm{d}^2T}{\mathrm{d}x^2} + 2a(ax+b)K_{xx}\frac{\partial \mathrm{T}}{\partial \mathrm{x}} - 2(ax+b)h(T-T_{oc}) = 0 \quad \text{или}$$

$$\frac{\mathrm{d}^2T}{\mathrm{d}x^2} + \frac{2a}{(ax+b)}\frac{\mathrm{d}T}{\mathrm{dx}} - \frac{2h}{(ax+b)K_{xx}}(T-T_{oc}) = 0. \qquad (45)$$

Это обыкновенное дифференциальное уравнение второго порядка с переменными коэффициентами[13].

Введем обозначение:

$$\bar{T}(x) = T(x) - T_{oc}.$$

Тогда (45) имеет вид

$$\frac{\mathrm{d}^2\bar{T}}{\mathrm{d}x^2} + \frac{2a}{(ax+b)}\frac{\mathrm{d}\bar{T}}{\mathrm{dx}} - \frac{2h\bar{T}}{(ax+b)K_{xx}} = 0. \qquad (46)$$

Пусть заданы исходные данные:

$a = -0{,}1;\quad b = 4\text{см};\quad h = 10\ \frac{\text{Вт}}{\text{см}^2{}^\circ\text{C}}\quad K_{xx} = 100\frac{\text{Вт}}{\text{см}^\circ\text{C}}.$

При принятых исходных данных уравнение (46) будет иметь следующий вид:

$$\frac{\mathrm{d}^2\bar{T}}{\mathrm{d}x^2} - \frac{0.2}{(-0.1x+4)}\cdot\frac{\mathrm{d}T}{\mathrm{dx}} - \frac{0.2}{(-0.1x+4)}\cdot\bar{T} = 0. \qquad (47)$$

Общее решение имеет вид:

$$\bar{T}(x) = \frac{k_1 \mathrm{c}_1 I_1\left(k_2\sqrt{40-x}\right)}{\sqrt{40-x}} - \frac{k_1 \mathrm{c}_2 K_{-1}\left(k_2\sqrt{40-x}\right)}{\sqrt{40-x}}, \qquad (48)$$

где k_1=1.41421, k_2=2.82843.

I_1 и K_{-1} - функции Бесселя первого рода 1-го порядка и -1-го порядка соответственно[14];

c_1 и c_2 - постоянные интегрирования.

Значения констант c_1 и c_2 определяются из граничных условий, для x=0 и x=l :

$$1)\qquad K_{xx}\frac{\partial\bar{T}}{\partial x} - q = 0,\ \text{при x=0 ,} \qquad (49)$$

$$2)\qquad K_{xx}\frac{\partial\bar{T}}{\partial x} + h\bar{T}(x)=0 \text{ при x=l.} \qquad (50)$$

Из (48) и из свойства Функций Бесселя I_1 и K_{-1} находим производную $\overline{T(\mathrm{x})}$:

$$\frac{\mathrm{d}\bar{T}}{\mathrm{dx}} = \left[\frac{k_1 I_1\left(k_2\sqrt{40-x}\right)}{2\sqrt{(40-x)^3}} - \frac{k_1 k_2 I'_1\left(k_2\sqrt{40-x}\right)}{2\sqrt{40-x}}\right]\mathrm{c}_1 -$$

$$\left[\frac{k_1 K_{-1}\left(k_2\sqrt{40-x}\right)}{2\sqrt{(40-x)^3}} - \frac{k_1 k_2 K'_{-1}\left(k_2\sqrt{40-x}\right)}{2\sqrt{40-x}}\right]\mathrm{c}_2. \qquad (51)$$

Отсюда находим значение $\frac{\mathrm{d}\bar{T}}{\mathrm{dx}}(x=0)$:

$$\frac{\mathrm{d}\bar{T}}{\mathrm{dx}}(x=0)=\left[\frac{k_1 I_1\left(k_2\sqrt{40}\right)}{2\sqrt{(40)^3}}-\frac{k_1 k_2 I'_1\left(k_2\sqrt{40}\right)}{80}\right]\mathrm{c}_1-$$
$$\left[\frac{k_1 K_{-1}\left(k_2\sqrt{40}\right)}{2\sqrt{(40)^3}}-\frac{k_1 k_2 K'_{-1}\left(k_2\sqrt{40}\right)}{80}\right]\mathrm{c}_2=A\mathrm{c}_1-\mathrm{Bc}_2, \quad (52)$$

где $A=\frac{k_1 I_1\left(k_2\sqrt{40}\right)}{2\sqrt{(40)^3}}-\frac{k_1 k_2 I'_1\left(k_2\sqrt{40}\right)}{80}$,

$$\mathrm{B}=\frac{k_1 K_{-1}\left(k_2\sqrt{40-x}\right)}{2\sqrt{(40)^3}}-\frac{k_1 k_2 K'_{-1}\left(k_2\sqrt{40-x}\right)}{80}. \quad (53)$$

Подставляя (53) в (49) получим:

$$A\mathrm{c}_1-\mathrm{Bc}_2=\frac{q}{K_{xx}}.$$

Теперь из (51) находим $\frac{\mathrm{d}\bar{T}}{\mathrm{dx}}(x=l)$:

$$\frac{\mathrm{d}\bar{T}}{\mathrm{dx}}(x=l)=\left[\frac{k_1 I_1\left(k_2\sqrt{40-l}\right)}{2\sqrt{(40-l)^3}}-\frac{k_1 k_2 I'_1\left(k_2\sqrt{40-l}\right)}{2(40-l)}\right]\mathrm{c}_1-$$
$$\left[\frac{k_1 K_{-1}\left(k_2\sqrt{40-l}\right)}{2\sqrt{(40-l)^3}}-\frac{k_1 k_2 K'_{-1}\left(k_2\sqrt{40-l}\right)}{2(40-l)}\right]\mathrm{c}_2=C\mathrm{c}_1-\mathrm{Dc}_2, \quad (55)$$

где

$$C=\left[\frac{k_1 I_1\left(k_2\sqrt{40-l}\right)}{2\sqrt{(40-l)^3}}-\frac{k_1 k_2 I'_1\left(k_2\sqrt{40-l}\right)}{2(40-l)}\right],$$

$$\mathrm{D}=\left[\frac{k_1 K_{-1}\left(k_2\sqrt{40-l}\right)}{2\sqrt{(40-l)^3}}-\frac{k_1 k_2 K'_{-1}\left(k_2\sqrt{40-l}\right)}{2(40-l)}\right]. \quad (56)$$

Из (48) определим $T(x=l)$:

$$\bar{T}\,(x=l)=\left[\frac{k_1 I_1\left(k_2\sqrt{40-l}\right)}{\sqrt{(40-l)}}\mathrm{c}_1-\frac{k_1 \mathrm{c}_2 K_{-1}\left(k_2\sqrt{40-l}\right)}{\sqrt{(40-l)}}\right]=E\mathrm{c}_1-\mathrm{Fc}_2. \quad (57)$$

Из граничного условия (49) при $x=0$ и из (51) получим

$$A\mathrm{c}_1-\mathrm{Bc}_2=\frac{q}{K_{xx}}. \quad (58)$$

Из граничного условия (50) совместно с (55) и (57) имеем

$$\bar{T}'(l)=-\frac{h}{K_{xx}}\bar{T}(l). \quad (59)$$

Далее подставляя (55) и (57) в (59) получим

$$C\mathrm{c}_1-\mathrm{Dc}_2==-\frac{h}{K_{xx}}(E\mathrm{c}_1+\mathrm{Fc}_2)$$

или

$$\left(C+\frac{Eh}{K_{xx}}\right)\mathrm{c}_1+\left(\frac{\mathrm{F}h}{K_{xx}}-\mathrm{D}\right)\mathrm{c}_2=0$$

или

$$G_1\mathrm{c}_1+G_2\mathrm{c}_2=0. \quad (60)$$

Теперь решая (58) и (60) совместно определим значения констант c_1 и c_2.

$$c_2=-\frac{AqG_1}{K_{xx}(AG_2+\mathrm{B}G_1)}, \quad (61)$$

$$c_1=-\frac{BqG_2}{K_{xx}(AG_2+\mathrm{B}G_1)}. \quad (62)$$

Далее подставляя (61) и (62) в (48) определяем закон распределения температуры по длине исследуемого стержня переменного сечения:

$$\bar{T}(x)=\frac{k_1 K_{-1}\left(k_2\sqrt{40-x}\right)}{\sqrt{40-x}}\frac{AqG_1}{K_{xx}(AG_2+\mathrm{B}G_1)}-\frac{k_1 I_1\left(k_2\sqrt{40-x}\right)}{\sqrt{40-x}}\frac{BqG_2}{K_{xx}(AG_2+\mathrm{B}G_1)} \quad (63)$$

Учитывая $\bar{T}(x) = T(x) - T_{oc}$ получим

$$T(x) = \bar{T}(x) + T_{oc} = \frac{k_1 K_{-1}\left(k_2\sqrt{40-x}\right)}{\sqrt{40-x}} \frac{AqG_1}{K_{xx}(AG_2 + \mathrm{B}G_1)} - \frac{k_1 I_1\left(k_2\sqrt{40-x}\right)}{\sqrt{40-x}} \frac{BqG_2}{K_{xx}(AG_2 + \mathrm{B}G_1)} + T_{oc}, \quad 0 \le x \le l \tag{64}$$

Для получения аналитического решения составлена программа на Python, листинг которой имеет вид:

```
from sympy import *
import sympy
import numpy
import numpy as np
import pprint
import matplotlib.pyplot as plt
import math
import pylab
#Импортируем пакет со вспомогательными функциями
from matplotlib import mlab
from mpmath import*
a=a1=2.82843
q=-600
Toc=40
Kxx=100
L=20
h=10
# Функции Бесселя в точках 0 и L
J0=besselj(3,a1*sqrt(40))
JL=besselj(3,a1*sqrt(40-L))
I0=besseli(-3,a1*sqrt(40))
IL=besseli(-3,a1*sqrt(40-L))
# Производные от функции Бесселя в точках 0 и L
JP0=diff(lambda x: besselj(3,x),a1*sqrt(40))
JPL=diff(lambda x: besselj(3,x),a1*sqrt(40-L))
IP0=diff(lambda x: besseli(-3,x),a1*sqrt(40))
IPL=diff(lambda x: besseli(-3,x),a1*sqrt(40-L))
A=0.75*a*sqrt(40)*J0+10*a**2*JP0
B=0.75*a*sqrt(40)*I0+10*a**2*IP0
C=0.75*a*sqrt(40-L)*JL + 0.25*a**2*(40-L)*JPL
D=0.75*a*sqrt(40-L)*IL + 0.25*a**2*(40-L)*IPL
E=-0.5*a*(40-L)**1.5*JL
F=0.5*a*(40-L)**1.5*IL
G=C-h*E/Kxx
K=D+h*F/Kxx
C2=(q/Kxx)/( A*K/G -B  )
```

```
C1=K*C2/G
def f(x):
J3=besselj(3, a1*sqrt(40-x))
I3=besseli(-3, a1*sqrt(40-x))
print("J3=",J3)
print("I3=",I3)
A1=-0.5*a*C1*(40-x)**1.5*J3
B1=0.5*a*C2*(40-x)**1.5*I3
print("A1=",A1)
print("B1=",B1)
return A1+B1+Toc
# Постоение графика
xlist =np.linspace(0.0, L-1, 11)
ylist = [f(x) for x in xlist]
print("ylist",ylist)
plt.plot (xlist, ylist)
plt.title(u"Температура",{'fontname':'Arial','fontsize':16})
plt.ylabel(u"T",{'fontname':'Arial','fontsize':16})
plt.xlabel(u" x ",{'fontname':'Arial','fontsize':16})
plt.show()
```

1. Практические результаты

Для получения численных результатов был взяты следующие исходные данные – (рисунок 1):

$L=20$ см, $r=1$см, $Kxx = 100\frac{Bm}{см\cdot^{\circ}C}$, Toc1=40 $^{\circ}C$,

$T_{oc} = 40\ ^{\circ}C$, $q = -600\frac{Bm}{см^2}$, $h = h1 = 10$.

Результаты вычисления следующие:

1. КВАДРАТИЧНАЯ АППРОКСИМАЦИЯ

#1 интервал Температура
T1= [67.92855, 42.029766, 43.049477]

#2_интервала Температура
T2=[69.068985, 49.928986, 43.50344, 41.026497, 40.44771]

#3_интервала Температура
T3=[69.20674, 54.493587, 47.0812, 43.297554, 41.51776, 40.67564, 40.373993]

#4_интервала Температура
T4=[69.23517,57.355713,50.1775,45.841362,43.306587,41.825996,41.002014,40.556072,40.364388]

#5_интервалов Температура
T5=[69.243614,59.300953,52.62903,48.16267,45.22441,43.296844,42.059654,41.270233,40.784866,40.498936,40.36207]

2. АНАЛИТИЧЕСКОЕ РЕШЕНИЕ

Y1=[69.504376630105682,43.437815854236263,40.501351299789739]

Y2=[69.504376630105682,50.824597262032803,43.437815854236263,40.844357649803541,40.501351299789739]

Y3=[69.504376630105682,55.270384039588436,47.558838457810936,43.437815854236263,41.370759023514708, 40.56444046836684,40.501351299789739]

Y4=[69.504376630105682,58.06019091538154,50.824597262032803,46.270006877712369,43.437815854236263,41.746126152703411,40.844357649803541,40.498277038170684,40.501351299789739]

Y5=[69.504376630105682,59.950758928780942,53.326760903953698,48.74512634530457,45.588792023303569,43.437815854236263,42.012380680912081,41.126708108557914,40.650654976243196,40.477835619354991, 40.501351299789739]

Эти результаты при разбиение стержня от одного до пяти элементов представлены в таблице 1.

Таблица 1 Численное и аналитическое решение для различных узлов

Решение для 1 элемента		Решение для 2 элементов		Решение для 3 элементов		Решение для 4 элементов		Решение для 5 элементов	
Численное	Аналитическое	Численное	Аналитическое	Численное	Аналитическое	Численное	Аналитическое	Численное	Аналитическое
67.93	69.50	69.07	69.50	69.21	69.5	69.24	69.5	69.24	69.5
42.03	43.44	49.93	50.82	54.49	55.27	57.36	58.06	59.3	59.95
	40.5	43.50	43.44	47.08	47.56	50.18	50.82	52.63	53.33
		41.03	40.84	43.30	43.44	45.84	46.27	48.16	48.75
		40.45	40.5	41.52	41.37	43.31	43.43	45.22	45.59
				40.67	40.56	43.05	41.75	43.3	43.44
				40.37	40.5		40.84	42.06	42.01
							40.49	41.27	41.13
							40.5	40.78	40.65
								40.5	40.47
								40.36	40.5

Закон распределения температуры по длине исследуемого стержня, полученные квадратичной аппроксимацией и аналитически представлены на рисунках 3 и 4, соответственно.

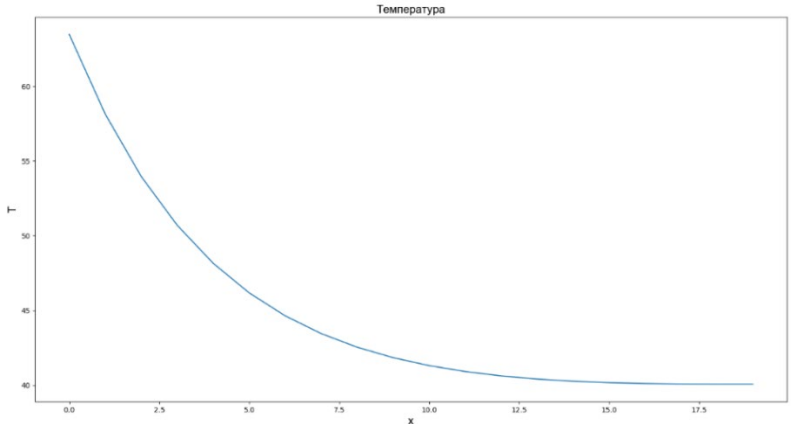


Рисунок 3. – Закон распределения температуры по длине исследуемого стержня при квадратичной аппроксимации

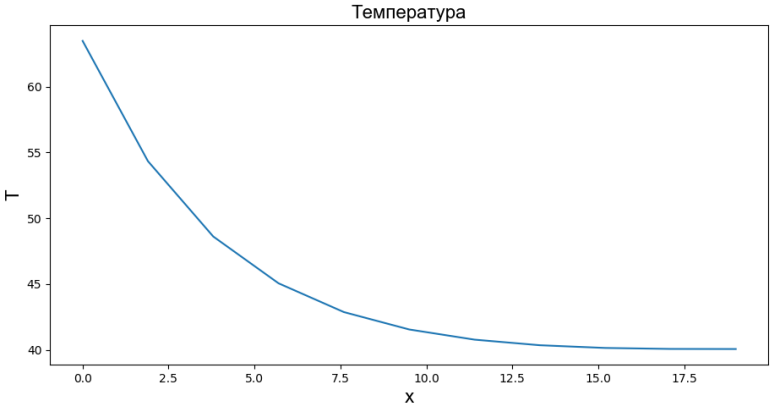


Рисунок – 4. Закон распределения температуры по длине исследуемого стержня с помощью аналитического метода

Сравнительные графики закона распределения температур, полученные квадратичной аппроксимацией и аналитическим способом от одного до пяти элементов показаны на рисунке 5.

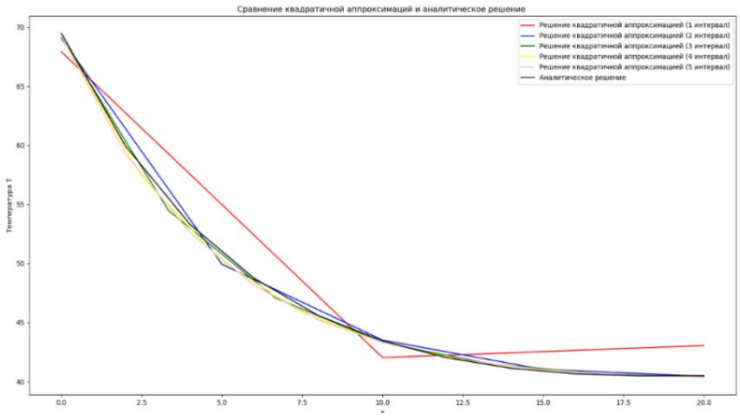


Рисунок 5. График закона распределения температур, полученные квадратичной аппроксимацией и аналитическим способом от одного до пяти элементов.

Максимальные относительные ошибки для различного количества элементов показаны в таблице 2.

Таблица 2 Изменение относительной ошибка с увеличением числа узлов

Относительная ошибка	Число узлов				
	2	5	7	9	11
Delta,%	6.2914	0.4459	0.3553	0.35	0.3489

Уменьшение относительной ошибки с увеличением числа элементов показано на рисунке 6

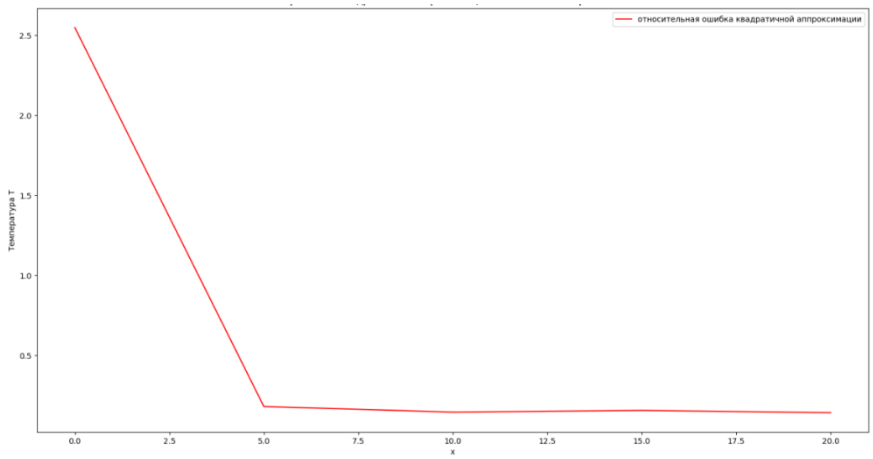


Рисунок 6. –Относительная ошибка квадратичной аппроксимации

Из таблицы 2 и из рисунка 6 видно, что уже после двух элементов относительная ошибка уменьшается незначительно.

Заключение

Пользуясь классическим вариационным принципом Эйлера, построено уравнение теплопроводности для стержня переменного сечения. Боковая поверхность стержня теплоизолирована. На площадь поперечного сечения левого конца стержня подведен тепловой поток постоянной интенсивности. Через площадь поперечного сечения правого конца стержня происходит теплообмен с окружающей ее средой. Полученное уравнение теплопроводности для исследуемого стержня является обыкновенным дифференциальным уравнением второго порядка с переменными коэффициентами. При конкретных исходных данных с использованием системы Wolfram Alfa построено общее решение получения уравнения теплопроводности. Это решение получено на основе Бесселевских функций первого рода первого и минус первого порядка. Практические результаты для рассматриваемого примера показали, что решение, полученное методом конечных элементов хорошо согласуется с аналитическим решением. Следует отметить, что решение, которое получено методом конечных элементов достаточно хорошо совпадает с аналитическим решением с Бесселевскими функциями.

Литература

1. Krieth F., Principles of Heat Transfer, 3-rd ed. Index Educational Publishers, N.Y., 1977
2. Huebner K.H., The Finite Element Method for Engineers, Wiley, N.Y., 1975
3. Harry J. Segerlind Applied Finite Element Analysis, N.Y., 1976
4. Visser W., Finite Element Method for Determination of Non-Stationary Temperature Distribution and Thermal Deformations, Proc. Conf. on Matrix Methods in Structural Mechanics, Air Force Inst. of Technology Wrights Patterson Air Force base, Dayton, Ohio, 1965
5. Conte S.D., Elementary Numerical Analysis, McGray-Hill, N.Y. 1965
6. Kreyszig E., Advanced Engineering Mathematics, 3-rd ed., Wiley, N.Y., 1972
7. Williams P.W., Numerical Computation, Nelson, Don Mill, Can., 1972
8. Johnson C., Numerical Solution of Partial Differential Equations by the Finite Element Method, Cambridge University Press, Cambridge, 1987

9. Gaspar Jr., Moreira M.L., Desampaio P.A.B. Temperature Distribution Fuel Rods: A study on the Effect of Eccentricity in the Position of U02 Pellets., 0-th International Conference «Nuclear Energy for New Europe» 2011

10. Zienkiewicz O.C. The method in Engineering science. Butterworth-Heinemann. - Oxford-Auckland-Boston-Johannesburg-Melburne-New Delhi, 2000. – P.690.

11. Timoshenko S, Goodier J.N. Theory of Elastic. N.Y., 1951

12. Сегерлинд Л. Применение метода конечных элементов. - М.: Мир, 1979.

13. https://math.semestr.ru/math/diffur.php

14. Дунаев А.С., Шлычков В.И. Специальные функции. – М.:Флинта: Издательство Уральского Университета,2017.- 938 с.

15. Ногайбаева М.О. Кудайкулов А.К. Определение термонапряженного состояния стержня переменного сечения

16. Anarbay Kudaykulov, Tashev Azat, Mukaddas Arshidinova and Kalamkas Begaliyeva Power research technique of thermomechanical condition of a core of restricted length, variable section at influence of heterogeneous types of sources of heat. 1st International conference on sustainable science and technology (ICSuSaT-2018) 12-16 October 2018, Antalya-Turkey

17. Arshidinova, M., Tashev, A., Kudaykulov, A. Software implementation of a computational algorithm for accounting for the presence of local superficial heat exchanges in rods of variable section // International Journal of Advanced Trends in Computer Science and Engineering 9(4), 366, с. 6710-6716
https://www.scopus.com/record/display.uri?eid=2-s2.0-85090274609&origin=resultslist

18. Кудайкулов А.К., Ташев А. Правила получения системы дифференциальных уравнений для оценки распространения тепла в стержне с использованием квадратичной аппроксимации при увеличении числа элементов // Проблемы информатики. – Новосибирск, 2016. – № 4. – С. 25-44.

НОВЫЕ ПОДХОДЫ РЕШЕНИЯ ЗАДАЧ МОДЕЛИРОВАНИЯ ПАВОДКОВЫХ И ПРОРЫВНЫХ ВОЛН И ПРОГНОЗИРОВАНИЕ АВАРИЙНОЙ СИТУАЦИИ

М.Н. Калимолдаев[1,2], Т.Ж. Мазаков[1,2], Ш.А. Джомартова[2],
Г.З. Зиятбекова[1,2], А.Т. Мазакова[1,2]
ziyatbekova@mail.ru
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Казахский национальный университет имени аль-Фараби, Казахстан

Аннотация. *Статья посвящена разработке методики моделирования речного потока. В данной работе рассматриваются возможные подходы моделирования течения жидкостей. Приводится описание технологии мониторинга паводков и наводнений, разработанной в Казахстане, обсуждаются результаты её практического использования в отдельных регионах и намечаются направления дальнейшего развития. Данная информация в последствии используется для прогнозирования аварийной ситуации.*

Ключевые слова: *наводнение, паводковые и прорывные волны, компьютерное моделирование.*

Введение. В настоящее время известно множество примеров чрезвычайных ситуаций (ЧС), связанных с затоплением, вызванных распространением паводковых и прорывных волн. В данное время в нашей стране стоит задача защиты сельскохозяйственных земель и населенных пунктов от затопления. Затопление сельскохозяйственных земель возникает как при пропуске крупномасштабных паводков, так и природных, техногенных факторах. В частности, опасность возникновения чрезвычайных ситуаций, связанных с затоплением территорий, остается очень высокой, продолжает увеличиваться количество пострадавших и экономический ущерб от наводнений.

Проблема паводков становится все острее. Ситуация, когда в разных регионах страны населенные пункты в буквальном смысле уходят под воду, стала уже нормой. При этом бюджетные средства по-прежнему идут на ликвидацию последствий наводнений, вместо того чтобы их не допустить. Паводок – фаза водного режима, которая характеризуется интенсивным, обычно кратковременным увеличением расходов и уровней воды и вызывается дождями или снеготаянием во время оттепелей. Весенний паводок является сезонным явлением, и, по сути, это явление в последнее время в той или иной степени избежать невозможно.

Методы исследования. Основными методами борьбы с наводнениями являются осуществление комплекса мер по предотвращению или смягчению последствий наводнений (строительство гидротехнических сооружений по регулированию стока, создание оградительных дамб и т.д.) и своевременное оповещение о возможности и масштабах наводнения. Для управления действиями по предотвращению нежелательного развития событий и преодолению последствий наводнений необходимо привлечение больших объемов разнородных данных, поступающих из различных источников (картографическая, аэрокосмическая,

гидрологическая информация), оперативная обработка и анализ этой информации, и представление ее в виде, обеспечивающем принятие решений в ограниченных временных рамках.

Попытки разрешить конфликт между необходимостью использования пойменных и прибрежных земель и убытками от возможных наводнений предпринимались неоднократно многими специалистами. Но до сих пор этот конфликт не разрешен. Для решения задачи о возможности использования прибрежных земель необходимо проводить анализ возможного ущерба при наводнениях.

В случае прохождения паводка или волны прорыва значительно ухудшается качество земель. Даже кратковременный подъем воды в реке во время паводка может вызвать затопление прибрежных земель, что неизменно повлечет за собой значительные убытки, связанные, как с возможной потерей урожая, так и с ухудшением качества земель.

В качестве мер по предупреждению ущерба, вызванного возможным наводнением, необходимо проводить такие инженерно-технические мероприятия, как:

– мониторинг и регулирование паводкового стока рек с использованием различных инженерных сооружений: плотин, дамб, укрепление берегов рек, спрямление русел и т. д.;

– проектирование и рациональное размещение элементов инфраструктуры и жилых построек в соответствии с учетом потенциально-опасных зон возможного затопления; в зонах с частыми случаями паводка возможно строительство домов на сваях, либо перевод первых этажей зданий в нежилой фонд;

– обеспечение устойчивости работы с учетом возможного возникновения ЧС, важных инфраструктурных элементов: мостов, линий связи и т.д.

Одной из наиболее эффективных областей приложения данных дистанционного зондирования Земли (ДЗЗ) является мониторинг чрезвычайных ситуаций (ЧС) [1]. В связи с развитием информационных технологий наступил период, когда нужно решать комплексные задачи по управлению половодьями и паводками для защиты населения и объектов экономики от наводнений с интеграцией разнородных информационных ресурсов из различных источников на основе общего, системного принципа. Идеально отвечают такой потребности геоинформационные системы (ГИС). ГИС, с одной стороны, родственны системам управления базами данных (СУБД), а с другой - графическим пакетам, прежде всего системам автоматизированного проектирования (САПР). Они позволяют привязывать базы данных к графическим объектам, то есть данные к пространственному положению объектов. А задачи, связанные с прогнозированием и оценкой последствий чрезвычайных ситуаций, требуют именно такого подхода [Jackson, etal., 1980]. Многие ГИС-аналитики утверждают, что до 80% информации, связанной с деятельностью человека, имеет пространственное распределение и, следовательно, лежит в области компетенции ГИС [Даниленко, 2006].

В рамках Госпрограммы предусматривалось разработать ряд комплексных ГИС-технологий мониторинга ЧС, обеспечивающих решение следующих задач:

– мониторинг паводков и оценка риска затопления регионов Казахстана;

– мониторинг лесных и степных пожаров и оценка рисков пожароопасности;

– раннее предупреждение и дистанционный контроль стихийных бедствий метеорологического характера;

– мониторинг трансграничных ЧС;

– дистанционный контроль температурного режима очагов сейсмической активности.

Работы по созданию технологий космического мониторинга паводков и наводнений ведутся в Казахстане с 2002 года [2-4]. В составе комплекса реализовано несколько технологических блоков, позволяющих:

– оперативно обнаруживать участки затопления;

– картировать и определять площади зон затопления с нарастающим итогом;

– осуществлять прогноз развития паводков и оценивать их потенциальную опасность для населенных пунктов и особо важных объектов;

– оценивать и анализировать риски затопления для различных регионов.

Для решения задачи о получении зон затопления в результате паводка возможны следующие способы получения результатов:

1. Физические модели;
2. Проведение аналитических расчетов;
3. Численное моделирование.

На сегодняшний день показано, что определить параметры распространения паводковых и прорывных волн можно только с применением численного компьютерного моделирования. Течения жидкостей, делятся на два сильно различных друг от друга типа: ламинарные (плавно изменяющиеся, регулярные) и турбулентные (неупорядоченные). В случаях распространение паводковых и прорывных волн течение жидкости будет турбулентным [5,6].

Все существующие программные комплексы можно разделить на одномерное, двумерное и трехмерное. Численное моделирование в одномерном и двумерном случае значительно упрощает исследуемую модель, и не дает полного представления о процессах, происходящих при распространении волны прорыва или волны паводка, что будет показано далее. Таким образом наиболее точным будет применение трехмерного численного моделирования для проведения расчета паводковых и прорывных волн.

В большинстве случаев базовой системой для гидродинамического моделирования служит трехмерная система эволюционных уравнений Навье-Стокса.

Проведем анализ необходимых исходных данных для различных способов моделирования.

Система дифференциальных уравнений Сен-Венана для неустановившегося движения жидкости, при условии движения потока в русле с достаточно большим уклоном дна может быть приведена к виду:

$$\frac{\partial h}{\partial t} + \frac{1}{b}\frac{\partial Q}{\partial x} = 0, \quad (1)$$

$$\frac{\partial Q}{\partial t} + \left(\frac{Q}{bK}\frac{dK}{dh}\right)\frac{\partial Q}{\partial x} - \frac{K^2}{2bQ}\frac{\partial^2 Q}{\partial x^2} = 0, \quad (2)$$

где: t – время, $0 \le t \le T = const$, с; x – пространственная координата по направлению движения, причем $0 \le x \le l$, м; J – уклон дна, м/м; b – ширина σрусла, м; h(x,t) – глубина русла, м; K(h) – расходная характеристика русла ($K(h) =$

$\frac{bh^{\frac{5}{3}}}{n}$, где n – коэффициент шероховатости); v(x,t) – средняя скорость течения в сечении русла, м/с; Q(x,t) – расход в выбранном сечении, $\frac{м^3}{с}$.

Для расчета по этим уравнениям, описывающих неустановившееся неравномерное движение водных масс, необходимо задать начальные и граничные условия на участке реки. Начальные условия требуют задать состояние потока, его скорость или расход во всех точках русла в момент времени t=0. Граничные условия определяют уровень воды, ее скорость или расход в верхнем и нижнем створах участка реки в любой момент времени.

Начальные условия будут иметь вид:

$$Q(x,0) = \sigma_0(x),\ b(x,0) = \gamma_0(x), \tag{3}$$

Граничные условия:

$$Q(0,t) = \sigma_1(t),\ h(0,t) = \gamma_1(t), \tag{4}$$

$$Q(l,t) = \sigma_2(t),\ h(l,t) = \gamma_2(t), \tag{5}$$

Поставленную задачу можно решать, разбивая интервал [0, T] на отрезки и рассчитывая на них все характеристики потока, поскольку для реальных речных русел в условиях неравномерного движения площадь поперечного сечения меняется в зависимости от x, а так как движение неустановившееся, тогда площадь зависит и от времени. Таким образом, следует разбить участок на отрезки с неизменными гидравлическими характеристиками, затем для отрезков решать систем уравнений Сен-Венана, где для первого участка входной гидрограф берется из начальных данных, затем рассчитываются параметры стока на этом участке и выходной гидрограф, который служит выходным гидрографом для второго участка, и так далее.

Задача моделирования речного стока является важной проблемой. В настоящее время нет единого решения для прогноза речного стока. Постоянное стремление к упрощению методов приводит к потере качества в результатах исследования. Но для более сложных моделей требуется задавать многочисленные данные наблюдений, которых зачастую нет, поэтому приходится прибегать к упрощению моделей. Одномерные модели моделирования речного стока могут применяться лишь для предварительных расчетов. Для более точного исследования следует применять модели более высокого уровня [7-9].

Выводы. В работе показано, что определить параметры распространения паводковых и прорывных волн можно только с применением численного компьютерного моделирования. Все рассмотренные методики не позволяют оперативно получать исходные данные для обоснования противопаводковых мероприятий и требует значительных материальных и временных ресурсов. Таким образом, очевидна необходимость создания упрощённой технологии инженерных обоснований противопаводковых мероприятий, сопоставимой по надежности получения результатов с существующими, но при этом обладающей преимуществом в скорости проведения моделирования и простоте реализации. Технология должна при минимальном наборе исходных данных позволять проводить моделирование

распространения волны паводка или волны прорыва, по результатам которого получать двумерную карту исследуемой местности с зонами затопления, ранжированными по глубине, а также другиепараметры, характеризующие распространение волн.

Работа выполнена за счет средств программно-целевого финансирования на основе договора по оказании услуг субподряда «Разработка национального электронного банка данных по научной зоологической коллекции Республики Казахстан, обеспечивающего их эффективное использование в науке и образовании».

Литература

1. Султангазин У.М., Спивак Л.Ф. Национальная система космического мониторинга Республики Казахстан: концепции, архитектура, направления развития // Исследование Земли из космоса, 2006. – №2. – С. 38-50.

2. Spivak L., Arkhipkin O., Pankratov V., Vitkovskaya I., Sagatdinova G. Space monitoring of floods in Kazakhstan. Mathematics and Computers in Simulation. 2004. – P. 365–370.

3. Спивак Л.Ф., Архипкин О.П., Панкратов В.С., Шагарова Л.В., Сагатдинова Г.Н. Технология мониторинга паводков и наводнений в Западном Казахстане // Современные проблемы дистанционного зондирования Земли из космоса: Физические основы, методы и технологии мониторинга окружающей среды, потенциально опасных явлений и объектов. Москва: Полиграфсервис, 2004. – С. 279-286.

4. Spivak L.F., Arkhipkin O.P., Sagatdinova G.N. Development of Flood Monitoring Information System in Kazakhstan // Proceedings of 31st International Symposium on Remote Sensing of Environment. Saint-Petersburg, 2005.

5. Бредшоу П. Введение в турбулентность и ее измерение. - М.: Мир, 1974. –239 с.

6. Кучмент Л.С., Гельфан А.Н., Демидов В.Н. Развитие физико-математических моделей формирования речного стока и опыт их применения при недостатке гидрометрических наблюдений // Тезисы докладов VI Всероссийского гидрологического съезда. – СПб.: Гидрометеоиздат. – 2004. – С. 121-123.

7. Абрахин С.И., Прокошев В.Г., Аракелян С.М. Математическое моделирование последствий прорыва плотины на реке с применением ГИС-технологий // XII Всероссийская научно-методическая конференция «Телематика – 2005»: Санкт-Петербург, СПбИТМО – 2005, т. 1, С. 216-217.

8. Виноградов Ю.Б., Виноградова Т.А. Математическое моделирование в гидрологии. – М.: Изд. центр «Академия», 2010. – 304 с.

9. Немировский А.А. Разработка метода формирования намывного хвостохранилища, утойчивого к ветровым потокам. – М.: Дис. канд.техн.наук, 2016. – 131 с.

ҚОЛДАНБАЛЫ МАТЕМАТИКАНЫ ЭКОНОМИКА ЖӘНЕ ҚҰҚЫҚТАНУ САЛАЛАРЫНА ҚОЛДАНУДЫҢ ЕРЕКШЕЛІКТЕРІ

Байбеков С.Н.
baibekovsn@mail.ru
«Қазақстан инжиниринг» R&D орталығы, Қазақстан

Аннотация. *Мақалада экономика және құқықтану салаларына қатысты көптеген процесстер мен құбылыстарды шешу кезінде қолданбалы математиканың алатын орыны мен ерекшеліктері анықтанылып, оны нақты сипаттау үшін бірнеше мысалдар қарастырылды. Мақала соңында заң ғылымдарын дамыту үшін болашақ мамандар дайындайтын заң факультеттерінде «Қолданбалы математика негіздерін заң процесстеріне пайдалану» атты қосымша оқу курсын ашу туралы ұсыныс берілді.*

Қолданбалы математика деп математикалық әдістер мен алгоритмдерді ғылым мен техниканың әртүрлі салаларында қолдануды қарастыратын математика саласын айтамыз. Алайда, ғалымдардың айтуы бойынша, қолданбалы математика не? - деген сұраққа нақты логикалық классификация жасау мүмкін емес.

Белгілі ғалым академик В.И.Арнольдтың әзілдеп ирониялық түрде айтқанына қарасақ: «Таза математика мен қолданбалы математиканың ғылыми түрде бір-бірінен ешқандай айырмашылығы жоқ, олардың айырмашылығы әлеуметтік сипатпен ғана ерекшеленеді. Осы себепті таза математикке математикалық фактілерді ашқаны үшін ақы төлесе, қолданбалы математикке практикалық есептерді шешкені үшін ақы төлейді. Ал Ресейде әрбір математик «таза» және «қолданбалы» математиканың өкілі болып табылады». Демек академик В.И.Арнольд «таза» және «қолданбалы» математиканы ажыратпай, оларды бірге және біртұтас қарастыруды меңзейді.

Дегенмен қазіргі кезде «қолданбалы математика» термині кең мағынада қолданылады. Тіпті таза математиканың құрамына кіретін сандар теориясы сияқты салалар да қазір қолданбалы математика салаларына қатысты бола бастады, бұған мысал үшін сандар теориясының криптографияда қолданылуын айтуға болады. Осы себепті кейбір ғалымдар «қолданылатын математика (применимая математика)» терминін физикамен қатар дамыған дәстүрлі қолданбалы математика мен қазіргі әлемдегі заманауи есептерге қолданылатын математиканың көптеген салаларын ажырату үшін қолданады.

Бұған қоса көптеген математиктер математикалық әдістермен айналысатын «қолданбалы математиканы» ғылым мен техникадағы «математиканың қолданылуынан» ажыратуды дұрыс деп санайды. Мысалы, популяция моделін қолданатын биологтар қолданбалы математикамен емес, математиканы қолданумен айналысады. Алайда осы математикалық биологтардың таза математиканың өсуіне түрткі болғанын да айта кетуге болады. Дегенмен әйгілі математиктер Пуанкаре мен В.И.Арнольд «қолданбалы математиканы (прикладная математика)» жоққа шығарып, ғылым мен техниканың және көптеген алуан түрлі процесстер мен құбылыстарды зеттеуге математиканың қолданылуын («приложение математики») айтады және соны ғана мойындайды.

Дегенмен қазіргі таңда «математикалық экономика» термині де көптеп қолданысқа кіре бастады. Бұндағы негізгі мақсат - экономикалық объектілер мен процестерді және құбылыстарды математикалық тұғырдан сипаттай (формалдай) отырып, оны тиянақты зерттеуге болатынын көрсету. Бұл жерде, яғни экономика саласына қолданылатын математикалық әдістер мен тәсілдер әрдайым нетривиальды болып, математикалық модель құру арқылы жүзеге асатынын да айта кету керек.

Осы жерде Н.И. Лобачевскийдің «Математика - ғылым тілі» - деп бағалағанын да айта кеткеніміз абзал. Бұл тілде өз ойын нақты білдіру дұрыс, алайда ол жеткіліксіз. Сондықтан осы «тілді» математиканың өзінде де, басқа ғылымдарда да еркін жұмыс істейтін алатын модельдер (моделирование) құру үшін қолдана білу керек.

Осы айтылған ойларды түсінікті түрде сипаттау үшін бірнеше мысалдар келтірейік.

1- ші мысал. Қарапайым есеп.

Кәсіркер A өте мұқтаж болып тұрғандықтан өзінің екі жолдасына келіп, біреуінен q_b, ал екіншісінен q_c мөлшерде қарыз алады.

Кәсіркер A өзінің қиналып тұрғанда жомарттық жасап, дер кезінде қол ұшын берген екі жолдасына ризашылығын білдіру үшін белгіленген уақытта сол қарызды едәуір мол етіп N мөлшерде ($N > q_b + q_b$) сол екі жолдасына беріп, «өздерің бөлісіп алыңдар» - деп, кетіп қалады Сонда олар осы қаржыны қалай бөліп алу керек?

Әрине осындай қарапайым есепті кез келген математикадан хабары бар адам оңай шеше алады. Есеп жауабы:

$$n_b = q_b \frac{N}{q_b+q_c} \text{ және } n_c = q_c \frac{N}{q_b+q_c}$$

Мұндағы n_b және n_c бірінші және екінші қарыз берген адамдардың қайтарылған

N суммадан алатын үлестері.

Енді осы есептің ешқандай «өзгеріссіз» экономика және бизнес саласына қолданылуын қарастырсақ, онда бұл есеп мүлдем басқаша сипат алып, тіпті басқаша, яғни күтпеген басқа тәсілмен шешілуі мүмкін. Осы айтқанымызды нақты сипаттау үшін келесі мысалды қарастырайық.

2-ші мысал. Бизнес дауы (болған оқиға ізімен)

Осыдан көп ұзамай көрші мемлекеттердің бірінде орын алып, шешімін әрең тапқан бұл оқиғаның мәнісі мынада...

Сол кезде бизнесі өте төмен (былайша айтқанда, қалтасында бір тиыны жоқ) кәсіпкер A өздерінің жағдайы жақсы B және C атты екі кәсіпкер жолдасына келіп, мынадай пайдасы зор бизнес жобаны қолға алайық деп өз ойын айтса, оны сол екі жолдасы бірден қолдап, үшеуі бірігіп, Z_{ABC} атты фирма құрып іске кірісіп кетеді. Кәсіпкер ***B*-да 5 миллион** доллар**,** ал кәсіпкер ***C*-да 7 миллион** доллар қаржы бар екен, олар кәсіпкер A-ға екеуі бірігіп 4 миллион доллар қарыз беріп (кәсіпкер B *1 миллион* доллар берсе*,* кәсіпкер C *3 миллион* доллар беріпті*),* үшеуі Z_{ABC} фирмасының тең дәрежелі учредителі (*негізін қалаушы*, *founder*) болады. Фирма жұмысы өте жақсы болып, жоба аяқталғаннан кейін, олар түскен пайда мен барлық қаржыны үшеуара теңдей бөлісіп, әрқайысы өзалды фирма құрып, жеке тірлік жасай береді. Ал Z_{ABC} фирмасы (есеп шотында бір тиын болмаса да) керек болып қалар деген оймен сол күйінде жабылмай тұра береді.

Бір жылдан кейін кәсіпкер A-ның бизнесі қатты дамып, ал B мен C толық банкротқа ұшырайды. Бұны естіген кәсіпкер A өзіне зор көмек берген екі жолдасына ризашылық сезімін білдіру үшін және жоғарыда айтылған қарызын қайтармақ мақсатпен Z_{ABC} фирмасына **12 миллион** доллар аударады да, жолдастарына: «Бұл қаржы менің қарыздарымды қайтарғанымның және сендерге білдірген ризашылығымның белгісі. Сендерге алуан-алуан рахмет! Мен енді шетел көшіп, жеке кәсіпкерлік жасаймын. Ал Z_{ABC} фирмасын жабасыңдар ма, әлде сақтап қаласыңдар ма – мен бәріне – сендер қалай шешсеңдер де мен соны қолдап, келісім беремін. Тіпті мені учредитель қатарынан шығарып, менің осы фирмадағы үлесімді қалай бөлісіп алсаңдар да мен бәріне келісім беремін. Осыған қоса мен жіберген 12 миллион қаржыны фирма атынан бизнеске саласыңдар ма, әлде өзара бөлісіп алсаңдар да – мен одан ештеме дәметпей, бәріне толық келісім беремін», - деп, қажетті құжаттарды нотариус арқылы растап, жолдастарымен қоштасып, басқа елге көшіп кетіпті.

Осыдан кейін кәсіпкер B: «Бастапқыда менде 5 миллион, ал сенде 7 миллион қаржы болды да, біз үшеуіміз оны бірдей пайдаланып, теңдей бөлісіп алдық. Демек **маған 5 миллион, ал саған 7 миллион тиесілі.** Ендеше кәсіпкер A жіберген барлық қаржыны осылай бөлісіп, Z_{ABC} фирманы жабуға болады», - десе, кәсіпкер C оған көнбей: «Олай дұрыс емес, себебі фирма пайдасын біз үшеуіміз теңдей пайдаландық. Бірақ сен кәсіпкер A-ға 1 миллион, ал мен 3 миллион бердім. Қорыта айтқанда, мен сенен үш есе есе көп бердім. Ендеше, менің үлесім де үш есе көп болу керек. Демек **саған 3 миллион, ал маған 9 миллион** тиесілі болу керек. Ал осы қаржыны бөлісіп алғаннан кейін фирманы жабуға қарсы емеспін», - десе, оған кәсіпкер B келісім бермей, қаржы бөлісудің арты дауға ұлғасыпты. Сол екеуінің осы дауынан хабардар бір жолдасы оларға көмектесу мақсатымен: «Кәсіпкер C, сенің қаржыны үш есе көп бердім дегенің дұрыс емес. Шын мәнінде сен A-ға екі миллион долларды ғана артығымен бердің, демек сенің үлесің екі миллионға артық болу керек. Сондықтан кәсіркер B-ның **бес және жеті миллионнан** бөлісу керек дегені дұрыс сияқты. Дегенмен осы бөлісті басқаша есептеп көрейік. Мына он екі миллионнан 1 миллионды кәсіркер B алсын, 3 миллионды кәсіпкер C алсын, бұны кәсіпкер A-ның қайтарған қарызы деп есептейік. Ал қалған *сегіз миллионды* кәсіпкер C-ға екі миллион долларды артық етіп бөлсек, онда B-ға *үш* миллион, ал C-ға *бес* миллион тиесілі болу керек. Егер осыған алғашқы *қарыз ретінде берілген* бір және үш миллионды қоссақ, онда сендер **төрт және сегіз миллионнан** бөлісіп алуларың керек», - десе, оған осының бәрін тыңдап отырған тағы бір жолдасы: «Кәсіпкер B кәсіпкер A-ға бір миллион берсе, кәсіпкер C үш миллион, яғни үш есе көп берді. Сондықтан кәсіпкер C-ның үлесі де үш есе көп болу керек. Осы себепті жаңағы айтылған сегіз миллионды *екі және алты* миллионнан, яғни үш есе көп етіп бөлу керек. Енді осыған жоғарыда айтқандай алғашқыдағы *қарыз ретінде берілген* бір және үш миллионды қоссақ, онда сендер **үш және тоғыз миллионнан** бөлісіп алуларың керек», - десе, кәсіпкер B бұған көнбей, дау өрши беріпті.

Осылай күтпенген жерден шешуі «қиын» проблема (есеп) пайда болыпты да, осы бір қарапайым проблеманы (есепті) ешкім шеше алмай, амалы таусылған екі кәсіпкер сотқа жүгінеді. Алдымен болған аудандық сот, олар да бұл есепті шеше алмай, амалының жоғынан жоғарыда айтылған есеп жауаптарының біреуін таңдап, не болса да орташа болсын деп «төрт және сегіз миллионнан бөлісіп алу керек» деген шешім шығарады. Бұған кәсіркерлердің екеуі де көнбей, екеуі де сот шешімін азсыныпты. Одан кейін облыстық сот та тура осындай шешім шығарады.

Кәсіпкерлер бұл шешімге де көнбей, дау Жоғарғы сотқа жетеді. Жоғары сот белгілі математик ғалымдарды шақырып, солардың сілтеуімен дұрыс шешім қабылданады. Кәсіпкерлер осы шешімге онша қанағат болмаса да, қарсы болуға ешқандай аргументі болмай, амалсыздан осы шешімге тоқтау жасапты.

Осы мысалдан жай ғана қарапайым математикалық (тіпті арифметикалық) есеп экономика және бизнес саласына қатысты болғанда, қалай күрделеніп кететіні анық көрініп тұр. Егер таза математика тұғырынан қарастырсақ жоғарыда көрсетілген үш шешімнің (***«бес және жеті миллионнан», «төрт және сегіз миллионнан» және «үш және тоғыз миллионнан»*** бөлісу керек) үшеуі де дұрыс сияқты. Бірақ оларды осы көрсетілген мысал үшін қолдануға болмайды. Себебі бизнес және экономикалық процесстер алуан түрлі себеп пен салдарларға байланысты өте күрделі процесс болып табылады. Бұл жерде қолданбалы математиканы пайдалана отырып, яғни осы процесстерді моделдеу арқылы ғана нақты шешімге қол жеткізуге болады.

Егер осы мәселені математиканы қолдана отырып құқықтану саласына сәйкес етіп шешсек, онда осы есеп шешімі мен осы есептің 1-ші мысалда келтірілген нұсқасының (яғни жалаң математикалық есептің) шешімі бір біріне сәйкес келмей, олардың айырмашылығы жер мен көктей болатынына көзіміз жетіп, алынған нәтижеден ерекше бір сезім аламыз. Бұл дайын жауапқа ие болғаннан өте әсерлі болады. Сондықтан оқырман да сондай ерекше сезімге ие болсын деген мақсатпан, аталмыш проблема шешімін оқырманның өзіне қалдыруды жөн санадық.

Енді осы мәселені сот арқылы шешу неге ұзаққа созылды деген сұраққа көніл аударайық. Бұның негізгі себебі заң ғылымы математикадан қол үзіп, шеткері қалған ғылым саласы. Математика заң ғылымына назар аудармай, ал заң ғылымы математикаға ілесе алмай, заң ғылымы осы күнге дейін догмалық деңгейден шыға алмай келе жатқаны баршамызға мәлім. Мысалы, бұрынғы немесе қазіргі таңда қолданыста жүрген кез келген заң тұжырымдары ешқандай дәлеудеусіз ақиқат ретінде қабылданатынына бәріміз куәміз. Оған мыңдаған, тіпті шексіз мысал келтіруге болады. Осы себепті құқықтану саласындағы кел келген заң тұрақты болмай, оған жыл сайын көптеген өзгертулер мен қосымшалар енгізіліп жатады. Осының салдарынан және математикалық тұрақтылықтың жоқтығынан заң ғылымы нақты шешім талап ететін процесс пен құбылысты қарастырған жағдайда дағдарысқа душар болып, дәрменсіздік танытады. Математикасы жоқ ғылымды әрдайым тығырық күтіп тұрады да, олар көп жағдайда осындай кептелістен өте алмай, амалсыздан догмалық дәлелі жоқ шешім қабылдауға мәжбүр болады. Заң ғылымы сондай ғылымдарың бірі десек, қате болмайды...

Осы айтқан заң ғылымының дәрменсіздігі туралы қорытындыны нақты сипаттайтын тағы да бір өмірден алынған мысал келтірейік.

3-ші мысал. Мұрагерлік дауы (болған оқиға ізімен).

XIX ғасырда бір бақуатты жас кәсіпкер емі жоқ нашар ауруға душар болып, өмірден өтер алдында артында қалған айы-күні жетіп отырған екіқабат жас келіншегіне арнап: «Менің артымда қалған дүние мүлікті бірдей үш бөлікке бөліп, егер әйелім қыз туса, онда бір бөлікті қыздың еншісіне, ал қалған екі бөлік әйеліме берілсін. Егер әйелім ұл туса, онда екі бөлік ұлым еншісіне, ал қалған бір бөлік әйеліме берілсін», - деген аманат қалдырып, дүниеден өтіпті. Көп ұзамай әйелі егіз ұл мен қыз туыпты. Енді еншіні қалай бөлу керек?..

Осы есептегі проблемаға назар аударсақ, күнделікті өмірде кездесетін қарапайым жағдай табан астында күрделеніп, күтпеген жауапты талап етіп тұр. Егер әйелі егіз екі ұл, немесе егіз екі қыз туса, сол сияқты екі ұл мен бір қыз туса немесе екі қыз бен бір ұл туса, онда бұл мәселені заң жүзінде қалай шешуге болады?

Осындай бір жағынан қарапайым, ал екіші жағынан күрделі мәселені заң жүзінде шешу үшін математикаға жүгінбесе, ешқандай нәтиже болмайтыны айдан анық. Бұл үшін, әрине, қолданбалы математика мен логика, яғни қарастырып отырған процессті математикалық тұғырдан моделдеу керек. Мысалы, көрсетілген проблеманың егіз туған ұл мен қыз үшін шешімі:

Моделдеу арқасында қарастырып отырған есептің ауызша шешуі. Аманат шарты бойынша үш бөліктің бір бөлігі қызға берілетін болса, анасы одан екі есе көп, яғни екі бөлік алу керек. Ал, ұл бала аманат шарты бойынша анасынан екі есе көп бөлік алу керек. Ендеше ұлдың үлесі төрт бөлік (яғни анасынан екі есе көп) болу керек. Демек, еншіні осылай тарату үшін бастапқы кезде барлық қазынаны 7 бөлікке бөлу керек те, бір бөлікті қызға, екі бөлікті анасына, ал қалған төрт бөлікті ұлға беру керек.

Ал егер анасы бір қыз бен екі ұл туса ше? Онда барлық дүниені он бір бөлікке бөліп, бір бөлікті қызға, екі бөлікті анасына, ал қалған сегіз бөлікті төрт бөліктен ұл балаларға бөліп беру керек...

Міне қолданбалы математика мен логиканы қолданып едік, нақты айтсақ - әрбір жағдайды математикалық тұрғыдан моделдеп едік, мәселе оңай, тіпті ауызша шешіле кетті.

Сөз соңында айтарымыз - оқу орындарында, әсіресе мектепте жалаңаш математиканы мағынасы «бұлыңғыр» жалаңаш сандар мен формулаларды тоқтаусыз оқыта бермей, жоғарыда көрсетілген есептер сияқты өмірден алынған мысал есептерге көп көңіл бөліп, оқушылар назарын қолданбалы математика саласына көбірек бейімдеу абзал. Тағы да айтарымыз – заң факультеттерінде «Қолданбалы математика негіздерін заң процесстеріне пайдалану» атты, тіпті болмағанда, қосымша оқу курсын ашса, бұдан ешқандай зиян болмай, заң ғылымының математикадан алшақтануы тоқтатылып, біраз игілікті істерге қол жеткізуге болар еді...

МОДЕЛИРОВАНИЕ СЕБЕСТОИМОСТИ УСЛУГ В ЖЕЛЕЗНОДОРОЖНОЙ ОТРАСЛИ В ВИДЕ МНОГОМЕРНОГО ИЗМЕРИТЕЛЯ

Абилкаева Ж.Н., Габбасов М.Б.
zhazira.nurlybekovna@gmail.com, gmarson19@gmail.com
Евразийский национальный университет им.Л.Н. Гумилева, г. Нур-Султан, Казахстан

Аннотация. *По своей природе количественные экономические показатели имеют многомерную структуру, которая определяется разложением значений этих показателей по различным признакам. Математический аппарат работы с кубическими структурами был описан в статье «Математические основы моделирования экономических показателей» [1], где были определены основные математические показатели для моделирования экономических показателей, такие как, факторы и измерители, и рассмотрены основные математические операции над данными сущностями. В данной статье будет рассмотрена возможность использования вышеназванного математического аппарата при моделировании себестоимости услуг в железнодорожной отрасли в виде многомерного измерителя.*

Для применения математического аппарата работы с кубическими структурами при расчете себестоимости услуг предприятий в железнодорожной отрасли необходимо учитывать специфику предметной области. На величину себестоимости перевозок влияют многие факторы: объем перевозок, структура по видам перевозок, видам тяги и родам грузов; техническое оснащение, методы эксплуатации, величины качественных показателей использования подвижного состава, направление перевозки - груженное или порожнее, природные, климатические условия и многие другие. Степень влияния этих факторов различна.

Себестоимость продукции предприятий железнодорожной отрасли, определяется величиной эксплуатационных расходов, приходящихся на единицу перевозок или отдельных видов работ и услуг, т.е. себестоимость равна величине всех расходов, которые были расходованы на оказание конкретного вида услуги, приходящаяся на единицу ее объема:

$$C = \frac{Z}{V} \quad (1)$$

где C – себестоимость услуги, Z – расходы, отнесенные на услугу, V – объем услуги.

Себестоимость, расходы и объем услуги являются количественными показателями, т.е. измерителями. Результат оказания услуги, перевозка железнодорожным транспортом, измеряется тонно-километрами и пассажиро-километрами. Себестоимость рассчитывают отдельно по грузовым и пассажирским перевозкам на основе распределения всех эксплуатационных расходов по видам перевозок:

$$C_{\text{гр.}} = \frac{Z_{\text{гр.}}}{V_{\text{ткм}}}, C_{\text{пасс.}} = \frac{Z_{\text{пасс.}}}{V_{\text{пкм}}} \quad (2)$$

Если предприятие оказывает несколько услуг:

$$C_1 = \frac{Z_1}{V_1}, C_2 = \frac{Z_2}{V_2}, \dots, C_n = \frac{Z_n}{V_n} \quad (3)$$

где, $Z = Z_1 + Z_2 + \cdots + Z_n$ – все расходы компании, $Z_1, Z_2, \dots, Z_n$ – расходы, отнесенные на соответственную услугу, n – количество услуг, оказываемых компанией. Отнесение расходов на услуги является сложной экономической задачей.

Различают два вида себестоимости: производственную $\mathrm{C}_{\text{произ}}$ и полную $\mathrm{C}_{\text{полн}}$. К производственной себестоимости относятся затраты, которые связаны с производством услуг. В полной себестоимости учитываются кроме производственных расходов и административные расходы:

$$Z_{\text{полн}} = Z_{\text{произ}} + Z_{\text{адм}} \quad (4)$$

где, $Z_{\text{полн}}$ – полные расходы, $Z_{\text{произ}}$ – производственные расходы, $Z_{\text{адм}}$ – административные расходы.

Производственная себестоимость состоит из зависящей и условно-постоянной частей в зависимости от объемов выпускаемой продукции или оказываемых услуг.

$$Z_{\text{произ}} = Z_{var} + Z_{const} \quad (5)$$

где, $Z_{\text{произ}}$ – производственные расходы, Z_{var} – переменные расходы, Z_{const} – постоянные расходы.

$$C = C_{var} + C_{const} \quad (6)$$

где, $C_{var} = \frac{Z_{var}}{V}$ – зависящая часть себестоимости, $\mathrm{C}_{\text{const}} = \frac{\mathrm{Z}_{\text{const}}}{\mathrm{V}}$ – условно-постоянная часть себестоимости.

В длительной перспективе при значительных изменениях объемов производства, производственных мощностей и производственных площадей все без исключения затраты можно отнести к переменным. Однако в практике экономических расчетов наиболее часто оцениваются незначительные, в пределах наличных производственных мощностей и производственных площадей изменения объемов производства. В этом случае при стабильных нормах, ценах, технологии и качественных показателях работы переменные расходы изменяются прямо пропорционально объему производства (стоимость сырья, основных материалов, топлива и энергии на производство и т.д.). Условно-постоянные расходы при этом практически не изменяются (расходы на отопление, освещение, ремонт и амортизацию зданий и сооружений, а также на содержание аппарата управления и т.п.).

Также определяются плановая $\mathrm{C}_{\text{план}}$ и фактическая $\mathrm{C}_{\text{факт}}$ себестоимость услуг. Плановые расчеты составляются на все виды продукции на год с разбивкой по кварталам, отражают максимально допустимый уровень затрат и включают только те затраты, которые при данной технологии, организации и структуре производства являются для предприятия необходимыми. В основе плановых калькуляций лежат стабильные нормы затрат ресурсов в натуральном выражении, установленные на данный плановый период времени (год, квартал), а также прогнозные цены на плановый период либо действующие на момент составления плана цены. Фактическая себестоимость продукции определяется по данным финансовой и статистической отчетностей предприятий об объемах производства по видам продукции и фактических расходах. Данные о фактической себестоимости продукции позволяют оценить фактическую эффективность мероприятий по совершенствованию производства, результаты хозяйственной деятельности предприятия и разработать план мероприятий по дальнейшему совершенствованию деятельности предприятия [2].

Себестоимость железнодорожных перевозок может рассчитываться на нескольких уровнях управления: в отделениях дорог (поездоучастках), в целом по сети железных дорог. В структурных подразделениях отделений дороги определяется себестоимость продукции их работы.

Для расчета себестоимости в конкретных условиях перевозок нельзя пользоваться среднесетевыми данными. При определении себестоимости конкретных перевозок применяются специальные расчетные методы, которые позволяют учесть особенности работы железных дорог в отдельных регионах страны, влияние резервов, структуры грузооборота, дальности перевозок, технического оснащения на отдельных участках и направлениях грузопотоков и вагонопотоков, влияние качественных показателей подвижного состава, уровня цен и норм на отдельные виды ресурсов и другие конкретные условия работы. Средняя себестоимость – усредненная себестоимость по всем грузовым отправкам за рассматриваемый период. Конкретная себестоимость – себестоимость перевозки конкретной грузовой отправки, или перевозки порожных вагонов, или услуги локомотивной тяги. Конкретная себестоимость услуги фиксирует конкретные значения всех факторов по всему маршруту оказания услуги [3].

Классификация себестоимости представлена на следующем рисунке 1:

Рисунок 1 – Классификация себестоимости

Себестоимость является важнейшим обобщающим показателем, характеризующим экономическую сторону деятельности предприятия. Расходы, относимые на себестоимость, классифицируются по статьям и для целей финансового учета по элементам затрат. Группировка затрат по калькуляционным статьям и элементам позволяет облегчить расчет плановой и фактической себестоимости отдельных видов продукции, анализировать причины изменения себестоимости продукции и определять направления ее снижения. В общепринятых подходах для группировки, зависящей от размеров перевозок эксплуатационные расходы выбирают калькуляционные измерители, а их в свою очередь относят к расходам хозяйств или структурных подразделений, то есть измеритель на самом

деле выступает как единица измерения работ, выполняемых участниками перевозочного процесса.

Элемент затрат — признак, различающий использованные в расчете затраты по их экономическому содержанию: «затраты на оплату труда», «отчисления от фонда оплаты труда», «материалы», «топливо», «электроэнергия», «оплата работ и услуг дочерних предприятий», «оплата работ и услуг сторонних организаций», «износ», «прочие расходы».

Технологию оказания услуг железнодорожными предприятиями необходимо рассматривать в качестве основы при создании модели. Любые экономические расчеты будут правильно отражать процесс оказания услуги только в том случае, если они опираются на технологический процесс предоставления услуги. Поэтому при расчете себестоимости необходимо учитывать операции перевозочного процесса.

Специфика и сложность перевозочного процесса, необходимость четкого взаимодействия каждого элемента производственного процесса оказывают влияние на состав и структуру эксплуатационных расходов транспорта и придают величине себестоимости перевозок как комплексному показателю особо важное значение. Каждый из видов себестоимости может быть представлен в виде измерителя, который имеет структуру многомерного куба с измерениями: элементы затрат, операции перевозочного процесса, участники перевозочного процесса. В ячейках куба будут показатели – значения себестоимости для отдельного элемента, как представлено на следующем рисунке 2.

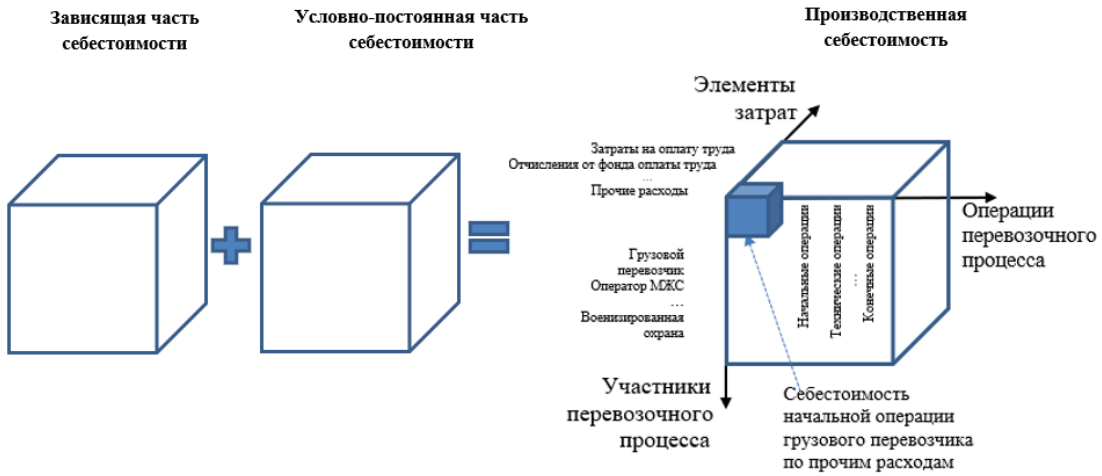


Рисунок 2 – Себестоимость в виде куба

Кроме факторов, показанных на рисунке 2, себестоимость перевозок зависит от факторов, каждый из которых имеет набор значений:

f^1 – «Тип тяги» с набором значений {«электровозная тяга», «тепловозная тяга»};

f^2 – «Вид сообщения» с набором значений {«республиканское сообщение», «экспортное сообщение», «импортное сообщение», «транзитное сообщение»};

f^3 – «Тип вагона» с набором значений {«полувагон», «крытый вагон», «цистерна», «платформа», «рефрежиратор», «прочий вагон», «цементовоз», «зерновоз», «фитинговая платформа», «минераловоз», «транспортер»};

f^4 – «Вид отправки» с набором значений {«повагонная отправка», «маршрутная отправка», «групповая отправка», «мелкая отправка», «контейнерная отправка»};

f^5 – «Категория поезда» с набором значений {«сквозной грузовой поезд», «участковый грузовой поезд», «сборный грузовой поезд», «передаточно-вывозной поезд», «одиночно-следующий локомотив», «ускоренный грузовой поезд»};

f^6 – «Род груза» с набором значений {«уголь каменный», «нефть сырая», «химические и минеральные удобрения», «зерновые грузы, семена», «продукция сельского хозяйства», «руда железная марганцевая», «нефтепродукты», «сырье минеральное, шлаки, цемент», «металлы черные», «металлы цветные», «машины и оборудование», «продукция химической промышленности», «продукция пищевой промышленности», «продукция легкой промышленности», «домашние вещи», «прочие грузы» и др.}.

Методика расчета себестоимости должна учитывать влияние вышеперечисленных и других факторов на себестоимость. При разработке единой методики необходимо данные себестоимости представлять в виде единого измерителя с учетом совместимости факторов. Согласно [1], если измеритель зависит от нескольких факторов $f^i = \{f_1^i, f_2^i, \dots, f_{n_i}^i\}, i = 1,2, \dots, k$, то эта зависимость определяется в виде $I[f^1 * f^2 * \dots * f^k]$, в нашем случае:

$$C[f^1 * f^2 * \dots * f^k]$$

где, С – себестоимость, $f^1, f^2, \dots, f^k$ – факторы, от которых зависит себестоимость, k – количество факторов.

Обозначение $C[f^1 * f^2 * \dots * f^k]$ говорит о том, что у измерителя *C* есть список дочерних показателей, порожденных значениями фактора $f^1 * f^2 * \dots * f^k$, но фактор $f^1 * f^2 * \dots * f^k$, как мы отметили выше имеет кубическую структуру, поэтому показателей измерителя тоже можно отображать в виде куба, каждой ячейке которой соответствует некоторый показатель. Для того, чтобы подчеркнуть, что мы рассматриваем показателей измерителя как ячейки некоторого куба измеритель $C[f^1 * f^2 * \dots * f^k]$ обозначается как $\mathrm{C}[f^1, f^2, \dots, f^k]$, при этом количество аргументов в квадратных скобках показывает количество измерений куба. В данном случае обозначение $\mathrm{C}[f^1, f^2, \dots, f^k]$ означает, что мы рассматриваем измеритель, как *k*-мерный куб.

Количество показателей измерителя $\mathrm{C}[f^1 * f^2 * \dots * f^k]$ равно $\prod_{j=1}^{k}(n_j + 1) - 1$, где n_j – количество значений j-го фактора, если указанные факторы независимы.

При добавлении всех вышеуказанных факторов в себестоимость получим многомерный куб, при этом количество всевозможных показателей себестоимости $\mathrm{C}[f^1 * f^2 * \dots * f^6]$ при независимости факторов равно 181440. Для расчета ячеек такого куба стандартное математическое моделирование не может быть применено.

Резервы снижения издержек производства и себестоимости продукции определяются на основе анализа эксплуатационных показателей и оценки влияния различных факторов на эти показатели. При составлении информационной модели такой оценки влияния факторов особенно удобной является моделирование экономических показателей в виде многомерных измерителей [3].

Моделирование деятельности предприятий, их экономических показателей требует одновременного учета различных показателей. Построение модели затрудняется с отсутствием статистических данных и взаимосвязью разнородных

измерителей. Степень влияния измерителей друг на друга может отражаться по-разному. В данной статье себестоимость рассмотрена в качестве измерителя, имеющего многомерную структуру. Данную теория можно развивать в части описания всех измерителей и факторов, влияющих на себестоимость услуг предприятий железнодорожной области, определения степени влияния значений факторов на экономические показатели предприятия. Данная модель может быть применена для расчета себестоимости услуг, анализа расходов и доходов, оценки экономической эффективности предприятий.

Литература

1. *Abilkayeva Zh. N. and Gabbassov M. B.* Mathematical foundations of modeling economic indicators. Journal of Physics: Conference Series, Volume 1988, Simposium Kebangsaan Sains Matematik ke-28 (SKSM28), 28-29 July 2021, Kuantan, Pahang. https://iopscience.iop.org/article/10.1088/1742-6596/1988/1/012026

2. *Смехова Н.Г. и др.* Себестоимость железнодорожных перевозок – М.: Маршрут, 2003. – 494 с.

3. *Великанов С.А., Габбасов М.Б., Ковальков М., Темирболат Н.С., Шпекпаев М.Б.* Автоматизированная информационная система расчета себестоимости грузовых железнодорожных перевозок. Шестая международная научно-практическая конференция «Информационные технологии на железнодорожном транспорте». г. Сочи, 10-14 октября 2001 года.

ОРМАН ЖӘНЕ ДАЛА ӨРТТЕРІНІҢ ДАМУЫН БАҚЫЛАУ ЖҮЙЕСІ

Т.Ж. Мазаков, А.А.Саметова
(Қазақстан Республикасының Білім және Ғылым Министрлігі Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан,
Әл–Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
tmazakov@mail.ru, sametova_aygerim@mail.ru)

Аңдатпа*. Төтенше жағдайлардың алдын алу және оларды жою проблемасы өзекті болып қала береді. Жер сілкінісі мен су тасқыны, сел, дауыл, орман өрттері, сонымен қатар техногендік саладағы төтенше жағдайлар - радиациялық және көліктік аварилар, химиялық және биологиялық қауіпті заттардың, жарылыстардың, өрттің шығуына байланысты апаттар табиғи саладағы ең үлкен қауіпті құрайды. Орман өрттерін жоспарлау мен ресурстарды жақсарту арқылы қауіпсіздікі қамтамасыз етіп қана қоймай бюджеттің едәуір үнемделуіне әкелуі мүмкін. Қазіргі уақытта орман өрттерін бақылау әдістері жеткілікті тиімді емес. Мұны шешу үшін біз нақты уақыт режимінде орман өрттерін бақылау және модельдеу жүйесін жасаудамыз. Бұл жүйе өрттің таралуын болжау процесіне, қоршаған ортаға келтірілген залалдың төмендеуіне, қауіпсіздіктің жоғарылауына әкеледі.*

Түйін сөздер: *өрт, дала өрттері, орман өрттері, орман өрттерін бақылау, дала өрттерін бақылау, бақылау.*

Кіріспе. Төтенше жағдайлардың алдын алу және оларды жою проблемасы өзекті болып табылады. Жер сілкінісі мен су тасқыны, орман өрттері, сонымен қатар техногендік саладағы төтенше жағдайлар – радиациялық және көліктік аварилар, химиялық және биологиялық қауіпті заттардың, жарылыстардың, өрттің шығуына байланысты апаттар табиғи саладағы ең үлкен қауіпті құрайды.

Орман және дала өрттері – ормандардың қызметі мен күйін айтарлықтай өзгертетін күшті табиғи фактор. Олар қоршаған ортаға орасан зиян келтіреді. Өрт сөндірудің тиімсіз шаралары өрттің кең аймаққа таралуына ықпал етеді және олар адам өмірі үшін өте қауіпті. Сондықтан да бірыңғай ақпараттық кеңістікте жұмыс жасайтын және дала өрттерінің туындауын болжау мен бақылайтын жүйе құру қажет.

Қазақстан Республикасы Президентінің 2003 жылғы 3 желтоқсандағы N1241 Жарлығымен бекітілген «2004-2015 жылдарға арналған Қазақстан Республикасының экологиялық қауіпсіздігі тұжырымдамасында экологиялық қауіпсіздіктің негізгі міндеті ретінде «табиғи және техногендік сипаттағы төтенше жағдайлардың алдын алу» көрсетілген.

Соңғы жылдары орман өрттері қоршаған ортаға да, экономикаға да үлкен зиян келтірді, сондықтан дала өртін табиғи қауіп деп атады. Орман өрттері табиғи циклдің бөлігі болып табылады және үнемі болады. Белгіленген орман өрттері экожүйеде өрттің табиғи рөлін сақтап қалудың негізі болып табылады. Олар фауна мен флора үшін жаңа тауашаларды құруға және топырақты тыңайтуға көмектеседі. [1]

Әдістер. Қойылған міндеттерді шешкенде мыналар қолданылады: автоматты басқару теориясы, интервалды талдау әдістері, үлгіні тану теориясы, деректерді статистикалық өңдеу әдістері, иерархиялық талдау әдісі, бақылау теориясы. Зерттеу объектісі - қоршаған ортаны бақылау жүйелері. Бұл жұмыстың тақырыбы - су тасқыны, орман мен дала өртінің салдарын бағалаудың математикалық модельдері. Зерттеу құралы - математикалық модельдер мен теориялар: математикалық бақылау теориясы, шешімдер теориясы, мәліметтерді өңдеу әдістері, интервалды талдау, ДҚБЖ, ақпараттық жүйелердің қазіргі заманғы жобалау мен әзірлеу жүйелері.

Нәтижелер. Өрт мониторингі мен модельдеу жүйесін үш негізгі кіші жүйеге бөлуге болады. Бұл кіші жүйелерді мәліметтерді жинау жүйесі, басқару орталығының жүйесі және жауап беру жүйесі ретінде анықтауға болады.

Экологиялық мониторингті қамтамасыз ету үшін математикалық модельдеуге негізделген автоматтандырылған ақпараттық жүйелер енгізілуде. Келесі орыс ғалымдарының еңбектері [2-6], оның ішінде диссертациялар [7-9] су тасқыны мен орман өртінің салдарын бағалау мәселелерін зерттеуге арналған.

Электрониканың жедел дамуы деректерді Интернет немесе спутниктік байланыс арқылы жіберуге қабілетті әр түрлі датчиктерді жасауға және нақты уақытта микропроцессорлық технологияға негізделген кіретін мәліметтерді өңдеуге мүмкіндік берді [10].

Деректерді жинау жүйесінде кең ауқымды GPS қабылдағышы мен термиялық бейнекамера бар. Деректер термиялық кескіндерді геореференциялау үшін қолданылады. Инфрақызыл сәуле түрінде шығарылатын жылуды өлшейтін термиялық бейнекамераны қолдану адамның көзімен анықталмайтын орман өрттерін ерте анықтауға және локализациялауға мүмкіндік береді. Сондай -ақ, камера тұманға, түтінге немесе қараңғылыққа байланысты төмен көрінетін жағдайларда өрттің дәл суреттерін береді. Бұл деректерді веб-сайтқа нақты уақыт режимінде жүктеуге арналған нақты уақыттағы деректерді жинау жүйесі өрт сөндірушілерге ресурстарды қайда бөлу керектігін тиімді анықтауға және қай жерде жасырынып жатқан өртті тез табуға көмектесу үшін жеткілікті. Бұл жүйемен алынған дәлдік өрттің орналасқан жері, көлемі мен бағыты туралы нақты есептерді алуға мүмкіндік береді.

Басқару орталығының жүйесі веб -бетті орналастырады. Оның жауапкершілігі көп. Үш негізгі міндеттің біріншісі - мәліметтерді жинау жүйесімен алынған барлық ақпаратты өңдеу. Екінші міндет - өрт мінез -құлқының функцияларын орындау. Соңғы үлкен жауапкершілік - өрт жағдайы туралы ақпаратты көрсету.

Соңғы кіші жүйе - жауап беру жүйесі басқару орталығы жүйесінің нәтижелерін пайдаланушыға көрсетуге мүмкіндік береді. Бұл жүйе пайдаланушыға басқару орталығы жүйесінен алынған нәтижелерді қарауға мүмкіндік береді.

Талқылау. Өрттердің табиғаты бойынша орман экожүйесінде күтпеген өзгерістер болды. Олар өртке бейім аймақтағы табиғи циклды өзгертуге қабілетті, бұл салдардың шиеленісуіне әкеледі. Осылайша, отты парадокс ретінде қарастыруға болады. Ол өсімдіктер мен жануарларды жойып, қоршаған ортаға айтарлықтай зиян келтіреді, бірақ сонымен бірге ормандарды молықтыру мен қоректік заттарды қайта пайдалану көзі болып табылады. Жануға сұйық химия, физика және механика кіреді. Өрт жабайы жерлерден отын жағғанда, процесте көптеген факторлар әсер етеді, оның ішінде турбуленттілік пен біркелкілік жоқ.

Орман және дала өрттері – ормандардың қызметі мен күйін айтарлықтай өзгертетін күшті табиғи фактор. Олар қоршаған ортаға орасан зиян келтіреді.

Өрт сөндірудің тиімсіз шаралары өрттің кең аймаққа таралуына ықпал етеді және олар адам өмірі үшін өте қауіпті. Сондықтан да бірыңғай ақпараттық кеңістікте жұмыс жасайтын және дала өрттерінің туындауын болжау мен бақылайтын жүйе құру қажет. Өрт және экологиялық қауіпсіздікті бақылау жүйесін жасау үшін түсіну керек:

- өрт және экологиялық қауіптердің пайда болуы мен дамуын анықтайтын факторлар;
- өрт қаупін азайту бойынша іс-шараларды әзірлеу және орындау;
- өрт қаупін, материалдық және қоршаған ортаға келтіретін зиянды азайту үшін нақты бағдарлама бойынша жүргізілетін алдын-алу шараларының тиімділігі.

Осыншама зардап келтіретін өрттің пайда болуының негізгі себептері әртүрлі. Көбінесе табиғи себептерден туындайды:

- Найзағай
- Адами факторлар
- Әдейі от қою

Көптеген жағдайларда ағаштар найзағай соққыларынан құрғақ найзағай деп аталатындықтан өртенді.

Екінші орында адам факторы: отты абайсыз қолдану нәтижесінде. Ауылшаруашылық борандардың (жайылымдарды тазарту үшін құрғақ шөптерді жағу) және ағаш жинаушылардың кінәсінен. Өрттің қалған бөлігі түсініксіз себептерге байланысты орын алады.

Өткен жылмен салыстырғанда орман өрттерінің саны 2019 жылдың басынан бастап 1,8 есе өсті (277 жағдайдан 499-ға дейін), ал орман өрттерінің аумағы 1,8 есе азайды (117 266,5 га-дан 65,437 га дейін).

Осыны ескере отырып, мониторинг жүйесінің негізгі міндеттері мыналар болуы керек:

- өрттің жағдайы туралы ақпарат жинау;
- ақпаратты өңдеу және талдау, өрт жағдайын бағалау;
- нақты фактілік және болжамдық мәліметтер негізінде өрт жағдайларын болжау;
- өрттегі жағдай индикаторларының өзгеру бағыттары мен бағыттарын анықтау (жағдайды дамыту сценарийлерін әзірлеу);

Қорытынды. Орман өрттері - бұл өте күрделі жүйе, онда метеорологиялық және өсімдік жағдайлары әсер ететін айнымалылардың бір бөлігі ғана. Жану, өрттің таралуы және өрттің таралуы көптеген айнымалылармен байланысты. Сондықтан, орман өрті тек табиғи себептерге тәуелді болмайынша, осындай қызметтің нәтижелерін күту орынды.

Орман мен дала өрттерінің болуын бақылау мен болжау жүйелері қолда бар құралдардың бірі ретінде қарастырылуы тиіс. Дегенмен, орман өрттерімен жұмыс істейтін адамдардың тәжірибесі тәуекелдерді талдаудың негізгі құралы болып қала береді. Олар ең қауіпті аймақтар, өрттің жел мен беткейлерге байланысты мінез-құлқы және өртті қалай сөндіру үшін қоршау керектігін біледі. Осы себепті алдын - алу режимін ескерусіз қалдырмай жыл сайын жетілдіру маңызды.

Практикалық маңызы аумақтық немесе республикалық деңгейде шешім қабылдаудың дұрыстығына ықпал ететін ағымдағы және болжамдық ақпаратты беретін жүйені дамытуда жатыр. Өрт қауіпсіздігі мониторингі жүйесіне

экологиялық қауіпсіздік жүйесін енгізген жөн. Өрт және экологиялық қауіпсіздік жағдайының мониторинг жүйесіне келесі кіші жүйелер кіреді: ақпаратты басқару, өңдеу және сақтау; ақпаратты талдау және бағалау; болжау. Ұсынылған мониторинг жүйесі жоғарыда аталған міндеттердің барлығын шешуді қамтамасыз етеді.

Орман өрттерін жоспарлау мен ресурстарды жақсарту арқылы қауіпсіздікі қамтамасыз етіп қана қоймай, қаржының едәуір үнемделуіне әкелуі мүмкін. Қазіргі уақытта орман өрттерін бақылау әдістері жеткілікті тиімді емес. Мұны шешу үшін нақты уақыт режимінде орман өрттерін бақылау және модельдеу жүйесі «Developing the concept and mechanisms of balanced territorial development of the economy and society of Kazakhstan» (Қазақстан экономикасы мен қоғамының теңдестірілген аумақтық дамуының тұжырымдамасы мен механизмдерінің дамуы) жобасы бойынша 2021-2022 жылдарға арналған ғылыми зерттеулерді бағдарламалық-мақсатты қаржыландыру есебінен жүргізілді.

Бұл жүйе өрттің таралуын болжау процесіне, қоршаған ортаға келтірілген залалдың төмендеуіне, қауіпсіздіктің жоғарылауына әкеледі.

Әдебиеттер

1. Саметова А.А., Салимханова А.С. Системы мониторинга развития лесных и степных пожаров в режиме реального времени //Новината за напреднали наука – 2020, София, 2020, №4

2. Ольховик О.В., Петрикин А.А., Богуславский И.В. Концепция разработки системы поддержки принятия решений в условиях чрезвычайной ситуации //Вестник ДГТУ. – 2010, том 10. – № 3(46). – С.350-354.

3. Мелехов И.С. Лесные пожары и борьба с ними. – Книга по Требованию. – 2012

4. Шаптала В.Г., Радоуцкий В.Ю., Шаптала В.В. Основы моделирования чрезвычайных ситуаций. – Белгород: Изд-во БГТУ, 2010. –166 с.

5. Гришин А.М. О математическом моделировании природных пожаров и катастроф //Вестник ТГУ. – 2008. – С. 105-114.

6. Гельфан А.Н. Динамико-стохастическое моделирование формирования талого стока. – М.: Наука, 2007. – 279 с.

7. Сердюцкая Л.Ф. Системный анализ и математическое моделирование экологических процессов в водных экосистемах. – М.: Книжный Дом «Либроком», 2009. – 144 с.

8. Перминов В.А. Математическое моделирование возникновения верховых и массовых лесных пожаров //Автореферат доктор.физ.-мат.наук, Томск, 2010.

9. Гугушвили И.В. Совершенствование методов расчета параметров движения волны прорыва по речной долине //Автореферат канд.техн.наук, Москва, 2011.

10. Шарапов В.М. и др. Датчики. - М.: Техносфера, 2012. -624 с.

11. Щербов Б.Л. Лесные пожары и их последствия. – Академическое издательство. – 2015

12. Доррер Г.А. Динамика лесных пожаров. – Новосибирск: СО РАН, 2008. – 404 с.

13. Саметова А. А., Мазаков Т. Ж., Салимханова А.С. Мониторинг развития лесных и степных пожаров // Вестник КазНИТУ, 2020. – №3. – С.175-179.

14. Голованов А.Н., Якимов А.С., Абрамовских А.А., Суков Я.Р. О математическом моделировании процессов зажигания и тления торфа //Теплофизика и аэромеханика. – 2008, том 15. – № 4. – С.699-710.

15. Колодкин В.М. Прогнозирование последствий аварий и рисков. – Ижевск: УдГУ, 2008. – 123 с.

RESEARCH PROPOSAL: SENTIMENT ANALYSIS OF FINANCIAL NEWS

Sagdat Okimbek, Razak Nurlan, Bulgyn Dyussenkulova, Shynarbekova Tolkyn, Daniyarbekov Sanzhar, Bashkeyeva Symbat, Akhmetov Iskander
s_okimbek@kbtu.kz, n_razak@kbtu.kz, bu_dyusenkulova@kbtu.kz, to_shynarbekova@kbtu.kz, s_daniyarbekov@kbtu.kz, sy_bashkeyeva@kbtu.kz, iskander.akhmetov@gmail.com,
Kazakh-British Technical University, Kazakhstan
Institute of Information and Computational Technologies
CS MES RK, Kazakhstan

Abstract

According to the Tuney's novel with unsupervised method for classification of reviews based on sentiment indicators, semantix measures are obtained parts of POS sentence.The summary text is classified by usage of average Semantic Orientation of the phrases. Schumaker and Chen had applied the textual models, which were bag of words(BOW), noun phrases and named entities.In order to minimize the size of features, feature selection strategies are used in the model of Kaya and Karsligil.Rani et al. presented a semi-supervised method for POS tagging that establishes a classifier model from a combination of POS tagged corpus and untagged text data.

I. INTRODUCTION

Nowadays, stream of fake news is getting widespread among the world. It is aimed at clickbait, propaganda, satire/parody, sloppy journalism and so on. Our research will be conducted in sentaimental analysis of fake news. Sentiment analysis studies information, such as expression, emotions, opinions, attitudes. Sentiment analysis for fake news detection will have significance in terms of avoidance of fake news based on emotions and news.

II. SYSTEM DESCRIPTION

The system which makes humans life more secure and trustworthy from simple 3 global functionality except many different technical methods and modules. Analyzing the system functionalities, below given those parts of the system. The steps:

• Text/Speech to Text The human recognizing step works with the MFCC(Mel Frequency Ceptral Coefficients) which is the most popular feature for speech recognition. MFCC (Mel Frequency Ceptral Coefficients) feature vectors are calculated for each frame of detected human speech. The detail work is illustrated in figure 2 with the seven level layers.

• Speech Acquisition This is language learning process after recognizing the human voice. It is very important part which influence on correctness of work.

• Text/Speech Analysis After second part the system read the architecture of the text than system trying to understand the meaning of the sentences. The goal of the part to find and analyze the date and author of the article, source of the news, the content jargon words and repeatable words.

III. LITERATURE REVIEW

A sentence is a outright thought in written, consisting of a subject and a predicate. The subject is “a person, thing or place that is performing some operation”, whereas the predicate describes this action. The most understandable form of the predicate is just a verb, e.g., in the sentence “I breathe.”. A more complex predicate can include an object, i.e., “a noun or pronoun that can be affected by the action of a subject”.The Subject-Verb-Object (SVO) rule is followed in simple sentences in English, where the verb shows the relationship between the subject and the object.SDS and PoS tags are used xLSA in order to identify the Subject, Verb and Object in a sentence along with their asymmetric relationships. This information is used to calculate the similarity of two sentences, by matching the SVO structure. Dependency is a formalism that introduces relations between words as directed connections. Verbs are considered structural centres of clauses and other structural units link with verbs by directed links. Dependency structure gives information about grammatical functions of words in relation to other words in the sentence. The English language has four types of sentences:• Simple sentences • Compound sentences • Complex sentences • Compound-complex sentences Turney [1] proposed a novel unsupervised method for classification of reviews based on sentiment indicators in a seminal 2002 paper. Sentiment measures are derived parts of speech (POS) sentences, which are normally a mixture of adjectives. The semantic orientation (SO) of all extracted phrases in a text is determined as the PMI-IR (Point wise Mutual InformationInformation Retrieval) between the phrase in question and the word ”excellent” minus the PMI-IR between the phrase in question and the word ”bad.” The summary text is then categorized using the average SO of the phrases. Pui et al. [2] proposed a method for mining multiple time series at the same time while relying on textual material as the primary source of prediction. The textual models used by Schumaker and Chen [3] were bag of words, noun phrases, and named entities. This study looked at whether individual stock prices could be predicted with a twenty-minute delay after an article was published. Cheng [4] used rough sets theories to translate unstructured data into structured data and then extract key phrases. Instead of using a single phrase, Kaya and Karsligil [5] proposed a model in which a noun and a verb are taken as a word pair. To minimize the size of features, feature selection strategies are used. Deng et al. [6] developed a stock market prediction model based on SentiwordNet (SWN) that generates scores for sentiment indicators and then calculates overall news sentiment. Hagenau et al. [7] used highly expressive features to represent text, as well as exogenous consumer input for word selection. Instead of using just the BOW (Bag of Words) method, various types of features were used to label the news stories, including noun-verb combinations, 2-gram, and 2-word combinations, as well as business feedback. Siering [8] used a lexicon-based method to train a machine learning classifier. The findings were classified into two categories: domain based and domain independent. Rout et al. [9] compared the two methods for detecting emotion in tweets and found that the proposed method was more reliable than the lexicon-based method. Zheng et al. [10] used N-char-grams and N-POS-grams to analyze sentiment in Chinese online reviews and discovered that 4-POS-grams provide the best results. Naik et al. [11] used publicly accessible movie analysis and university selection datasets to extract tri-co-occurrences of emotion terms and assess the semantic orientation of phrases. Rani et al. [12] proposed a semi-supervised approach for POS tagging that builds a classifier model from a combination of POS tagged corpus and untagged text data using association rules. Analysis of the style of the text, not the content. The essence of the method is that falsifiers, wanting to mislead the reader, use certain techniques to impose the desired idea and not be caught in a lie. This is manifested in certain stylistic features that are not always noticeable to a person: a certain frequency and pattern of the use of negatives, pronouns and conjunctions,

as well as the level of vocabulary and the complexity of the text, can serve as indicators of falsification. Distribution analysis. The method is based on the use of special models that resemble models of infectious disease epidemics and allow predicting how disinformation will spread. Analysis of user activity. The method is to assess the participation of readers in the creation and dissemination of fake news. Users are divided into two classes: ”attackers” who benefit from the creation and distribution of fakes, and ordinary users who distribute fakes without specific intent, usually at the same time as the attackers.

IV. METHODOLOGY

This section shows the algorithms and models that our team used to build the system. Separately, it is worth highlighting the components of data preparation and model training. Fortunately, in order to quickly start with NLP, there is a ready-made solution - the NLTK and TextBlob libraries. The second is a wrapper over NLTK, which does the routine work - makes feature extraction from the training set, and then trains the model at the first classification request. Data preparation is needed before training the model. So, can be distinguished three functions, which are essential at the stage of data loading:

• Connecting to a data source - for CSV or JSON, in our case it is implemented inside the read_csv or read_json function;

• Data loading using load_data method;

• Support for format features;

• Preliminary preparation of data Before training the data, it is needed to opt for the model. It can help to find the best result. Therefore, will be used following algorithms and models: • Support vector machine. This algorithm allows to significantly reduce the need for labeled training copies for various types of training. Classifiers of this type demonstrate high efficiency on new data, reaching an accuracy of more than 90 • Naive Bayesian Model.This model is popular as a simple tool for creating probabilistic classifiers of fake news, demonstrating sufficient efficiency in complex realistic conditions. All methods can demonstrate excellent results, but the best efficiency in most cases (both when recognizing fake news and in other classification problems) is shown by logistic regression, Bayesian models and deep learning, which has shown itself well on different datasets and when working with different schemes. processing. Convolutional networks are more likely to perform better on heterogeneous datasets, while HANs are more likely to perform well on large datasets. Typically, CNN can achieve accuracy over 90%, and this indicator can be improved by using schemes that compensate for the lack of remembering previous events. One such pattern is ”long short term memory.” This is a kind of recurrent neural networks with loops and blocks that allow you to memorize values for a certain period of time, which allows you to trace the relationship between the words that begin and end the analyzed text.

V. OUTLINE FOR THE EXPERIMENT

While training our model, the accuracy of the training was equal to: 65,77. And it was not best result for our experiment. The causes are lack of data for compare and not good hyperparameters to train our model. It is being planned to supplement dataset and see the loss and accuracy of the out model. If the result is not changeable, it is mean, we should change our model. So, the available corpuses of already marked up fake and real news increase the accuracy of the classifiers regardless of the machine learning method used. Publicly available datasets of this kind include: Kaggle - a database of fake news containing several thousand entries. LIAR is a set of test data containing about 13 0000

verified statements by various speakers on various topics. BuzzFeed - an updated list of sites that publish fabricated information.

VI. CONCLUSION

In conclusion, in our research we were able to sparce data from sites with news. In models and methods, written in Methodology section, could not get exact results.But in further research, models will be improved, otherwise, will be selected the another appropriate models in order to get results whether news are fake or not.

References

1. Turney P. D. Thumbs up or thumbs down? Semantic orientation applied to unsupervised classification of reviews //arXiv preprint cs/0212032. – 2002.
2. Fung G. P. C., Yu J. X., Lam W. News sensitive stock trend prediction //Pacific-Asia C onference on Knowledge Discovery and Data Mining. – Springer, Berlin, Heidelberg, 2002. – pp. 481-493.
3. Schumaker R. P., Chen H. Textual analysis of stock market prediction using breaking fi nancial news: The AZFin text system //ACM Transactions on Information Systems (TOIS). – 200 9. – T. 27. – №. 2. – pp. 1-19.
4. Cheng S. H. Forecasting the change of intraday stock price by using text mining news o f stock //2010 International Conference on Machine Learning and Cybernetics. – IEEE, 2010. – T . 5. – pp. 2605-2609.
5. Conroy N. K., Rubin V. L., Chen Y. Automatic deception detection: Methods for findin g fake news //Proceedings of the association for information science and technology. – 2015. – T. 52. – №. 1. – pp. 1-4.
6. Kaya M. I. Y., Karsligil M. E. Stock price prediction using financial news articles //201 0 2nd IEEE International Conference on Information and Financial Engineering. – IEEE, 2010. – pp. 478-482.
7. Li Q. et al. The effect of news and public mood on stock movements //Information Scie nces. – 2014. – T. 278. – pp. 826-840.
8. Lin I. H. Creating and verifying sentiment dictionary of finance and economics via finan cial news //Unpublished masterLs thesis). Accounting, National Taiwan University. Taipei, Taiw an (ROC). – 2013.
9. Buntain C., Golbeck J. Automatically identifying fake news in popular twitter threads // 2017 IEEE International Conference on Smart Cloud (SmartCloud). – IEEE, 2017. – pp. 208-215.
10. Sullivan D. Document warehousing and text mining: techniques for improving business operations, marketing, and sales. – John Wiley & Sons, Inc., 2001.
11. Dong Z., Dong Q. Hownet and the computation of meaning (with Cd-rom). – World Sci entific, 2006.
12. Zheng L., Wang H., Gao S. Sentimental feature selection for sentiment analysis of Chin ese online reviews //International journal of machine learning and cybernetics. – 2018. – T. 9. – № . 1. – pp. 75-84.
13. Naik M. V., Vasumathi D., Kumar A. P. S. An enhanced unsupervised learning approac h for sentiment analysis using extraction of tri-co-occurrence words phrases //Proceedings of the S econd International Conference on Computational Intelligence and Informatics. – Springer, Singa pore, 2018. – pp. 17-26.
14. Rani P., Pudi V., Sharma D. M. A semi-supervised associative classification method for POS tagging //International Journal of Data Science and Analytics. – 2016. – T. 1. – №. 2. – pp. 1 23-136.

VARIATIVE SOLUTION OF THE COEFFICIENT INVERSE PROBLEM FOR THE HEAT EQUATIONS IN A QUADRANGULAR PLANE

L. Yermekkyzy, Zh. Madibaiuly
e-mail:yermekkyzylaura@gmail.com
Al-farabi Kazakh National University, Almaty, Kazakhstan

Abstract

One of the main types of inverse problems for partial differential equations are problems in which the coefficients of the equations or the quantities included in them must be determined using some additional information. Such problems are called coefficient inverse problems for partial differential equations. Coefficient inverse problems (identification problems) have become the subject of close study, especially in recent years. Interest in them is caused primarily by their important applied values. They find applications in solving problems of planning the development of oil fields (determining the filtration parameters of fields), in creating new types of measuring equipment, in solving problems of environmental monitoring, etc. The standard formulation of the coefficient inverse problem contains a functional (discrepancy), physics. When formulating the statements of inverse problems, the statements of direct problems are assumed to be known. The solution to the problem is sought from the condition of its minimum. Inverse problems for partial differential equations can be posed in variational form, i.e., as optimal control problems for the corresponding systems. A variational statement of one coefficient inverse problem for a one-dimensional heat equation is considered. By the solution of the boundary value problem for each fixed control coefficient we mean a generalized solution from the Sobolev space. The questions of correctness of the considered coefficient inverse problem in the variational setting are investigated.

Key words: coefficient inverse problem, variational statement

1. Statement of the problem. The paper considers a one-dimensional heat conduction equation

$$\frac{\partial}{\partial x}\left(\lambda\frac{\partial u}{\partial x}\right)=\rho c\frac{\partial u}{\partial t}$$

$$c\rho(u)u_t=\left(\lambda(u)u_x\right)_x,\quad (x,t)\in(0,a)\times(0,T) \tag{1}$$

with initial boundary conditions

$$u(x,0)=\varphi(x),\qquad x\in(0,a) \tag{2}$$

$$u(0,t)=g_1(t), \tag{3}$$

$$u(a,t)=g_2(t),\qquad t\in(0,T). \tag{4}$$

Usually, a direct task is understood as finding a solution u problems (1) - (4) for the given functions $c,\rho,\lambda,\varphi,l_1,l_2$.

Let the following conditions be satisfied

$$\begin{cases} c\rho(u) \in C^2[b,c], \\ \lambda(u) \in C^3[b,c], \\ g_1, g_2 \in W_2^1[0,T], \\ u_0 \in W_2^1[0,a], \qquad g_1(0) = \varphi(0),\ g_2(0) = \varphi(a), \end{cases}$$

$[b,c]$ contains domain of values $u(x,t)$ for all sufficiently small variations λ. In this case, the domain of definition of functions $c(u), \lambda(u)$ is fixed, since by virtue of the maximum principle [1]

$$b = \min\left\{\min_{[0,T]} g_1(t), \min_{[0,T]} g_2(t), \min_{[0,a]} \varphi(x),\right\}$$
$$c = \max\left\{\max_{[0,T]} g_1(t), \max_{[0,T]} g_2(t), \max_{[0,a]} \varphi(x),\right\}.$$

Then there is a solution to the problem (1)-(4) $u \in W_2^{2,1}\left((0,a)\times(0,T)\right)$ [1].

However, the coefficients are not always c, λ predetermined. More often, a situation arises when they are subject to determination based on some additional information. Such problems are called coefficient inverse problems for the heat equation.

This article considers the coefficient inverse problem in the following setting: the known $c, \rho, \varphi, g_1, g_2$ find a couple of functions (u, λ) so that the additional condition [2]

$$u\left(d(t),t\right) = f(t), \quad t \in (0,T),\ 0 < d(t) < a, \tag{5}$$

where $d(t), f(t)$ some famous features. Let be $x = d(t)$ - piecewise smooth function.

The task of determining (u, λ) (1)-(4) To avoid the indicated difficulty, instead of solving the incorrect problem (1)-(4) we have to involve stable initial-boundary value problems for the same heat equation. Problem (1) - (4) with a given coefficient $\lambda(u)$.

Thus, the operator:

$A: \lambda \to f$,

conjunctive λ with f: $\left(A(\lambda)\right)(t) = f(t)$, $t \in (0,T),\ 0 < d(t) < a$. Investigation of operator properties A and its adjoint operator allows using variational methods to find an approximate solution to the inverse problem (1)-(5).[3]

2. Variational formulation of the problem of finding the coefficient λ.

It is required to minimize the functionality

$$J(\lambda) = \int_0^T \left[u\left(d(t),t,\lambda\right) - f(t)\right]^2 dt. \tag{6}$$

where $u(x,t,\lambda)$ - solution of problem (1) - (4) corresponding to the coefficient $\lambda(u)$. Here T is fixed number.

The specified functional is minimized according to the following algorithm:

1. Choose an arbitrary initial value of the coefficient $\lambda_0 \in C^3[b,c]$.
2. We solve the direct problem (1) - (4) with the coefficient and find its solution $u(x,t;\lambda_0)$
3. We calculate the value of the functional $J(\lambda_0)$ according to the formula (6).

4. its necessary to choose $\lambda_1(\cdot) = \lambda_0(\cdot) + \delta\lambda_0(\cdot)$ so that the inequality $J(\lambda_1) < J(\lambda_0)$.
5. Repeat the cycle until $|J(\lambda_{k+1}) - J(\lambda_k)| < \varepsilon$, where $\varepsilon > 0$ specified accuracy.
6. For selection $\lambda_1(\cdot)$ optimal choice is necessary $\delta\lambda_0(\cdot)$.

3. Rationale for the optimal choice $\delta\lambda_0$

Let be $\delta\lambda_0 \in C^3[b,c]$. We denote $u(x,t;\lambda_0) = u_0,\ u(x,t;\lambda_0 + \delta\lambda_0) = u_1$ solutions of problem (1) - (4) with coefficients $\lambda_0(u), \lambda_0(u) + \delta\lambda_0(u)$ accordingly. Convenient designation $\delta u_0 = u(x,t,\lambda_0 + \delta\lambda_0) - u(x,t,\lambda_0) = u_1 - u_0$. Let us find a problem that satisfies δu_0. For this, we write down problem (1) - (4) with the coefficient $\lambda_0(u) + \delta\lambda_0(u)$, using the introduced designations [4]

$$c\rho(u_0 + \delta u_0)(u_0 + \delta u_0)_t = \left(\left(\lambda_0(u_0 + \delta u_0) + \delta\lambda_0(u_0 + \delta u_0)\right)(u_0 + \delta u_0)_x\right)_x, \quad (7)$$

$$(u_0 + \delta u_0)\big|_{t=0} = \varphi(x), \quad (8)$$

$$(u_0 + \delta u_0)\big|_{x=0} = g_1(t), \quad (9)$$

$$(u_0 + \delta u_0)\big|_{x=b} = g_2(t). \quad (10)$$

By virtue of the maximum principle

$$b \le u_0(x,t) + \delta u_0(x,t) \le c\rho$$

$$\forall\,(x,t) \in (0,a)\times(0,T),$$

and therefore functions

$$\lambda_0 + \delta\lambda_0 \in C^3[b,c],\ \ c(u_0 + \delta u_0) \in C^2[b,c],$$

and these functions are defined for any $(x,t) \in (0,a)\times(0,T)$. The solution of the problem (7)-(10) $u_0 + \delta u_0 \in W_2^{2,1}\left((0,a)\times(0,T)\right)$. As $u_0, u_0 + \delta u_0 \in W_2^{2,1}\left((0,a)\times(0,T)\right)$, then it follows that $\delta u_0 \in W_2^{2,1}\left((0,a)\times(0,T)\right)$.

We use in (7) the following expansions

$$\lambda_0(u_0 + \delta u_0) = \lambda_0(u_0) + \lambda_0'(u_0)\delta u_0 + o(\|\delta u_0\|),$$

$$\delta\lambda_0(u_0 + \delta u_0) = \delta\lambda_0(u_0) + (\delta\lambda_0(u_0))'\delta u_0 + o(\|\delta u_0\|),$$

where $\|\delta u_0\| = \|\delta u_0\|_{W_2^{2,1}((0,a)\times(0,T))}$.

Then for δu_0 it is easy to get the following problem

$$\left(c(u_0)\delta u_0\right)_t = \left(\lambda_0(u_0)\delta u_{0x}\right)_x + \left(\lambda_0'(u_0)\delta u_0 \cdot u_{0x}\right)_x + \left(u_{0x}\delta\lambda_0(u_0)\right)_x + o(\|\delta u_0\|), \quad (11)$$

$$(x,t) \in (0,a)\times(0,T),$$

$$\delta u_0(x,0) = 0, \quad (12)$$

$$\delta u_0(0,t) = \delta u_0(a,t) = 0. \quad (13)$$

Let be $\Phi(x,t)=\left(u_{0x}(x,t)\delta\lambda_0\left(u_0(x,t)\right)\right)_x+o(\|\delta u_0\|)$, then the estimate $\|\delta u_0\|_{W_2^{2,1}((0,a)\times(0,T))}\le M_1\|\Phi\|_{L_2((0,a)\times(0,T))}\le M_2\|\delta\lambda_0\|$,

where $\|\delta\lambda_0\|=\|\delta\lambda_0\|_{C^2[b,c]}$.

Using the equality $\left(\lambda_0(u_0)\delta u_0\right)_{xx}=\left(\lambda_0'(u_0)\delta u_0\cdot u_{0x}\right)_x+\left(\lambda_0(u_0)\delta u_{0x}\right)_x$ and discarding in (11) the quantities of higher order of smallness $o(\|\delta\lambda_0\|)$, we write down the final task for $w\approx\delta u_0$

$$\int_0^T\left(\lambda_0(u_0)w\right)(x,t)\big|_{x=d(t)}\left[\psi_x(x,t)\right]_{(d(t),t)}dt=\int_0^T\int_0^a\left(\delta\lambda_0(u_0)u_{0x}\right)_x\psi dxdt, \qquad (14)$$

where $\left[\psi_x(x,t)\right]_{(d(t),t)}=\psi_x\left(d(t)+0,t\right)-\psi_x\left(d(t)-0,t\right)$ - function jump ψ_x at the point $\left(d(t),t\right)$.

Let be ψ_x satisfies the additional condition

$$\left(\lambda_0(u_0)w\right)(x,t)\big|_{x=d(t)}\left[\psi_x(x,t)\right]_{(d(t),t)}=2\left[u_0\left(d(t),t,\lambda_0\right)-f(t)\right]. \qquad (15)$$

Consider the difference between the functionals, hence, taking into account relations (14), (15), we arrive at the representation

$$\delta J(\lambda_0,\delta\lambda_0)=\int_0^T w\left(d(t),t\right)\cdot 2\left[u_0\left(d(t),t,\lambda_0\right)-f(t)\right]dt=\int_0^T\int_0^a\left(\delta\lambda_0(u_0)u_{0x}\right)_x\psi dxdt.$$

Now choose $\delta\lambda_0$ so that the condition $\delta J(\lambda_0,\delta\lambda_0)<0$, then $J(\lambda_0+\delta\lambda_0)<J(\lambda_0)$.

References

1. Kabanikhin S.I. Inverse and ill-posed problems. Novosibirsk: Siberian Scientific Publishing House,2009, 457

2. Kabanikhin S.I., Koptyug I.V., Iskakov K.T., Sagdeev R.Z. Inverse problem for diffusion transport of water upon single pellet moisture sorbition. International Journal of Nonlinear Sciences and Numerical Simulation Shanghai University v.1, 2000, pp.31-42.

3. Kabanikhin S.I., Koptyug I.V., Iskakov K.T. and Sagdeev R.Z. Inverse problem for a quasilinear equation of diffusion. Journal of Inverse and Ill-Posed Problem (1998) vol. 6(4), The Netherlands, Utrecht, pp. 335-352.

4. Denisov A.M. Introduction to the theory of inverse problems. M .: Publishing house of Moscow State University, 1994, 208 p.

APPLICATION OF THE ENERGY METHOD TO SOLVE THE NONLINEAR PROBLEM OF THERMOELASTICITY OF A ROD OF VARIABLE SECTION.

Kudaykulov A.K., Begaliyeva K.B., Arshidinova M.T.
e-mail: mukaddas_arshidi@mail.ru

Institute of Information and Computing Technologies CS MES RK

Abstract–*A horizontal rod of limited length is considered. Radius of the rod varies linearly along its length. The cross-sectional area of the left end is greater than the right one. The lateral surface of the test rod is completely insulated. The heat flow is fed to the cross-sectional area of the left end. Through the cross-sectional area of the right end of the rod, heat exchange takes place with the surrounding medium. The field of distribution of temperature, displacement, three components of deformation and stresses are determined in the work, provided that both ends of the rod are rigidly fixed. And also, the magnitude of the elongation of the rod is determined when one end of the rod is fixed and when the other is free. In the case of fixing the two ends of the rod, the magnitude of the resulting axial compressive force is also calculated. When studying the rod, the fundamental laws of conservation of energy were used.*

Keywords-*Elongation, axial force, cross-section, temperature, displacement, deformation, stress.*

Introduction.Many load-bearing elements of gas-generator, nuclear and thermal power stations, jet engines and the processing industry are rods of variable cross-section. To ensure reliable operation of these equipments, it is necessary to provide the thermal strength of load-bearing elements in the form of variable-section rods that operate with the simultaneous action of dissimilar kinds of heat sources. Because of the variability of the cross section, nonlinear thermomechanical processes appear in such rods. To study the nature of such processes, consider a horizontal rod of limited length, of variable cross-section. In this case, the radius of the section varies linearly along the length of the investigated rod, i.e. $r = ax + b$, $(0 \le x \le l)$, where is the l - length of the rod, $a, b - const.$. The cross-sectional area of the rod varies nonlinearly along the length of the rod in the following manner $F(x) = \pi(ax+b)^2$ [cm^2]. The lateral surface of the test rod along the entire length is heat-insulated. On the cross-sectional area of the left end of the rod $F(x=0) = \pi b^2$, a heat flux with a constant intensity $q[\frac{watt}{cm^2}]$. Through the cross-sectional area of the right end of the rod $F(x=l) = \pi(al+b)^2$, heat exchange takes place with the surrounding medium. At the same time, the heat transfer coefficient $h[\frac{watt}{cm^{2\,0}C}]$, ambient temperature T_{oc} [^{0}K], the physical and mechanical properties of the core material is characterized by the

coefficient of thermal expansion $\alpha[\frac{1}{^0K}]$, thermal conductivity $K_{xx}[\frac{watt}{cm\cdot^0K}]$ and modulus of elasticity $E[\frac{\kappa\Gamma}{cm^2}]$. The scheme of the investigated rod is shown in Figure 1.

In the presence of heat flow, heat insulation and heat transfer, the functional of the total thermal energy for the investigated rod has the form [1]:

$$J = \int_{F(x=0)} qTds + \int_V \frac{K_{xx}}{2}(\frac{\partial T}{\partial x})^2 dv + \int_{F(x=l)} \frac{h}{2}(T - T_{oc})^2 ds, \quad (1)$$

where $T = T(x)$ the field of distribution of temperatures along the length of the rod, which is approximated by a complete polynomial of the fourth order

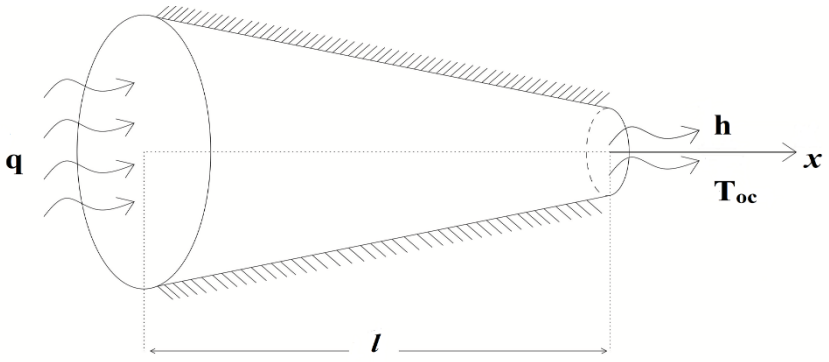


Figure 1. Scheme of the investigated rod.

$$T(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 = \varphi_i(x)T_i + \varphi_j(x)T_j + \varphi_k(x)T_k + \varphi_m(x)T_m + \varphi_n(x)T_n \quad (2)$$

where $\varphi(x)$ - are spline functions:

$$\begin{aligned}
\varphi_i(x) &= \frac{(3l^4 - 25l^3x + 70l^2x^2 - 80lx^3 + 32x^4)}{3l^4}, \\
\varphi_j(x) &= \frac{(48l^3x - 208l^2x^2 + 288lx^3 - 128x^4)}{3l^4}, \\
\varphi_k(x) &= \frac{(-36l^3x + 228l^2x^2 - 384lx^3 + 192x^4)}{3l^4}, \\
\varphi_m(x) &= \frac{(16l^3x - 112l^2x^2 + 224lx^3 - 128x^4)}{3l^4}, \\
\varphi_n(x) &= \frac{-3l^3x + 22l^2x^2 - 48lx^3 + 32x^4}{3l^4},
\end{aligned} \quad (3)$$

$0 \le x \le l$ where the nodal temperature values

$$T_j = T(x=0); \quad T_i = T(x=\frac{l}{4}); \quad T_k = T(x=\frac{l}{2}); \quad T_m = T(x=\frac{3l}{4}); \quad T_n = T(x=l); \quad (4)$$

Taking into account (2–4), minimizing (1) with T_i, T_j, T_k, T_m and T_n we obtain a resolving system of algebraic equations taking into account existing natural boundary conditions. Solving the system we determine the nodal values of temperature (4), and by (2) we construct the field of temperature distribution along the length of the rod. If one end of the rod is fixed and the other end is free, then the length of the rod Δl_T [cm] is determined according to the general law of thermophysics [1]

$$\Delta l_T = \int_0^l \alpha T(x)dx. \tag{5}$$

If both ends of the rod are rigidly fixed, then an axial compressive force R[kG] arises in the rod, which is determined from the compatibility condition of the deformation [1]

$$R = \frac{\Delta l_T \cdot E \int_0^l F(x)dx}{l^2}. \tag{6}$$

In this case, a distribution field of the thermo-elastic component of the voltage $\sigma(x)[\frac{\kappa\Gamma}{см^2}]$ arises in the rod:

$$\sigma(x) = \frac{R}{F(x)}, \quad 0 \le x \le l. \tag{7}$$

Then, according to Hooke's law, we can determine the distribution field of the thermo-elastic deformation component Ɛ(x) [dimensionless]:

$$\varepsilon(x) = \frac{\sigma(x)}{E}. \tag{8}$$

The temperature component of deformations $\mathcal{E}_T(x)$ [dimensionless] is determined according to the general law of thermophysics [1]:

$$\mathcal{E}_T(x) = -\alpha T(x). \tag{9}$$

Then, according to Hooke's law, the field of distribution of the temperature component of the stress

$\sigma_T(x)\,[\frac{\kappa\Gamma}{см^2}]$:

$$\sigma_T(x) = E \cdot \varepsilon_T(x) = -\alpha E \cdot T(x). \tag{10}$$

According to the theory of thermoelasticity, the laws of distribution of elastic components of deformations Ɛx(x) [dimensionless] and stresses $\sigma_T(x)[\frac{\kappa\Gamma}{см^2}]$:

$$\varepsilon_x(x) = \varepsilon(x) - \varepsilon_T(x), \tag{11}$$

$$\sigma_x(x) = E \cdot \varepsilon_x(x) = \sigma(x) - \sigma_T(x). \tag{12}$$

The potential energy of elastic deformations is used to determine the displacement field [4]:

$$\Pi = \int_V \frac{\sigma_x(x)}{2}\varepsilon_x(x)dv - \int_V \alpha E \cdot T(x) \cdot \varepsilon_x(x)dv. \tag{13}$$

According to the Cauchy relation [4], we have:

$$\varepsilon_x(x) = \frac{\partial U}{\partial x}, \tag{14}$$

$$U = U(x) = \varphi_i(x)U_i + \varphi_j(x)U_j + \varphi_k(x)U_k + \varphi_m(x)U_m + \varphi_n(x)U_n, \tag{15}$$

where U is the displacement field.

Minimizing Π from the nodal values of the displacement, a system of linear algebraic equations is constructed. To solve this system, it is necessary to specify the conditions for securing the two ends of the rod, i.e. $U_i = U(x=0) = 0$ and $U_n = U(x=l) = 0$.

Further, defining U_i, U_j, U_k, U_m, U_n and substituting them in 15), a displacement field is constructed. For practical application of the above method and algorithm, we take the following initial data l=20см; $a = \frac{1}{10}$; $b = 4$см; $\alpha = 0{,}0000125\frac{1}{^0K}$; $E = 2\cdot 10^6 \frac{\kappa G}{cm^2}$; $K_{xx} = 100\frac{watt}{cm\cdot{}^0K}$; $h = 10\frac{watt}{cm^2\cdot{}^0K}$; $T_{oc} = 40^0 K$; $q = -500\frac{watt}{см^2}$;

With these initial data, the solutions obtained are shown in Figure 2-5.

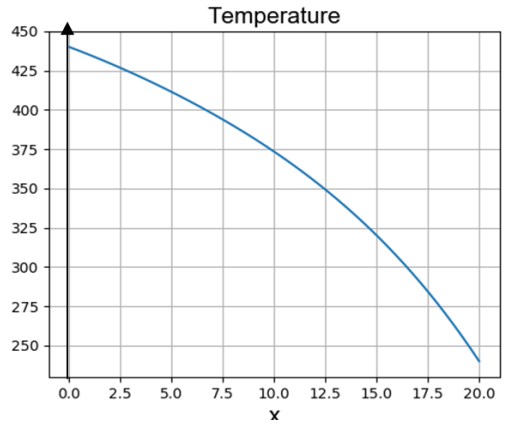


Figure 2. Dependences of the temperature T Dependencies along the length of along the length of the rod

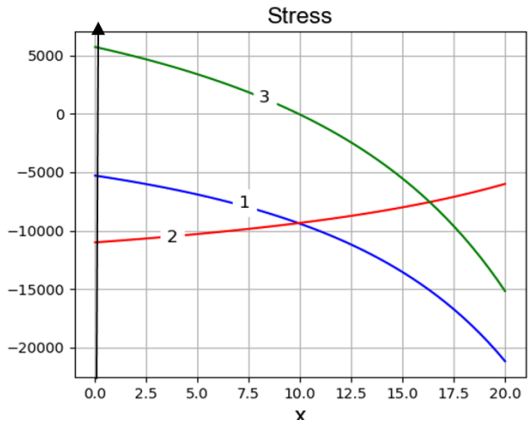


Figure 3. Stress

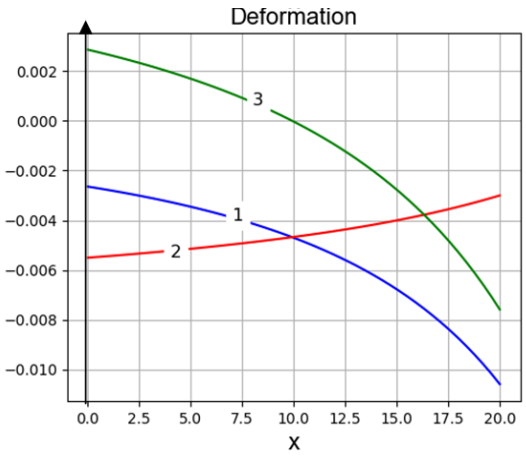


Figure 4. Dependence of the deformation displacement along the along the length of the rod

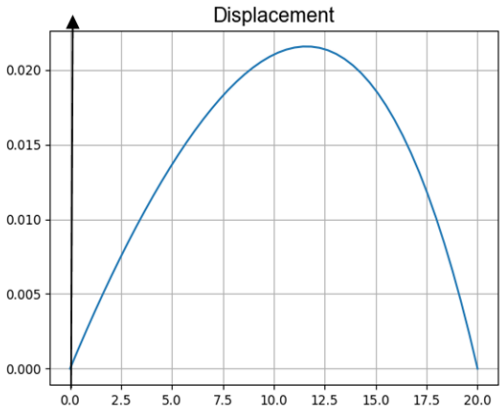


Figure 5. Dependences of length of the rod

Figure 2 shows that the temperature is higher near the left end of the rod, where the heat flow is supplied. Due to the thermal insulation of the lateral surface, heat is lost minimally, so that the temperature at the right end of the rod is maintained at 240^0K.

The stresses along the length of the rod are shown in Figure-3 $(1-\sigma(x)-$ thermoelastic, $2-\sigma_T(x)-$ temperature, $3-\sigma_x(x)-$ elastic component of the stress). It can be seen from the figure that the thermoelastic $-\sigma(x)$ and temperature $-\sigma_T(x)$ components of the stress along the entire length of the rod are of a compressive nature. While the elastic $-\sigma_x(x)$ component of the stress in the region $0 \le x \le \frac{l}{2}$ has a tensile character, and in the region $\frac{l}{2} \le x \le l$ it is compressive.

Dependences of deformations along the length of the rod are shown in Figure 4 ($1-\sigma(x)-$ thermoelastic, $2-\sigma_T(x)-$ temperature, $3-\sigma_x(x)-$ elastic component deformation). The distribution field of the deformation components is proportional to the corresponding stresses.

Figure 5 shows the field of distribution of displacements of a rod fixed at two ends. From this it can be seen that all sections (except for exceptions) move in the direction of the *x* axis. The greatest amplitude of displacement corresponds to the coordinate of $x \approx \frac{3l}{5}$.

A numerical model of nonlinear thermomechanical processes in a rod of variable cross-section is developed, based on the fundamental law of conservation of energy. This allows to obtain reliable numerical results taking into account all natural boundary conditions. The results obtained are consistent with the corresponding laws of physics. This method can be used for the numerical solution of a class of problems determined by the steady-state thermomechanical state of load-bearing structural elements operating under the influence of dissimilar kinds of heat sources.

References

1. Kudaykulov A., Zhumadillayeva A. Numerical simulation of temperature distribution field in beam bulk in the simultaneous presens of heat insulation, heat flux and heat exchange // Acta physica polonica A, 2016. – P. 335-336.

2. Tashenova Z., Nurlybaeva E. , Kudaykulov A. Method preparation and solution algorithm for resolving stationary problem of a rod under thermo - stressed condition restrained at both ends affected by heat exchange and heat flows // 2012 International Conference on Advanced Material and Manufacturing Science, 2012. – P.12-18.

3. Muheyat Niyazbek, Kuenssaule Talp, Kudaykulov A.K. Computer and Mathematical Modeling of Thermomechanical Processes in Element of Constructions / Acta Scientiarum Naturalium Universitatis Nankaiensis, Tianjin, China.- 2017.- Vol. 50, № 3.- P.354.

4 Timoshenko S., Goodyear J. N. Theory of Elasticity / McGRAW-Hill. Book. Company. Inc. , 1987. – 567 p.

ТӨТЕНШЕ ЖАҒДАЙЛАРДА ЭВАКУАЦИЯЛАУ ЕСЕПТІҢ МАТЕМАТИКАЛЫҚ ӘДІСТЕРІ МЕН МОДЕЛЬДЕРІ

[1,2]Козбакова А.Х., [1]Амиргалиев Е.Н., [1,2]Калижанова А.У., [1,2]Маликова Ф.У.,
[1]Атаниязова А., [1]Меліс З,
e-mail: ainur79@mail.ru
Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан
Алматы технологиялық университеті, Алматы, Қазақстан

Аңдатпа. *Бұл жұмыста төтенше жағдайларда оқу орнынан адамдарды эвакуациялау есептерді шешудің моделдері мен әдістері қарастырылған, ғимарат ішіндегі адамдардың қозғалыс ағынына математикалық модельдері қолданып эвакуациялау жоспарларды бағалау алынды. Есептің математикалық қойылымы мен пәндік аймаққа талдау жасалды.*

Түйін сөздер: *Эвакуация, төтенше жағдай, математикалық модель, алгоритм, максималды ағын.*

Кіріспе. Эвакуациялау тұрғындарды қорғаудың бір тәсілі болып табылады. Бұл қауіпті аудандардан адамдарды шығару немесе шығарып салу. Ол бейбітшілік кезінде де, соғыс кезінде де қолданылуы мүмкін. Эвакуациялау тұрғындарды қорғау тәсілі ретінде бұрыннан қолданылып келеді.

Тұрғындарды бейбітшілік, соғыс кездерінде қорғау амалы ретіндегі эвакуациялаудың көкейкестілігі соңғы жылдары төмендемеу түгілі жоғарылап кетті. Тұрғындар дүлей апаттарға, транспорт пен өндірістердегі қирау мен зілзалаларға тап болу себептерінен көптеген қауіптерге кезігуіне заманауи өмірдің тәжірибесі куә. Мысалы, дүлей апатты алайық: жер сілкінісі, су тасқыны, қар көшкіні, сел тасқыны, көшкіндер, ормандардың жаппай өртенуі. Мұндай жағдайлардың барлығында дерлік эвакуациялауға жүгінуге тура келеді. Атом электростанцияларында апаттық жағдай бет алғанда, биологиялық зиянды заттардың және апатты химиялық қауіпті заттектердің таралуы мен құйылуы кезінде, мұнай өндіруші және мұнай-химия өнерәсіп зауыттарындағы ірі көлемдегі өрттер кезінде эвакуациялық іс-шаралар жүргізілуі мүмкін.

Қойылған тапсырмада апаттық жағдайда оқу орнынан адамдарды эвакуациялау қаралады. Оқу кестесіне байланысты адамдардың ішкі бөлмелерге тұрақсыз таралуы оқу орны тапсырмасының негізгі ерекшелігі болып табылады. Бұл адамдардың кедергісіз қозғалуын ұйымдастыру көзқарасы бойынша оқу кестесін бағалауды қажет етеді. Жоғарыда айтылып өткендей берілген тақырып көкейкесті және көкейкесті болып табылады, себебі апаттық жағдайлар жиі кездесетін болды.

Эвакуациялау туралы есепті шешу алгоритмі

Оқу орнында төтенше жағдай болды делік, нәтижесінде адамдарды эвакуациялауға тура келеді. Ғимараттағы аудиториялардың әр бірінде 30 студенттен отырған 24 аудитория, сонымен бірге 8 баспалдақ орны және 2 шығысы орналасқан. Оқу орнынан студенттерді эвакуациялаудың уақытын, жылдамдығын және бағытын есептеу қажет.

Әр бір доғаның бағыты $v \epsilon V$ ағын қозғалысының бағытын білдіретін $G=<E, V, H>$кескінін береміз, мұндағы әр бір доғаның өткізу қабілеттілігі dv тең. E төбелер жиынтығында аудиториялар орналасқан. E төбелер жиынтығында екі төбе, яғни

төбенің басталуы мен аяқталуы белгіленген. 0 төбесі ағынның көзі, 35 ағу болып табылады. E -нан i үшін 2 сан берілген: сол жерде отырған адамдар саны мен бір мезетте сол жерден жүгіріп шығып жатқан адамдар саны. Доғалар- бұл байланыстар арасындағы баспалдақ орындары мен коридорлар.

Әр доға шектеулі өту қабілеттілігіне ие болғандықтан мүмкін болған ағынның болуын тексеруді оларды іздеумен максималды ағын туралы есеп пен оны Форд және Фалкерсон алгоритмімен шешу көмегімен жүзеге асыруға болады.

Максималды ағын есебінде ағын бастапқы төбенің біреуінен соңғының біреуіне өтеді. Барлық доғалар белгіленген өту қабілеттілігіне ие. есепті мұндай түрге алып келу үшін жалған ii және kk екі төбені қосамыз. i_0 ағын көзін ii біріктірейік. Ол үшін өту қабілеттілігі $-q_{i^0}(i_0)$ тең болады. $q_i(i) > 0$-лі ағып кетулерді kk төбені доғалармен біріктіреміз. Бұл доғаларға өту қабілеттілігі сәйкесінше $q_i(i)$ тең. Нәтижеде максималды ағын туралы стандартты түрдегі есепті аламыз, оны шешу үшін кез келген атақты алгоритмдердің бірін қолданамыз. Егер максималды ағын $q_{i^0}(i_0)$ кем болған болса, онда бір қабаттың қорытынды есебі , сәйкесінше есеп түгелімен шешімге ие болмайды. Мұндай жағдайда минималды қиылған жер қосымша доғалардан тысқары орналасады[1].

Егер максималды ағын $q_{i^0}(i_0)$ тең болған болса, онда инварианттық жаңғыртулармен теңсалмақтылық жағдайына өткізетін ұйғарынды ағынды аламыз.

Гриндшилс формуласының көмегімен коридор және баспалдақ арқылы адамдардың ағын қозғалысын суреттейік.Келесі белгілерді енгізейік: желі ауданының ұзындығы– L, ауданда қозғалу уақыты–T, уақыт бірлігінде жолдың қиылған жерінен өткен ағын– x , ағын тығыздығы–P, жолақтардың саны– S, ағын қозғалысының жылдамдығы–W ,коридордың орташа ұзындығы – λ .

Ағынды анықтауға сәйкес $\rho=1/\lambda$. W–студент жылдамдығы болсын,ал W_{max} – максималды жылдамдығы болсын. Адамның λ ұзындықтағы жол бөлігін басып өту уақыты $\tau=\lambda/v$ тең болады. уақыт бірлігінде студенттер саны $\kappa=1/\tau$ тең болады. Мұнан $x = ks = \frac{1}{T}S = \frac{w}{\lambda} = wps$. ағынның жылдамдығы мен тығыздылығы өзара $w/w_{max} + p/p_{max} = 1$(Гриндшил формуласы) сызықты тәуелділігімен байланысқан деп есептейік. Мұнан $w = w_{max}(1 - p/p_{max})$, немесе $p = p_{max}(1 - w/w_{max})$ [2].

Ағын болу үшін оған тіреу қойсақ, $x = swp_{max}(1 - w/w_{max})$ аламыз. Келіп шыққан функция төменге бағытталған тармақтары бар парабола, ол $w = w_{max}/2$ кезінде максимумға жетеді, сәйкесінше $x_{max} = s(w_{max}p_{max})/4$.

Міне осылай, біз максималды ағынның мөлшерін алдық.Ол ескерілмей кетуі де мүмкін.

ρ орнына формула қойсақ, келесі формуланы $w^2 - w_{maxx}w + \left(\frac{w_{max}}{sp_{max}}\right)x = 0$ аламыз.

Барлық студент өз жылдамдығын максималды жасауға тырысатынын ескере отырып Виета формуласы бойынша $w = w_{\max}(1 + \sqrt{1 - x/x_{max}})/2$ аламыз.

Осыдан алатынымыз, желі ауданында қозғалу уақыты келесі тәуелділікпен белгіленеді: $T(x) = 2T_{min}/(1 + \sqrt{1 - \frac{x}{x_{max}}})$, мұндағы T_{min} –ағын онымен нөлге тең болған жағдайда аудан ішінде қозғалудың минималды уақыты.

Эвакуациялық қозғалыстың ағынын қарастырайық. Берілген зерттеулер негізінде ені 0,6 м тең болып, бірнеше ағындар енінің жолы үшін оның кішкене қысқаруына рұқсат етіп қабылдануы мүмкін. Сонымен бірге, кездейсоқ кездескен

қозғалыс немесе қозғалыстың тоқтап қалуы кезінде басып өту мүмкіндігін қамтамасыз етуден, жолдың енінен тәуелсіз түрде бір ағынды ендейтін жолды бірнеше артық енмен қабылдау қажет. Осыны, сонымен бірге бар әрі бейімделіп жатқан эвакуациялық жолдарда ағын сандарының қажеттілігін есепке ала отырып, горизонтальды жол түрінде де баспалдақ қадамы түрінде де ағындардың енінің санын анықтау үшін кестені келтіруге болады.

Кесте 1- Ағын санының анықталуы

Қарапайым ағындардың саны	Эвакуациялық жол ені		
	Орташа	Минималды	Максималды
1	0,9	0,9	1,2
2	1,2	1,2	1,7
3	1, 8	1,7	2,3
4	2,4	2,3	3

Практикада жаппай қозғалудың жылдамдығы минутына 5-тен 75-ке дейін ауытқиды. Ұзақ қозғалу кезінде тығыздық физикалық көлем мөлшеріне қол жеткізе алмайды, сондықтан аудан ұзындығын есеп түрінде қабылдау орынды. Жазықтық жол үшін минутына 16 метрмен , баспалдақпен түсу үшін 10 метрмен және кем дегенде 20% көтерілу үшін минутына 8 метрмен жылдамдық көлемін есептеу анықталады.

Қарапайым ағынды минутына өткізу қабілеттілігі ағын тығыздығына жылдамдықтың бөлінуі жеке түрде анықталады. Толық өткізу қабілеттігі жол енінен табылған көлемнің ағындар санына және эвакуациялаудың созылуын құраушы сандар минутына көбейтілуімен түсіндіріледі. Мұнан түсінетініміз, эвакуациялық қозғалыс факторларының жиынтығынан тәуелді көбейтінді нормалар ұсынып отырғандай бірқалыпты көлемді көрсете алмайды, бірақ эвакуациялаудың созылуына мүмкіндік берудің үлкеюімен өсуіне және жергілікті шарттарға тәуелді белгілі бір дәрежеде өзгеріп отыратын көлем бола алады. Ұйғарынды жол ұзындығына уақыт нормалары тікелей әсер етеді.

Жол ұзындығы бірінші кезең үшін шығыстан шекті жойылуын сипаттайды да, көбіне ірі бөлмелер үшін маңыздылыққа ие. Бұл нормалар бірінші және екінші кезең қосындысы үшін сыртқа немесе баспалдаққа шығудың орналасуы мен сандар қатынасында бөлек қабаттардың жоспарлануын алдын ала шешеді. Үш кезеңнің қосындысы үшін осы нормалар үшінші кезеңнің өсуі бойынша бірінші және екінші кезеңдердің қысқаруын есепек ала отырып, қабатты шектеп, бөлмелерді қабаттарға топтастыруды диктовкалай отырып, жалпы ғимарат жоспарлануына әсер етеді[3].

Берілген бір есепті шешу үшін № 2 кестеде көрсетілген мәндер қолданылады, мұндағы «*н*» - доға басы, «*к*» - доға аяғы, W_{max} – максималды жылдамдық, P_{max} – максималды тығыздық, S – жолақтар саны, L – коридор ұзындығы.

Кесте 2 - Есепті шешу үшін бастапқы мәліметтер

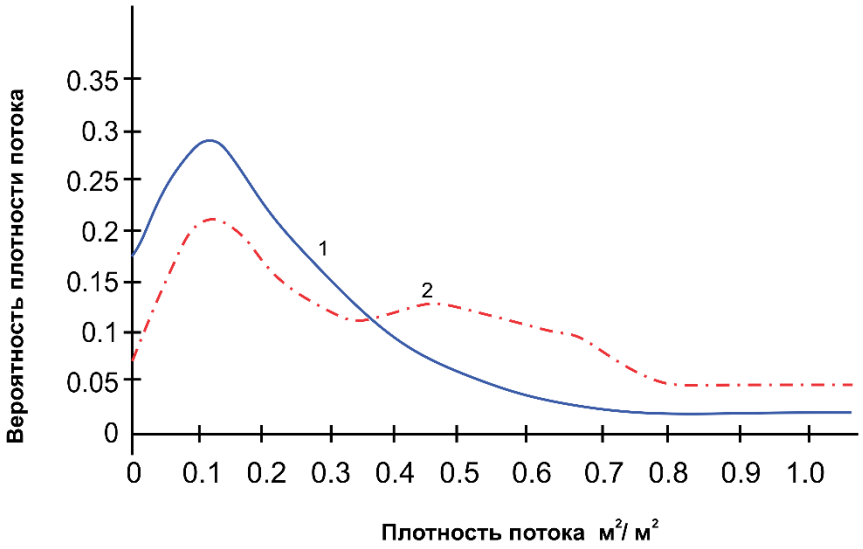
№ дуги	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
н	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	3	2	4	5	6	7	12	11	10	12	13	14	15	20	19	18	20
к	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	3	2	1	5	6	7	8	11	10	9	13	14	15	16	19	18	17	21
W_{max}	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
P_{max}	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
S	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
L	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10

Эвакуациялау туралы есепті шешу үшін желіде максималды ағын туралы есепті қолдану қажет. Сонымен бірге доға бойынша ағын қозғалысының анализін де, Форд пен Фалкерсон алгоритмін және потенциалдар әдісін қарастыру қажет.

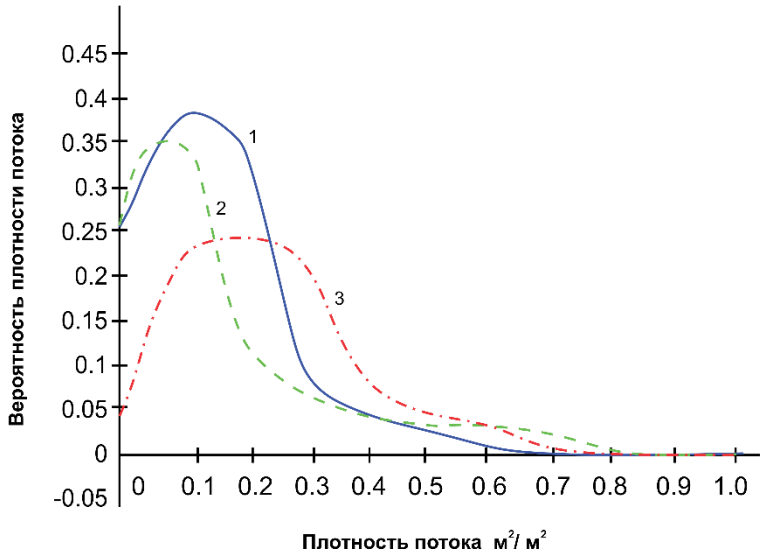
Адамдар ағыны N адамдар санымен және D тығыздығымен, яғни ағын орналасқан ауданға қатысты адамдар санымен сипатталады. $D_{макс}$ = 0,92 м^2/ м^2 адамдар ағынының тығыздылығының максималды мәні. Адамдар ағынын зерттеулер кейбір жағдайларда $D_{макс}$ ағын тығыздығы 0,92 м^2/ м^{2}шамасынан жоғары бола алатынын көрсетті (мысалы, енсіз есік орындарында). Адамдар ағыны белгілі бір V қозғалыс жылдамдығына ие. Жол Q өткізу қабілетімен яғникөлденең қима жол арқылы бір уақыт бірлігінде өтуші адамдар санымен сипатталады. Сәйкес, тығыздықтың физикалық тұрғыдан шегі түрінде $D_{ф.п.}$=1,15м^2/ м^2 шамасын есептеуге болады. Жол кенеттен тарылатын жерлерде ағын тығыздығы жоғары шамаға қол жеткізеді. Әр түрлі жол телімдері үшін ағын тығыздылығының ықтималдылығы 1-2. суреттерінде берілген [4].

Әрбір адам адамның өлшемімен анықталатын f көлденең кескін ауданымен сипатталады. Адам өлшемі физикалық мәліметіне, жасына және киіміне байланысты өзгереді. Адамдар өлшемінің және алынған нәтижелердің қорытындысының негізінде, кестеде–2.1 көрсетілген, адамның келесі орташа есептелген өлшемдері алынды [4].

Әрбір адамды V_0 ерікті қозғалыс жылдамдығымен және көңіл-күй жағдайының деңгейімен сипаттауға болады. Көңіл-күй жағдайының деңгейі белгілі бір адамдар ағынының қозғалыс категориясына сәйкес келеді: жайлы, байсалды, белсенді, жоғары белсенді [5-7].



Сурет 1-Ағын тығыздығының ықтималдығы: 1- есіктерде, 2- өзге жолдарда



Сурет 2-Ағын тығыздығының ықтималдығы: 1- баспалдақтар жоғарыға, 2- баспалдақтар төменге, 3- оқу орны

Кесте 1–Адамның орташа есептелген өлшемдері

Адамның жасы	Ені, м	Жуандығы, м	Көлденең кескін ауданы, $м^2$
Киімдегі ересек адам			
жазғы	0,46	0,28	0,100
көшеге арналған маусымаралық	0,48	0,30	0,113
көшеге арналған қыстық	0,50	0,32	0,125
жасөспірім	0,43 - 0,38	0,27 - 0,22	0,090-0,067
сәби	0,34 - 0,30	0,21-0,17	0,056-0,040

Клеткалы автоматтар, желілік модельдер, адамдар қозғалысын сұйықтық (гидроаналогия) ағынының ағымы түрінде беру адамдар қозғалысын модельдеудің жиі қолданылатын әдістері болып табылады [8].

Қорытынды: Гидравликалық желілер теориясының есептерін шешудегі тәжірибеміз ұсынылған амалдың тиімділігіне сенім арттырады. Осылай, мысалы, шамамен 1500 доға мен 1000 төбешік өлшемділігіндегі қалалық сумен жабдықтау желісінде, жылумен қамтамасыз ету желісіндеағынның таралу есебін 15-30 секунд ішінде дербес компьютерлерде шешу жол-көлік желілеріндегі ағынның таралуы қолайлы болған уақыт ішінде орындалуын топшылауға мүмкіндік береді. Ұсынылған алгоритмдер паралельдеу алгоритмдерін қолдануға мүмкіндік береді, бұл өз кезегінде кең көлемде заманауи көп процессорлы компьютерлік желілерді қолдануға мүмкіндік береді.

Ғылыми зерттеу жұмыстары Қазақстан Республикасы Білім және Ғылым министрлігінің гранттық қолдауымен № AP09259547 «Нақты уақыт режимінде эвакуациялау тапсырмалары үшін интеллектуалды ақпараттық технологияларды құру» жобасы аясында, Ақпараттық және есептеуіш технологиялары институтында жүргізілген.

Әдебиеттер

1. World Academy of Science Engineering and Technology «Evaluation of Parameters of Subject Models and Their Mutual Effects», Paris, International Science Index Vol:8 No:5 2014.– 600c.

2. Васин А.А., Морозов В.В. Теория игр и модели математической экономики. Москва: МАКС Пресс, 2005. – 237с.

3. Беляев С.В. Эвакуация зданий массового назначения. Москва: Издательство «Всесоюзной Академии Архитектуры», 1938. – 257с.

Малинецкий Г.Г. Моделирование движения толпы при помощи клеточных автоматов / Г. Г. Малинецкий, М. Е. Степанцов// Известия ВУЗов. Сер. Прикладная нелинейная динамика. 1997. Т. 5. С. 75-79.

Малинецкий Г.Г. Клеточные автоматы для расчета некоторых газодинамических процессов/ Г.Г. Малинецкий, М.Е. Степанцов // Журнал вычислительной математики и математической физики. 1996. Т. 36, № 5. С. 137145.

Малинецкий Г.Г Применение моделей класса решеточных газов для решения задач газодинамики / Г.Г. Малинецкий, М.Е. Степанцов // Изв. вузов. Прикладная нелинейная динамика. 1996. Т. 4, № 4,5. С. 59.

Малышкин В.Э. Основы параллельных вычислений. Методическое пособие. Новосибирск: НГТУ, 1998. 55 с.

Мациевский С. В. Нечеткие множества: Учебное пособие.- Калининград: КГУ, 2004. 176 с.

СЕКЦИЯ 2

Ақпараттық-телекоммуникациялық технологиялар. Деректерді жіберу желілері мен жүйелері. Интернет технологиялар. Бұлттық технологиялар. Параллельді есептеу. Үлестірімділік есептеулер. Суперкомпьютерлік және кластерлік жүйелер. Үлкен көлемді деректерді (Big-data) өңдеу. Геоақпараттық жүйелер және технологиялар. Инновациялық оқыту технологиялары

Информационно-телекоммуникационные технологии. Системы и сети передачи данных. Интернет-технологии. Облачные технологии. Параллельные вычисления. Распределённые вычисления. Суперкомпьютерные и кластерные системы. Обработка больших объёмов данных (Big-data). Геоинформационные системы и технологии. Инновационные образовательные технологии

Information and telecommunication technologies. Systems and networks of data transmission. Internet technologies. Cloud technologies. Parallel computing. Distributed computing. Supercomputer and cluster systems. Processing large volumes of data (Big-data). Geoinformation systems and technologies. Innovative educational technologies

БАЙЛАНЫС ИНЖЕНЕРЛЕРІН ҚАЙТА ДАЯРЛАУ БАРЫСЫНДА БІЛІМ БЕРУДІҢ ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯСЫ РЕТІНДЕ ИНЖЕНЕР КЕЙСІ - ӘДІСІНІҢ ҚОЛДАНЫЛУЫ

Бесбаева М.Қ., Медерова А. Ж.
e-mail: mbesbayeva89@gmail.com
ҚР ҰҚК Академиясы, Қазақстан

Аңдатпа. *Мақалада байланыс инженерлерін қайта даярлау барысында білім берудің инавациялық технологиясы ретінде инженер кейсі - әдісінің қолданылуының маңызы көрсетілген. Бұл әдісті қолданудың өзектілігі қазіргі таңда болашақ байланысшы мамандарының кәсіби құзіреттілігін қалыптастыра отырып жас маманның жұмысқа бейімделген яғни, техникалық пайдаланудағы жабдықтың істен шығуы немесе зақымдану сипатының мәселелерін талдап, тиімді және жылдам ойланып жабдықты қайта іске қосу үшін аналитикалық – шығармашылық ойлау қабілетін дамыту болып табылады.*

Қазіргі заманда болашақ байланысшы тек сауатты ғана емес, сонымен қатар техникалық пайдаланудағы жабдықтың істен шығуы немесе зақымдануы сипатының мәселелерін талдап, тиімді және жылдам ойланып жабдықты қайта іске қосу үшін аналитикалық – шығармашылық ойлау қабілеті дамыған болуы керек. Осыған байланысты, ең алдымен, бүгінгі заманға сай, сонымен қатар жұмыс орнына жаңадан орналасқан күннен бастап лауазымдық нұсқаулығына сәйкес бейімделген болуы үшін білім берудің жаңа әдістерінің қажеттілігі туындайды.

Оқытудың инновациялық технологиялары, интерактивті әдістері әртүрлі және олардың әрқайсысы өзінің артықшылықтары мен ерекшеліктеріне ие. Оқытудың интерактивті технологиялары арасында шығармашылық тапсырмалар, шағын топтарда жұмыс істеу, жұптасып жұмыс істеу, кейс-стадиялар, көрнекі құралдармен, бейне - және аудио материалдармен жұмыс істеу, проблемалық оқу, тәжірибеге бағытталған оқу кеңінен танымал. Интерактивті оқыту технологиясы тек қана бұрын оқытылған материалдарды бекітуге ғана емес жаңаларында оқытуға бағытталған [1].

Кейс – технология әдісі немесе талдау әдісінің негізгі ерекшелігі – студенттерге іскерлік тәжірибемен таныстыру және оқыту. Кейс технологиясын шет ел және ресей басылымдарда әр түрлі атауда кездестіруге болады, олар: стадилерді зерттеу әдісі, бизнес тарихы әдісі, кейс әдісі және т.б. Бұл әдістің басты мақсаты ақпаратпен жұмыс жасап үйрену, олардың туындаған мәселелерінің шешімін өндеу және студенттін қабілеттілігін арттыру. Яғни, студент оқытушымен алынған нәтижені өз бетінше өңдей білу керек. Бұл студенттің өзіндік тәжіриебесін және шешімін қалыптастырды, алынған білімін тәжірбиеде қолдану арқылы өзінің ой–өрісін, көз–қарасын мәселелерді шешуде қолдана алады[2].

Байланысшыларды оқытуда оқытушыларының алдында тәжірибеге бағытталған техникалық білім беру сапасын арттырудың маңызды міндеті тұр. Оларды іске асыру болашақ байланысшыларды оқытудың жаңа тәсілдері мен заманауи технологияларын, оқу процесіне оқытудың интерактивті әдістерін енгізуді талап етеді.

Бүгінгі заманда кәсіптік білім беру саласында адамның табиғи ерекшеліктеріне сәйкес мыңдаған мамандықтар мен кәсіптерге дайындау кезек күттірмейтін талап.

Адам еңбек ету іс-әрекетінде білім мен ептілікті игеру үшін кәсіптік білім беру қажет. Кәсіби білім – қандай да бір кәсіп аясында біліктілік қызметіне қажетті жүйелі білік, дағдыларды игеру процесі, құралы мен нәтижесі, және де сол кәсіби ортаға сай мінез-құлық ережелері мен нормаларды сақтауды қарастырады [3].

Осы мәселеге орай байланысшы мамандығы бойынша тыңдаушыларды оқытудың маңызды мақсаты байланыс жүйелері мен желілерінің жабдықтарын техникалық пайдаланудағы негізін тану, жабдықтардың істен шыққан бұзылымдарын жөндеу немесе жабдықты баптау арқылы іске қосу ғана емес, сондай-ақ телекоммуникация желілерінің заманауи міндеттерін шешуге қабілетті өз бетінше және аналитикалық тұрғыда ойлана алатын маманды дайындау болып табылады.

1-сурет. Инженер кейсі - әдісін қолдану пайдасы

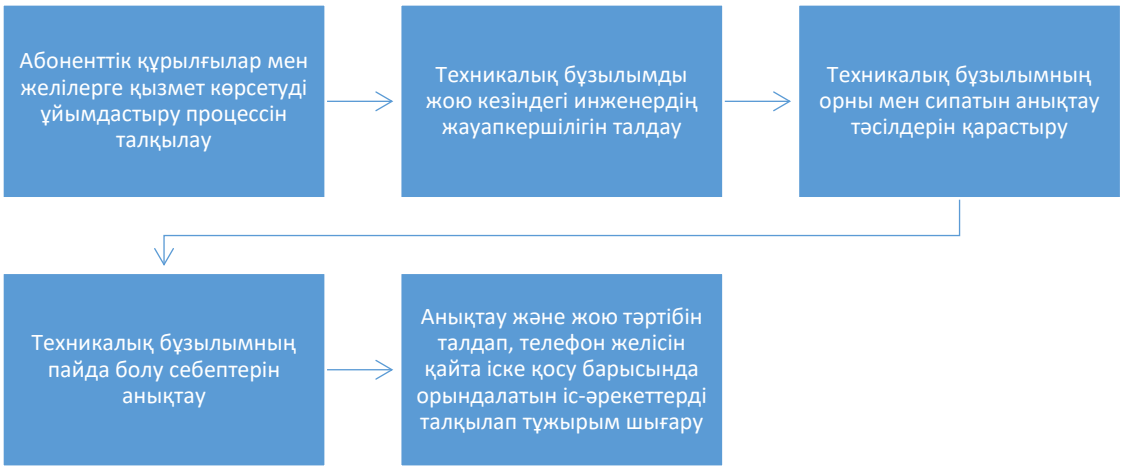
Сіздердің назарларыңызға практикалық техниканы пайдаланудағы жабдықтардың істен шығуына байланысты техникалық бұзылымды анықтап қайта іске қосу процессіндегі жағдайларды талдауға негізделген *инженер кейсі* - әдісін ұсынбақпын. Бұл әдісті қолданғанда болашақ байланысшының аналитикалық – шығармашылық ойлау қабілеті дамитын білім алуға екпін бар, ол бір техникалық бұзылымды жөндеу немесе техникалық жабдықты конфигурациялау тәсілінің

практикалық мысалына қарағанда анағұрлым көп шешімді болуы мүмкін. Бұл шешімдер әртүрлі іздеу тәсілдері және оларға жауаптар, тыңдаушылармен бірге пікірталастар барысында пайда болады. Пікірталас барысында тыңдаушылардың өз шешімдерін қорғауы, тыңдау және дұрыс шешім табу үшін пікірталас жүргізу қабілеті дамиды.

Осы әдіс бойынша талдау жүргізу үшін ұсынылған әрбір оқиғаның өзіндік ерекшелігі бар және байланысшыларға білім беруде осы әдіс станциялық жабдықтарын техникалық пайдалану пәнін оқытудың өзіндік ерекшелігі болып табылады. Әдіс бойынша тапсырмалар - оқытушының практикасынан алынған жағдай, анық, дәйекті, сонымен бірге қысқа. Бұл - түрлі байланыс жабдықтарының техникалық пайдалану барысында кездесетін бұзылымдардың түріне байланысты тиімді және уақытты үнемдей отыра бұзылымды анықтауға көмектесетін негізгі білімі мен аналитикалық ойлау қабілетін ортаға сала отырып дәйекті алгоритм құрып, белгілі бұзылымды жою үшін жөндеу жұмысына кірісуге мүмкіндік береді.

Инженер кейсінің барлық материалдары жазбаша түрде белгілі бір форматта және әртүрлі нұсқада ұсынылады, мысалы:

№1 нұсқада – Телефон желісінің бұзылымы, мысалы "Үзілу" ;"қысқа тұйықталу"; туындаған жағдайда, техникалық бұзылымды жою мақсатында қалай және қандай іс-әрекет жүргізілетінін болашақ инженер анықтап, телефон желісін іске қосу үшін тексеру және жөндеу әрекеттерінің алгоритмін құру үшін 2 сурет бойынша топтық аналитикалық талдау жасалады.



2-сурет. Телефон желісін іске қосу үшін тексеру және жөндеу әрекеттерінің алгоритмін құру схемасы

Инженер кейсі - әдісі бойынша телефон желісін қайта іске қосу барысында іс-әрекеттер алгоритмі:

1. Абоненттік құрылғылар мен желілерге қызмет көрсетуді ұйымдастыру үшін:
- техникалық бұзылым туралы өтінімдер жөндеу бюросына түседі;
- өтінім келіп түскен кезде техникалық бұзылымның түрі анықталады;
- өлшеу үстелінен АТС желілері мен жабдықтары жағына тексеру жүргізіледі.

2. Техникалық бұзылымды жою кезіндегі инженердің жауапкершілігі:
- инженер орындалатын жұмыстардың сапасына, бақылау мерзімінде техникалық бұзылымды жоюға, техникалық қауіпсіздік ережелерін сақтауға жауапты болады.

3. Техникалық бұзылымның орны мен сипатын анықтау:

- абонент жабдықтарының техникалық бұзылымы микрофон мен телефон немесе параллель қосылған микротелефон түтігінің көмегімен анықталады;

- АТС кроссынан қосу шкафына дейінгі бұзылымдар жөндеу бюросының өлшеу үстелінен немесе кростың қорғау жолақтарынан тікелей анықталады;

- тарату шкафынан және телефон аппараты жағындағы бұзылымды микротелефон түтігінің көмегімен анықтайды;

- телефон желілерінің техникалық бұзылымы желілік-абоненттік, кабельдік және станциялық-абоненттік болып бөлінеді.

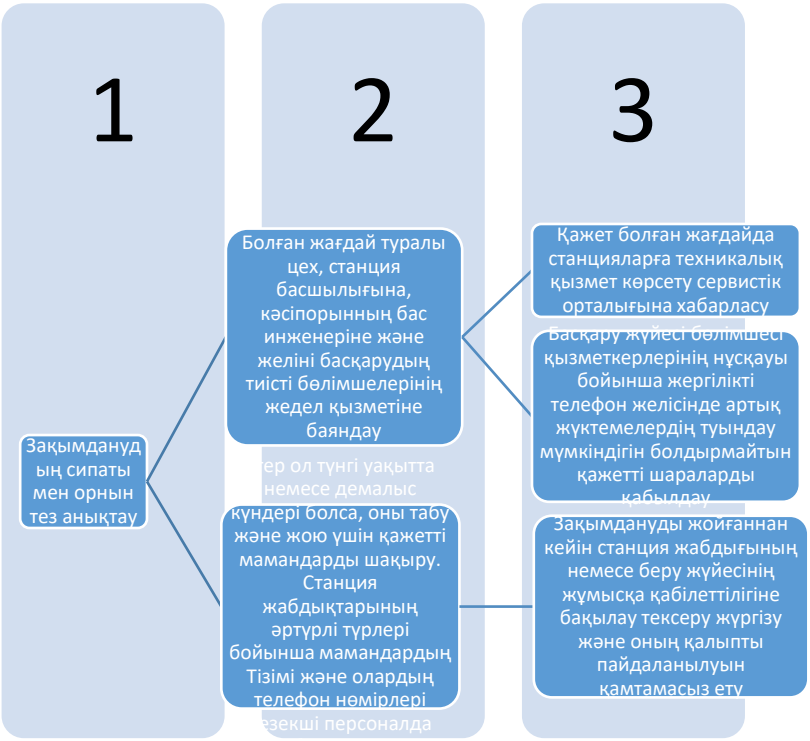
4. Техникалық бұзылымның пайда болу себептері:

- жабдықтың тозуы;
- механикалық әсер ету;
- климаттық жағдайлар;
- персоналдың дұрыс емес іс-әрекеттері болуы мүмкін.

5. Анықтау және жою тәртібі:

"Үзілу" зақымданған кезде - телефон сымын плинт клеммаларына қосқанда станция (зуммер) жауабының пайда болуы, станцияға дейінгі учаскеде зақымданудың болмауының белгісі болып табылады. Зуммер болмаған жағдайда зақымдалған сызық қорапта жабылады. Зуммердің болмауы үзілу шкафтан таратқыш қорапқа дейінгі учаскеде екенін растайды.

№2 нұсқа - станцияда авария немесе бірінші санатты зақымдану туындаған кезде техникалық персоналдардың іс – әрекетінің алгоритмін құру үшін (3-сурет).



3-сурет. Станцияда авария немесе бірінші санатты зақымдану туындаған кезде техникалық персоналдардың іс – әрекеті

Қажет болған жағдайда станцияда жоғарыда аталған бұзылымдардың кейбірі үшін индикацияның жекелеген түрлері көзделуі мүмкін. Бұл ретте мыналар белгіленуі тиіс:

- зақымданудың пайда болу орны, сипаты, ұзақтығы;
- зақымданудың пайда болуына ықпал еткен техникалық себептер;
- бұзылымдарды жою жөніндегі жұмыстарды ұйымдастырудың дұрыстығы және оларды анықтау және жою үшін қажетті техникалық құралдардың дайындығы;
- зақымдануды жоюға қатысқан техникалық персоналдың іс-қимылдарын, сондай-ақ зақымдануды жою процесінде өндірістік бөлімшелер басшыларының іс-қимылдарын білу және жеделдету.

Осындай мысалға алынған нұсқаларды инженер кейсі әдісімен талдау барысында, қосымша ретінде желілік байланыс құрылғыларына техникалық қызмет көрсету саласы бойынша түрлі сұрақтар-шеңбері арқылы техникалық қызмет көрсету қандай жұмыстарды қамтитыны қарастырылады, мысалы:

Жоспарлы-профилактикалық техникалық қызмет көрсету келесі жұмыстарды қамтиды:

- желілік құрылғыларды тексеру және профилактикалық қызмет көрсету;
- байланыс желілерінің электр сипаттамаларын жоспарлы және бақылау өлшеулерін жүргізу;
- пайдалануға түсетін жаңа кабельдерді, сымдарды, шеткі кабельдік құрылғыларды, жабдықтарды тексеру;
- желілік құрылыстарды күзгі-қысқы кезеңде, су тасқыны және найзағай кезеңінде жұмысқа дайындау.

Осы әдісте қолданылатын сұрақтар-шеңбері арқылы нақты және қисынды ойлану мен альтернативті шешім қабылдау барысында шығармашылық қабілетін қалыптастырған болашақ маман жұмыс барысында дұрыс шешім қабылдауға бейімделеді.

Кейс бойынша қорытынды (проблеманы анықтау, деңгейге бөлу, алгоритм құру) - бұл кейсті талдауға оқытушының авторлық тәсілін баяндаумен мәселені шешудің идеялары мен тәсілдері. Инженер кейсі арқылы оқытушы өзінің педагогикалық әлеуетін дамытады, тыңдаушылармен кәсіби түрде өсе алады, оқу үрдісінде инновациялық тәсілдерді ұстанады.

Инженер кейсі - әдісі станциялық жабдықтарды техникалық пайдалану бөлімшесі қызметкеріне қажетті білік, дағдыларды терең меңгеруге ықпал ете отырып, аналитикалық – шығармашылық ойлау қабілетін дамытады.

Әдебиет

1. Бұлақбаев М.К. Инновациялық технологияларды болашақ мұғалімдердің шығармашылық әлеуетін дамытуда қолданудың маңызы / Білім берудегі менеджмент – Менеджмент в образовании. – 2009. – No 2. – 66-69 б.

2. Учебно-методическое пособие. — Саратов: Издательский центр «Наука», 2009. – 52 б. – ISBN 978-5-91272-909-6.

3. Өстеміров К.У. Қазіргі оқыту технологиялары Алматы: АИПА, 2006. - 230 б.

БІЛІМ БЕРУДІ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ КИБЕРПЕДАГОГИКА

Мекебаев Н.О., Назкенова Б.Б., Касымова Д.Т.
e-mail: nurbapa@mail.ru , nazkenova_bayan@mail.ru, dika.cat@mail.ru
әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан

Аңдатпа. *Мақала педагогика ғылымының саласы ретінде киберпедагогика мәселелеріне арналған. Киберпедагогиканың қалыптасуының алғышарттарының кейбір аспектілері қарастырылады Киберкеңістік адам өмірінің жаңа ортасы және әлеуметтік өзгерістер факторы ретінде сипатталады. Ақпараттық–коммуникациялық технологияларды қолданатын киберәлеуметтену мәдениетін, сондай-ақ киберпедагогиканы – XXI ғасыр ғылымын дамытудың маңыздылығы киберкеңістіктің оқу, тәрбие және даму процестеріне әсерін ескере отырып, қазіргі заманғы білім беруді ұйымдастырудың негізі ретінде қарастырылған. Ресейлік және отандық йалымдардың ғылыми зерттеулерін талдау негізінде киберпедагогикаға байланысты ұғымдар талданған. Білім беруде Цифрлық қоғам – адамдардың өмір жағдайына, олардың біліміне және жұмысына, сонымен қатар мемлекет, бизнес және қоғам арақатынасына ақпараттық-коммуникациялық технологиялар арқылы шешуші әсер ететін, қоғам өмірінің барлық салаларында білім мен ақпараттық доминантты рөлімен ерекшеленетін өркениет дамуының заманауи кезеңі ретінде сипатталады.*

Кіріспе. Қазіргі әлемнің дамуы өте күрделі де жылдам және ол процесс ақпараттық-коммуникациялық бағытпен сипатталады. Адамның қажеттіліктері ақпарат алу, байланыс және басқалармен қарым-қатынас орнату тек тікелей ғана емес, сонымен бірге Интернет арқылы да қанағаттандырылады. Ол үрдіс білім беру саласына, білім жүйелеріне өз ықпалын кеңінен әсер етіп жатыр деп айтуға болады. Осы тұрғыда педагогика, психология салаларында жаңа ағымдар байқалады. Онлайн және офлайн оқыту формаларында оқу процесін сапалы қамтамасыз ету мақсатында балаларды, барлық санаттағы білім алушыларды, мұғалімдерді, оқытушыларды, ата-аналар мен ғалымдарды байланыстыратын педагогика ғылымының инновациялық салаларының дамуы. Бұл зерттеудің мақсаты - оқытуда АКТ-ны қолдану нәтижесінде пайда болған педагогика, психология әдістемелері мен теорияларындағы Өзгерістерді анықтау және киберпедагогиканы педагогика ғылымының жаңа саласы ретінде қарастыра отыра, оның ұғымдарының сиппатамасын қарастыру.

Үздіксіз білім берудің мақсаты – адамның білім беру қажеттілік-терін толығымен қанағаттандыру екендігі белгілі, бұл оның өзін-өзі толық жүзеге асыруға деген ұмтылысының көрінісі де, тез өзгеретін әлемнің жағдайларына бейімделу болып табылады. Мұндай жағдайда адамның өзі оқу процесінің белсенді қатысушысы болады. Білім беру жүйесі жеке адамның, қоғамның және экономиканың қарқынды өзгеретін қажеттіліктеріне реакциясын қамтамасыз ететін икемді білім беру траекторияларын қалыптастыру үшін жағдай жасауды қажет етеді. Сонымен бірге, өзгермелі қоғамдағы білім ақпараттық және коммуникациялық, электрондық, цифрлық, компьютерлік және интернет технологияларға әлеуметтік-

экономикалық дамудан туындаған кең ауқымды білім беру қажеттіліктерін қанағаттандырудың жалпы міндеттерін қояды[1].

Бүгінде еліміздің экономикасының барлық салаларын цифрландыру күн тәртібінің басты тақырыптарының бірі болып отыр. Осы бағытта жүріп жатқан белсенді жұмыстың басым бағыттардың бірі білім беруді қамтиды. Білім саласындағы цифрландырудың ең басты міндеті білім беру сапасын арттыру, яғни халықаралық дейгейде әртүрлі салаларда, оның ішінде «жасанды интеллект» және «ауқымды деректер» жасау саласында бәсекеге қабілетті ел жастарын дайындау. Бұл тұста болашақ педагог мамандардың цифрлық сауаттылығына көңіл аудару қажет. Цифрлік сауаттылық — бұл адамның өмірдің барлық салаларында цифрлік технологияларды сенімді, тиімді, сыни және қауіпсіз қолдануға дайындығы және қабілеті. Ол қазіргі таңдағы өзекті мәселеге айналып отырғаны рас. Адамның миын алмастыру мүмкін болмағанымен, оны жасанды интеллект арқылы жүзеге асыруға болады. Жасанды интеллект- бұл адам ойын компьютерде бейнелейтін программалық жүйе.Ауқымды деректер -білім беру жүйесі деректерден білім алудың заманауи әдістері, модельдеу мен болжаудың математикалық әдістері, заманауи бағдарламалық жүйелер мен деректерді талдауға арналған бағдарламалау әдістері саласындағы дайындықты көздейді. Қазіргі таңдағы педагогиканың жаңашыл инновациялық саласы ретінде кеңінен қолданылып айтылып келе жатырған киберпедагогика ұғымы пайда болуда. Соңғы кезде педагогика және психология ғылымдарында қарастырылып отырылған проблемаға байланысты жаңа терминдер жиі қолданылып жүр. Олар виртуалдық педагогика, коммуникациялық педагогика, интербелсенді педагогика, цифрлық педагогика, интернет-педагогика. Сонымен қатар қазіргі білімдік бірлестікте **киберпедагогика** деген термин, ұғымды жиі кездестіреміз [2].

Кибер –(ағылш. Cyber) – компьютерлік электрондық цифрлық технологиялармен байланысты кибер әртүрлі желілік ресурстарға, ақпараттық объектілер мен оқиғаларға және т.б. сілтеме жасау үшін қолданылатын бүкіләлемдік ғаламдық желілік түбір. Сол себепті білім беру жүйесіне «виртуалды шындық технологиясы» ұғымы мен киберлік әлеументтендіру үрдісінде кибербілім беру және оқыту, кибербілім беру бойынша арнайы ұйымдастырылған мақсатты, жүйелі іс-әрекеттер маңызды орын алып отыр.

Қазақстандық авторлардың пікірінше, интернет-педагогика – бұл педагогиканың бір саласы, барлық жастағы, санаттағы білім алушыларды, стейкхолдерлерді қашықтықтан оқытудың барлық электрондық материалдарына бірыңғай жылдам қол жеткізу негізінде электрондық оқыту принциптерін іске асыратын жеке іздеу жүйесі. Интернет педагогикасының негіздері, дәстүрлі педагогика сияқты, жалпыадамзаттық құндылықтар, отбасы мен қоғамның құндылықтары, АКТ-ға негізделген заманауи дидактика [3]. Шын мәнінде, қоғамның даму тарихында алғаш рет ақпарат пен ғылыми білім оны жетілдірудің құралы ғана емес, оның әлеуметтік-экономикалық қызметінің негізгі өнімі болып табылады. Сонымен қатар, ақпарат пен білім – бұл ақпараттық қоғамның негізгі активтері мен өнімдері, оның одан әрі әлауқаты мен әлеуметтік дамуы тікелей байланысты. Ақпараттық және коммуникациялық, электрондық, цифрлық, компьютерлік және интернет-технологиялар осы дамудың маңызды құрамдас бөлігі болып табылатындығын тағы бір рет атап өткен жөн.Ол технологиялардың дамуы тез және үздіксіз өзгерістермен сипатталатын ортаны тудырады [4].

Білім беру тарихына үңілсек, киберпедагогиканың пайда болуына, дамуына өз негіздері бар. Адам өмірінің мәдени, тарихи, әлеуметтік-психологиялық және

педагогикалық негіздері уақыт өте келе тарихи сипаттағы ақпараттық төңкерістермен анықталды.

Мысалы, XX ғасырдың ортасын ақпараттық технологиялардың қалыптасуының, компьютерлер мен компьютерлік желілерді, мәліметтер базасын құрудың бастау кезеңі деп айтуға болады. Осы кезеңнен бастап білім саласында жаңа оқу тәсілдері, жүйелері пайдалана басталады.

Олардың ішінде : бағдарламаланған оқыту (Б. Ф. Скиннер, Н.А. Краудер (АҚШ), (В.П. Беспалько, Ю.А. Самарин және т.б.); нейрожелілік педагогика (М.М. Бонгард); кибернетикалық оқыту тұжырымдамасы (С.И. Архангельский, Л.Б. Ительсон және т.б.); кибернетикалық дидактика (Ф.Хайманн) және т.б.

Ресей ғалымы В.А. Плешаковтың айтуынша, XX ғасырдың ортасынан XX ғасырдың 90-жылдарына дейін жалғасқан уақыт – төртінші ақпараттық революция кезеңі. Бесінші ақпараттық революция, ғалымның пікірінше, XX ғасырдың соңында басталды (1990 ж. – Н.В.): "... ол қазіргі адамзатқа өркениет эволюциясының сапалы жаңа кезеңіне-киберэволюцияға көшуге мүмкіндік беріп, бүкіл әлемдегі әлеуметтік құрылымдардың жаңа түбегейлі өзгерістерінің катализаторы болды" [5].

Сонымен, біздің теориялық шолуымыз аясында мүлдем жаңа жағдайда адам іс-әрекетіне тікелей байланысты ақпараттық төңкерістердің салдары ерекше маңызды болып табылатынын атаймыз. Ал бұл процесс педагогика, психология ғылымдарының әдіснамаларына көп өзгерістерді енгізуді талап етті.

Жаңа ақпараттық қоғамның негізі – нейрондық желі, жасанды интеллектті кеңінен қолдану, цифрлық технологиялар, жаңа басқару технологиялары болып табылады. Қоғам кибер-виртуалдық формацияға енеді, онда болып жатқан процестер тек бақыланатын ғана емес, сонымен бірге осы технологиялар арқылы басқарылады. Ең бастысы, кибервиртуалистика білім беру, тарих, әлеуметтану, психология сияқты маңызды салаларды қамтиды, педагогика – киберпедагогикада жаңа парадигманың қалыптасуына ықпал етеді.

Киберпедагогика проблемаларын зерттеп жүрген ғалымдардың пікіріне сүйене отыра, киберпедагогиканың негізгі мынадай мақсат-міндеттерін белгілеуге болады: жеке тұлғанын киберәлеуметтендіру мәдениетін қалыптастыру үшін қауіпсіз жағдайлар жасау, осы процесті оңтайлы (жасына, адамның әлеуметтік мәртебесіне және т.б. байланысты) сүйемелдеу, оны киберәлеуметтендіру процесінде адамға уақтылы пара-пар көмек көрсету. Үздіксіз білім берудің мақсаты адамның білім беру қажеттіліктерін толығымен қанағаттандыру екендігі белгілі, бұл оның өзін-өзі толық жүзеге асыруға деген ұмтылысының көрінісі болып табылады және тез өзгеретін әлем жағдайларына бейімделу. Мұндай жағдайда адамның өзі оқу процесінің белсенді қатысушысы болады. [5]

Білім және ғылым министрі Асхат Аймағамбетов жаңа оқу жылында 1-11 сынып оқушылары қашықтықтан білім алатынын мәлімдеген болатын. Министрдің айтуынша, елде эпидемиологиялық жағдай 1-тоқсаннан кейін жақсаратын болса, дәстүрлі түрдегі білім беру форматына көшудің стратегиясы әзірленіп қойған. «Қазір індеттің таралуы «қызыл» деңгейде болып тұр. Сондықтан қашықтықтан білім беру өте маңызды. Одан кейін жағдай жақсарып, «қызғылт сары түс» немесе «сары», «жасыл» деңгейге жеткен кезде, білім беруді ұйымдастырудың басқа бірнеше нұсқасын қолданатын боламыз. Осы нұсқаларға көшу арқылы кезең-кезеңмен дәстүрлі түрде білім беруге қайта ораламыз. Бұл стратегия дайын. Ол

бекітіліп, сәйкес министрлікпен келісілді. Сол себепті, эпидемиологиялық ахуалға байланысты жұмысты жалғастыра береміз», – деген Асхат Аймағамбетов. Министрдің сөзінше, індет тарамаған шалғай жатқан ауылдардағы шағын жинақты мектептерде бұрынғыдай дәстүрлі түрде білім беруге рұқсат бар. Ал егер балалар мен ұстаздардың денсаулығына қандайда бір қауіп төне қалса, білім беру үдерісі теледидар және басқа да құралдар арқылы қашықтықтан жалғасады. Сондай-ақ, дәстүрлі форматта білім алуға бастауыш сынып балаларының да мүмкіндігі бар. Оларға тиісті санитарлық-эпидемиологиялық қауіпсіздік шараларын сақтай отырып білім берілмек. Алайда осындай қауіпті кезде баланы мектеп қабырғасында оқыту үшін ата-анасы жазбаша өтініші беруге міндетті. Ал қыркүйек айынан бастап көптеген оқушы білім алуға үйіндегі компьютерінің алдында отырып кіріседі. «Шынымен де мектептегі компьютерлердің көбі ескіріп қалды. Қажет еткен балаларға уақытша пайдалануға беруге болатын осы тәрізді құрылғылар жеткіліксіз. Сол себепті 36 мыңнан астам компьютер сатып алынды. Ал 1 қыркүйекке дейін өңірлердегі әкімдіктер керегінше қосымша компьютерлер сатып алуы керек. Бүгін Үкімет отырысында осындай тапсырма берілді», – деді Асхат Аймағамбетов. Қашықтықтан білім беру кезінде интернет платформалардың атқаратын маңызы өте зор екені белгілі. Ведомство басшысының айтуынша, бұл тұрғыда да бірқатар іс атқарылған. «Біз IT-компаниялармен бірлесіп жұмыс істеп жатырмыз. Олар бүгінгі күнге дейін платформаларын жетілдірді. Платформалар әлдеқайда қолайлы бола түсті. «Күнделік» және басқа жүйелерге жақсырақ интеграцияланды. Айта кетерлігі, бұл интернет платформалар да келер оқу жылының 1-2 тоқсаны үшін материалдар дайын. Қазіргі кезде осы сайтттар ерекше қажеттілігі бар балаларға арнап икемделуде», – деген министр, теледидарға арналған бейнесабақтар да түсіріліп жатқанын айтты. Асхат Аймағамбетовтің сөзінше, қашықтықтан білім беру форматында жұмыс істеу үшін педагогтен бірнеше құзыреттілік талап етіледі. Ол үшін педагогтер біліктілігін арттыру курстарында оқиды. «Біріншіден, педагогтің IT-технологиялар жөнінен құзыреттілігі керек. Интернет жүйелерді және технологияларды білуге тиіс. Сол себепті, педагогтерге әзірленген курстар аясында міндетті түрде біліктілігін арттыру мүмкіндігі беріледі. Екіншіден, жаңа жағдайда білім беру әдістемесін, киберпедагогиканы білу мәселесі тұр. Өйткені дәстүрлі түрде сыныпта және қашықтықтан сабақ берудің айырмашылығы жер мен көктей. Әріптестеріміздің барлығының біліктілігін арттырамыз», – деді. Айта кетсек, білім берудің жаңа форматы тек мектепке ғана қатысты емес. Елдегі колледждер мен университеттер де жаңа оқу жылын қашықтан білім беру арқылы бастайды. [6]

Қорытынды. Қазіргі кезеңдегі қоғамның қарқындылық дамуы мен әлеуметтік институттарды ақпараттандырудың тереңдігі, барлық салаларды цифрландыру, басқадай факторлар білім беруді одан әрі ақпараттандыру, өзгеруін және жағыртуды талап етеді. Осы жағдайдайлар қоғамдық құндылықтарды өзгеруге апарып, адамды желілік сәйкестендіруге әкелді. Бүгінгі таңда адамға жаңа практикалық дағдылар мен теориялық білім ғана емес, сонымен қатар осы білім мен дағдыларды үнемі жетілдіру мүмкіндігі қажет. Басқаша айтқанда, адамзат өмір бойы киберәлеуметтендіру контекстінде үздіксіз білім беру мәдениетін жан-жақты дамытуы керек, өйткені жаңа технологиялар дәстүрлі білім беру процесінің шеңберін өзгертеді. Сондықтан педагогика ғылымындағы ғасырлар бойы қалыптасып келе жатқан кейбір ұстанымдар өзгерістерді талап етеді.

Жасалған сараптама бойынша, ғалымдардың пікіріне сүйене отыра, үздіксіз білім беру жүйесінің дамуында жаңа өзгерістерге сәйкес педагогика, психология

ғылымдарындағы жаңа ұғымдардың, терминдердің өз орнын алып жатқанын байқаймыз. Осыған байланысты пайда болып жатқан негізгі ұғымдар: киберпедагогика, киберәлеуметтендіру, киберкеністік, цифрлық білім беру ортасы, т.б.

Бұл ұғымдар педагогика ғылымында инновациялық сала ретінде киберпедагогиканың негізін құрайды деп айтуға болады.

Асхат Аймағамбетовтің сөзінше, қашықтықтан білім беру форматында жұмыс істеу үшін педагогтен бірнеше құзыреттілік талап етіледі. «Біріншіден, педагогтің IT-технологиялар жөнінен құзыреттілігі керек. Интернет жүйелерді және технологияларды білуге тиіс. Екіншіден, жаңа жағдайда білім беру әдістемесін, киберпедагогиканы білу мәселесі тұр. Өйткені дәстүрлі түрде сыныпта және қашықтықтан сабақ берудің айырмашылығы жер мен көктей. Әріптестеріміздің барлығының біліктілігін арттырамыз», – деді. Айта кетсек, білім берудің жаңа форматы тек мектепке ғана қатысты емес.

Әдебиеттер

1. Игібаева А.Қ., Төлеуханова А.Д. Киберпедагогика–педагогика ғылымының инновациялық саласы ретінде/ Вестник КазНПУ им. Абая, серия «Педагогические науки», №4 (68), 2020 г. С. 12-16

2. Элен Битэм, Рона Шарп. Педагогиканы цифрлық дәуірде қайта зерделеу. XXI ғасырдағы оқыту дизайны. - Алматы: «Ұлттық аударма бюросы» қоғамдық қоры. - 2019 жыл. – 328 б.

3. Бахтиярова Г.Р. Қазақстан Цифрлық дәурде оқыту дизайнын құруда интербелсенді ідстерді пайдаланудын жолдары. Хабаршы «Педагогикалық сериясы» Абай атындағы Қазақ ұлттық педагогикалық университет. 2020. №1(65). – 65-71 б.

4. Карауылбаев С.К., Артюхина М., Жумабаева А.М., Муратова Г.И. Границы развития интернетпедагогики/ / Педагогика және психология. Абай ат. ҚазҰПУ,2020. – 2-10 б.

5. Плешаков В.А. Перспективы киберонтологического подхода в современном образовании // Вестник Московского городского педагогического университета. Серия: педагогика и психология. 2014. № 3(29). – С. 1-18

6. Маденова Л.М. Бүгінгі білім берудегі цифрландыру –киберпедагогика мәселесі - https://bilimger.kz/85387/ (09.04.2021)

7. Аймағамбетов А. Мұғалімдер киберпедагог құзыретін алады - https://inbusiness.kz/kz/news/mugalimder-kiberpedagog-kuzyretin-alady

МӘЛІМЕТТЕРДІ ЕНГІЗУ МЕН ӨҢДЕУГЕ АРНАЛҒАН ГЕТЕРОГЕНДІК АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ ӘКІМШІЛІК ГРАФИКАЛЫҚ ИНТЕРФЕЙСІН ҚҰРУДАҒЫ АДАПТИВТІ ТЕХНОЛОГИЯЛАР

Мухитова А.А.
e-mail: mukhitova.aigul@gmail.com
әл-Фараби атындағы Қазақ ұлттық университеті, Казахстан
Адалбек А.
e-mail: q_al@mail.ru
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Казахстан
Еримбетова А.С.
e-mail: aigerian@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аңдатпа. *Таратылған гетерогенді ақпараттық жүйелерге арналған графикалық әкімшілік WEB-интерфейстер ортасымен мәліметтерді енгізу мен өңдеудің адаптивті модельдерін жүзеге асыру технологиялары қарастырылған. XSLT технологиясын қолданып XSD мәліметтер сұлбасын анықтау негізінде XML форматында мәліметтерді енгізу мен өңдеудің адаптивті моделын жүзеге асыру мысалы келтірілген. Гетерогендік ақпараттық жүйелерге арналған XML-жазбаларын өңдеушісінің ұсынған бағдарламасын ZooSPACE платформасымен интеграция жасауға болады.*

Әдетте, қолданушылардың талабына сай икемделе алатын мүмкіндігін адаптивті қолданушы интерфейсі деп түсінеміз. Бірақ адаптивтіліктің басқа да қыры бар ол – ақпарат көздерінің қызметтері мен құрылымына икемделе алатын мүмкіндігі. Төменде дәл осы адаптивтілік қарастырылатын болады.

Ақпараттық ресурстармен жұмыс істеуге арналған қолданушы интерфейстерінің, кем дегенде, ақпараттарды іздеуді басқаратын элементтері мен табылған ақпараттарды көрсететін мүмкіндіктері болу керек. Біртекті ақпарат көздері үшін бұл мәселе қарапайым түрде шешіледі, бірақ біртекті емес ақпарат көздері үшін мәселелер туындайды. Бір жағынан, басқару элементтері ақпаратты көрсету мен іздеу параметрлерін таңдаудың анағұрлым кең диапазонында бапталу керек, бірақ енді бір жағынан, әрбір нақты ақпараттық ресурсқа олардың мүмкін болатын мәндерінің аз параметрлер тізбегі сәйкес келуі жеткілікті. Әртүрлі ақпараттық ресурстарға арналған басқару элементтерінің параметрлерін таңдағанда қолданушы интерфейсіне салмақ салатын, қолдануға келмейтін мәндерді жою үшін нақты ақпараттық ресурстар туралы қосымша ақпараттар талап етіледі.

Ақпараттық ресурстардың сипаттамасына икемделе алатын қолданушы интерфейстерін төменде адаптивті деп атаймыз.

Жоғарыда айтылған мағынадағы адаптивті қолданушы интерфейсін жүзеге асыру үшін әрбір ақпарат көздерінің қызметтік қасиеттері туралы кіріс ақпараттары қажет. Ақпараттық ресурстарға қол жеткізу үшін қолданылатын технологияларға байланысты мұндай ақпаратты алуға және өңдеуге болады. Атап айтқанда, [1] еңбекте өзінің әртүрлі модификациясындағы Explain [2, 4-5] қызметтеріне негізделген Z39.50 [2] мен SRW/SRU [3] платформаларын қолданып ақпаратты

іздеуді басқаруы мен алынған ақпараттарды көрсету тәсілдеріне арналған адаптивті қолданушы интерфейсін құру технологиясы қарастырылған. Сонымен қатар, ZooSPACE [6-7] платформасына арналған адаптивті интерфейстерді жүзеге асыру қарастырылған.

Бірақ ақпараттық жүйелердің қолданушы интерфейсінен басқа, сонымен қатар, біртекті емес жүйелер әкімшілік интерфейспен бірге біртекті емес мәліметтерді басқаруға мүмкіндік беретін интерфейстері болуы керек. Ең алдымен, мәліметтерді құруға және өзгертуге арналған интерфейстер туралы айтып отырмыз.

Біртекті ақпарат көздеріне (жазба құрылымы бекітілген) арналған мәліметтерді құру мен өңдеу мәселесі қарапайым түрде шешіледі, алайда гетерогенді ақпарат көздері үшін (жазба құрылымы кез келген болуы мүмкін) қажетті қызметтері бар графикалық интерфейстерді құру үшін адаптивті технологияларды қолдану керек болады.

Төменде адаптивті графикалық WEB-интерфесті біртекті емес ақпараттық жүйелердегі мәліметтерді құру мен өңдеуге арналған технология қарастырылатын болады. Сонымен бірге, мәліметтер сәйкес келетін ақпарат көздерінен XML-форматында алынуы мүмкін. Негізінде басқа құрылымдық форматтарды да қолдануға болады, бірақ XML форматы мәліметтерді өңдеудің WEB интерфейстерін құру үшін ең қолайлысы.

Құрылымданған ақпараттарты көрсету үшін XML форматын қолданғанда XML жазбасының құрылымын құру ережелерінің сипаттамасы болуы қажет, яғни мәліметтер схемасының сипаттамалары. Әдетте XML үшін бұл ережелер XSD [8-10] терминдерінен тұжырымдалады және стандартты құралдармен өңделетін XML құрылымын білдіреді, мысалы XSLT [11].

Гетерогенді ақпараттық жүйедегі нақты ақпарат көзінен жазбаны шығарған кезде және осы жазбаны өңдеу үшін XML форматында ұсынған кезде мәселелер туындайды - шығарылған жазбаның мүмкін болатын құрылымының толық сипаттамасын қайдан алуға болады?. Шын мәнінде, келесі нұсқалар болуы мүмкін:

–XML өңдеу үшін алынған жазбада қолданатын атаулар кеңістігін анықтау кезінде schemaLocation атрибутының мәні ретінде URL түрінде пайдаланылған XSD мәлеметтер схемасына сілтеме болуы мүмкін. Ол әдетте жазбаның түпкі XML элементінде болады. Бұл жағдайда XSD алу мәселесі тривиалды түрде шешіледі.

–XML өңдеу үшін алынған жазбада атаулар кеңістігінің идентификаторы (URI) болады, бірақ қолданылатын XSD деректер схемасына URL сілтемесі жоқ. Бұл жағдайда XSD-ді атаулар кеңістігінің идентификаторымен қамтамасыз ету үшін ақпараттық жүйеге сұраныс қажет. ZooSPACE платформасы үшін осыған ұқсас сұраныстар Explain қызметімен өңделуі мүмкін.

–XML өңдеу үшін алынған жазбада атаулар кеңістігінің анықтамасы жоқ. Бұл жағдайда мәліметтерді алу үшін құрылған сұранысқа сәйкес келетін XSD немесе XSD-ні ақпараттық ресурстардың атауы бойынша көрсету туралы ақпараттық жүйеге сұраныс талап етіледі.

Жоғарыда аталған жағдайлардың кез келгенінде мәліметтерді өзгертудің графикалық интерфейстерін инициализациялау үшін мыналар қажет:

–XSD ережелеріне сәйкес XML құрылымы түрінде мәліметтер схемасын сипаттау.

–алынған мәліметтерден тұратын XML құрылымы, өңдеуге арналған (жаңа

жазбаны жасау үшін қажет емес).

–Графикалық интерфейс элементтерін қалыптастыратын стильдерінің сипаттамасы (міндетті емес).

–XML өңделетін жазба элементтерінің мәндері мен XSD қолданылатын ережелерге сәйкес келетін графикалық интерфейс элементтерін құрайтын ережелерді сипаттау. Алайда, бұл ережелер XSD-ге қолданылатын XSLT түрлендіру ережелері де болуы мүмкін.

1 – суретте ZooSPACE платформасының (ZooSPACE-W) WEB серверіне орнатылған клиент-сервер архитектурасындағы адаптивті XML жазбалар өңдеушісінің алгоритмі көрсетілген. XML өңдеушісінің өзі сервер жағындағы үзік сызықпен қоршалған аймаққа сәйкес келеді. Клиент бөлігі үшін мәліметтерді енгізуге және (немесе) өңдеуге дайын HTML формасы ұсынылған. Сонымен қатар, бұл формада деректерді дұрыс енгізу үшін барлық қажетті нұсқаулықтар бар (java скрипттері), соның ішінде:

–XSD - мен сәйкес қайталануы мүмкін элементтерді көшіруге арналған скрипт.

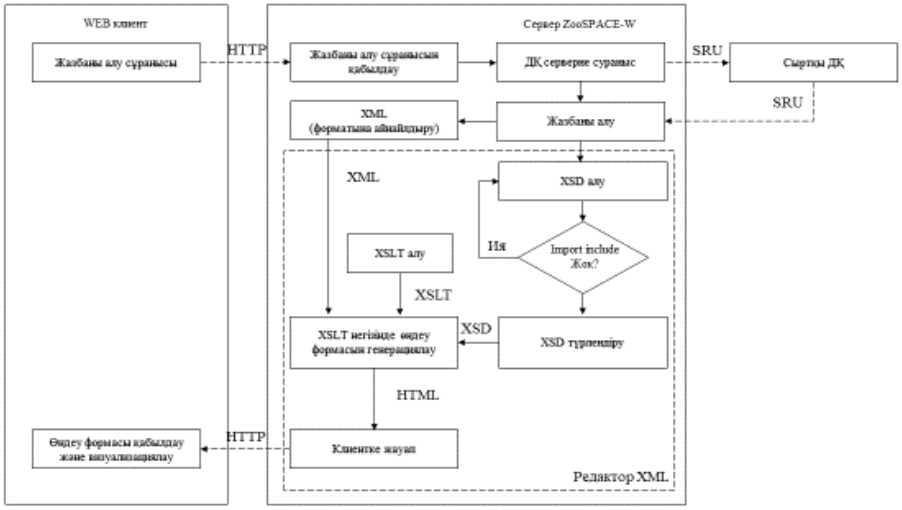
–XSD-ге сәйкес жою мүмкін болатын элементтерді жоюға арналған скрипт.

–егер XSD-де тұрақты өрнек түріндегі үлгіге (шаблон) сәйкес болса, онда мәліметтерді енгізудің дұрыстығын тексеруге арналған скрипт.

–Өңдеу формасындағы кез келген мәліметтерді жасыру-ашуға арналған скрипт.

Сонымен қатар, XSD мәліметтер схемасын анықтау ағымдағы атаулар кеңістігін (элемент xsd:include) және де басқа атаулар кеңістігін (элемент xsd:import) анықтауға көмектесетін басқа да XSD мәліметтер схемасына сілтемелері болатынына көңіл бөлу керек. Сондықтан, XSLT процессормен өңделмес бұрын бастапқы XSD құрылымы қосымша анықтамаларды ескеру үшін өзгертулерді қажет етеді.

Жоғары да айтылғандай, өңдеу формасының генерациясы өзгертілген XSD құрылымының XSLT түрлендіру әдісімен сервер жағында жүргізіледі. Сонымен бірге, алдымен XSLT процессоры жұмысын аяқтағаннан кейін, XML форматындағы жазба мәліметтерімен толтырылатын бос өңдеу формасы құрылады (мәліметтерсіз).



1 – сурет. ZooSPACE-W негізінде гетерогендік жүйедегі жазбаларды өңдеу формасын құру алгоритмі

Бос редакциялау формасын құру кезінде (2-суретті қараңыз) келесі ережелер орындалады:

–Мәліметтер схемасының идентификаторы көрсетілген жақтаулар генерацияланады.

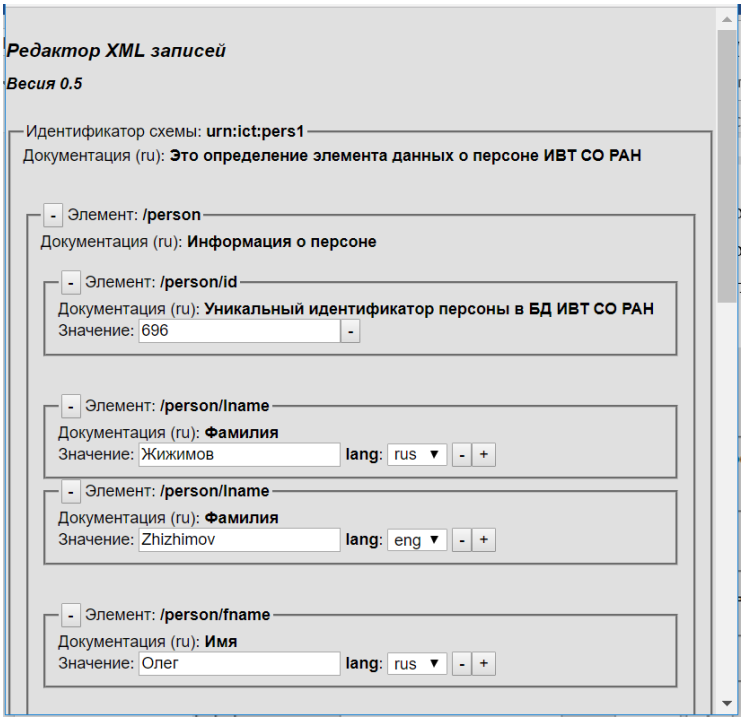
–Мәліметтер схемасына арналған құжатнама (аннотация) генерацияланады.

–XSD-де анықталған әрбір мәліметтер элементі үшін мыналар генерацияланады:

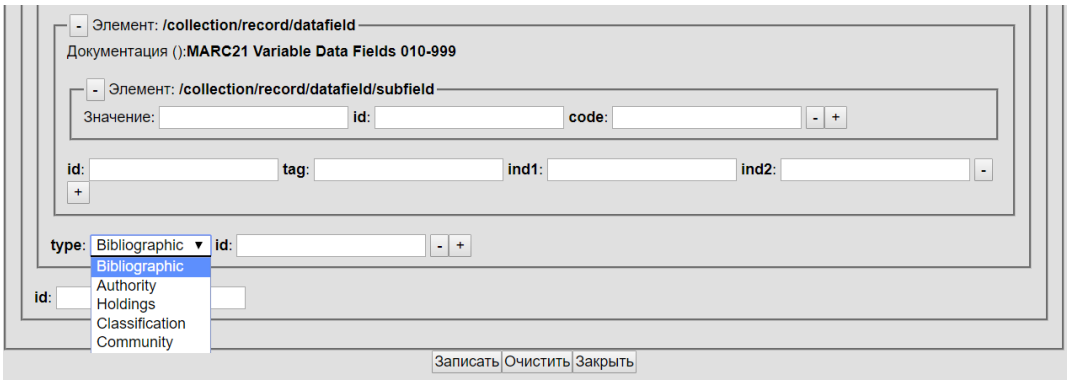
- XML жазбалар құрылымында орыны мен элементтің атауы көрсетілген жақтау;
- Өңдеу формасында элементті жасыру-ашу батырмасы;
- тілді көрсете отырып, құжаттама (аннотация);
- кірістірілген элементтер (құрылымданғандар үшін);
- элементтің мәнін енгізу жолы (қарапайым құрылым үшін);
- мүмкін болатын атрибуттардың әрбірі үшін атаулар мен мәліметтерді енгізу жолдары;
- элементті жоюға (егер рұқсат етілсе) және қайталауға (егер рұқсат етілсе) арналған батырмалар.

–Келесі батырмалар генерацияланады:

- «Записать» - өңдеу нәтижесін сақтауға арналған;
- «Очистить» - өңдеудің бос формасын қайталап генерациялауға арналған;
- «Закрыть» - өңдеу формасындағы мәліметтерді сақтамай жабуға
- арналған.



2 – сурет. XML жазбасын өңдеудің графикалық интерфейсі



3 – сурет. XML жазбасының графикалық редакторы: мәліметтерді енгізу жолы

Мәліметтерді енгізу жолдарын құру кезінде мәліметтер типі мен қойылған шектеулер ескеріледі. Атап айтқанда, элементтер мен атрибуттарға арналған енгізу жолдары XSD типті анықтамалары болған кезде ашылатын мәндер тізімі болады (3 – суретті қараңыз):

```
<xsd:simpleType name="recordTypeType">
    <xsd:restriction base="xsd:NMTOKEN">
      <xsd:enumeration value="Bibliographic"/>
      <xsd:enumeration value="Authority"/>
      <xsd:enumeration value="Holdings"/>
      <xsd:enumeration value="Classification"/>
      <xsd:enumeration value="Community"/>
    </xsd:restriction>
  </xsd:simpleType>
```

Егер XSD элементінде шаблонға көрсеткіш болса, мысалы:

```
<xsd:simpleType name="indicatorDataType" id="ind.st">
      <xsd:restriction base="xsd:string">
          <xsd:pattern value="[\da-z ]{1}"/>
       </xsd:restriction>
   </xsd:simpleType>
```

онда өңдеу формасы енгізілген мәліметтер шаблонға сәйкес келетінін тексеретін функцияны шақыруды генерациялайды.

XSD негізінде XML құруды сипаттаған тәсілде рекурсивті анықтаулар мәселесі туындайды. Рекурсивтілік тип пен атауларға сілтемелерді қолдану кезінде пайда болуы мүмкін. XSD-ді қолданатын схеманың төмендегі үзіндісі үшін

```
      <xsd:complexType name="organization">
        <xsd:sequence>
        <xsd:element name="id" type="int"/>
        <xsd:element name="name" type="string"/>
            <xsd:element name="sub-org"
            type="tns:organization"/>
  </xsd:sequence>
</xsd:complexTyp
            e>
```

```
<xsd:element name="region">
   <xsd:complexType>
   <xsd:sequence>
        <xsd:element name="id" type="int" />
        <xsd:element ref="tns:region" />
   </xsd:sequence>
   </xsd:complexType>
</xsd:element>

<xsd:element name="record">
   <xsd:complexType>
   <xsd:sequence>
        <xsd:element name="id" type="int" />
        <xsd:element name="organization"
        type="tns:organization" />
        <xsd:element ref="tns:region" />
   </xsd:sequence>
   </xsd:complexType>
</xsd:element>
```

XPath ұзындығы шектеусіз XML элементтері болуы мүмкін:

```
/record/organization/sub-org/sub-org/sub-org . .
.
/record/region/region/region/region . . .
```

Жазбаларды өңдеудің графикалық интерфейстер құру кезінде элементтердің шексіз кірістірілуін алып тастау үшін кірістірулердің санын басқаруды қолдана аласыз және оларды ағымдағы қажеттілікке сәйкес шектей аласыз.

Осылайша, ғылыми еңбектен алынған негізгі нәтижелер ретінле мыналарды көрсетуге болады:

- XML-мәліметтерді өңдеу жолдары зерттелді;
- Өңдеу құралдарын құруға арналған технология таңдалды;
- Өңдеу құралының бағдарламалық қаңқасы жобаланды;
- Мәліметтерді енгізу мен өңдеудің адаптивті моделі жасалынды;
- XML - элеметтерді HTML – формаға айналдыратын өңдеу құралы жасалынды;
- XML – енгізу мен өңдеуге арналған адаптивті моделдің негізгі принциптерін жүзеге асыратын өңдеу құралының негізгі компонеттері құрылды.

XML – жазбаларының жасалынған құралы кез келген XML – мәліметтерді импорттауға мүмкіндік береді және олардың құрылымын өзгерту тиімді әрі қарапайым, сонымен қатар өңдеудің бір ғана үрдісі бағдарламалық кодты еш өзгертпей бастапқы мәліметтерді кез келген құрылымға ауыстыруға мүмкіндік береді.

XML – жазбаларының құрылған адаптивті өңдеу құралы қазіргі кезде ZooSPACE платформасының (Ақпараттық және есептеу технологияларының Федеральдық Зерттеу орталығы, Новосибирск қаласы) ZooSPACE-W ішкі жүйесіне енгізілген. Оның функционалдық мүмкіндіктерін жоғарлату жұмыстары жүріп

жатыр, нақтырақ айтсақ, XSD және JSON элеметтерін қолдайтын тізім кеңейтілуде. Веб-сервис пен клиенттік қосымшаның жұмысын ұйымдастыру кезінде әртүрлі ортада жүзеге асыруға тағайындалған WSDL спецификациясының анықталмағандығын тудыратын таратылған жүйелердің өзара қатынасында мәселелер туындау мүмкіндігін ескеру қажет. Аталған концепцияларды жүзеге асыру әртүрлі платформалардағы гетерогенді типті ортада жұмыс жасағанда сервер мен клиент қосымшасының кепілденген өзара қатынаспен қамтамасыз етеді.

Әдебиеттер

1. Mukhitova, A., Zhizhimov, O.L.: Implementation of an adaptive model of input and editing information based on XSLT transformation for heterogeneus data. Open Semantic Technologies for Intelligent Systems, Iss. 3., 173-178, (2019)

2. Zhizhimov, O.L.: Explain Services on ZooSPACE Platform and Adaptive User Interfaces. CEUR Workshop Proceedings, Vol.1536, 30-36, (2015) http://ceur-ws.org/Vol-1536/paper4.pdf.

3. ANSI/NISO Z39.50-2003. Information Retrieval (Z39.50): Application Service Definition and Protocol Speciation. NISO Press, Bethesda, Maryland, U.S.A. Nov 2002. ISSN: 1041-5653. ISBN: 1-880124-55-6.

4. XML Schema Part 0: Primer Second Edition: W3C Recommenda-tion, http://www.w3. org/TR/xmlschema-0, Last accessed 20 Aug 2021

5. XML Schema Part 1: Structures Second Edition: W3C Rec-ommendation, http://www.w3. org/TR/xmlschema-1, Last accessed 21 Aug 2021

6. XML Schema Part 2: Datatypes Second Edition: W3C Rec-ommendation, http://www.w3. org/TR/xmlschema-2, Last accessed 22 Aug 2021

7. XSL Transformations (XSLT) Version 2.0: W3C Recommenda-tion, http://www.w3.org/ TR/xslt20, Last accessed 18 Aug 2021

8. Mukhitova, A.A., Zhizhimov, O.L.: Adaptive technologies in the context of designing administrative graphic inter-faces for heterogeneous information systems of inputting and editing data. XVI Russian conference of ”The distributed information-computational resources. Science in digital economy”(DICR-2017): Proceedings of XVI All-Russia Conference, Novosibirsk, 142-149, (2017) http://elib.ict.nsc.ru/jspui/bitstream/ICT/1467/20/paper16.pdf

9. Zhizhimov, O.L., Fedotov, A.M., Shokhin, Y.I.: The ZooSPACE platform-access organization to various distributed resources. Digital libraries. The Russian scientific e-magazine, Vol.17, No 2, ISSN 1562-5419, (2014) 10. Mukhitova, A., Zhizhimov, O.L.: Application of XML-technologies in the Construction of Input and Editing Data Model in the Adaptive Administrative Graphical Web Interfaces for Heterogeneous Information Systems. Data Analytics and Management in Data Intensive Domains: XX International Conference DAMDID/RCDL’2018, Moscow: FRC CSC RAS, 157-160, ISBN: 978-5-519-65438-8, (2018).Ковалев, А. М. Правила оформления научных докладов / А. М. Ковалев. – Москва: Издательство ВВВ, 1999. – 167 с.

ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА КРИТЕРИАЛДЫ БАҒАЛАУ АРҚЫЛЫ АҚПАРАТТЫҚ-ИНТЕЛЛЕКТУАЛДЫ ҚҰЗЫРЕТТІЛІКТІ ҚАЛЫПТАСТЫРУ

Сейсенбекова П.Б.
E-mail: ms.perizat@mail.ru
Әл-Фараби атындағы Қазақ ұлттық университетінің PhD докторанты, Қазақстан

Аңдатпа. *Бұл мақалада болашақ информатика мұғалімінің ақпараттық-интеллектуалды құзыреттілігінің құрылымы теориялық тұрғыдан негізделді. Білім алушылардың ақпараттық-интеллектуалды құзыреттілігін білім, дағды және потенциал критерийлері бойынша анықталды. Білім алушылардың ақпараттық-интеллектуалды құзыреттілігін қалыптастыру мақсатында білім беруді үш кезең бойынша қарастырылды. Студенттердің ақпараттық-интеллектуалды құзыреттілігін анықтауға арналған сұрақтар үлгісі бойынша құрылды. Болашақ информатика мұғалімдерінің ақпараттық-интеллектуалды құзыреттілігін дамыту бойынша оқыту технологиясының артықшылықтары көрсетілді және критериалды бағалау бойынша білім алушылардың білім жетістіктері бағаланды. Тәуелсіз Стьюденттің t-критерийі бойынша эксперимент жұмыстары жүргізілді.*

Кіріспе

Елбасы Нұрсұлтан Назарбаев: «Болашақ жастардың қолында екенін жиі айтып келеді. Сол себепті цифрлық Қазақстанға қол жеткізу үшін еліміздің жастарына артар үміт зор. Цифрландыру – Қазақстан Республикасының озық ел атану жолындағы басты құралы. Қазақстан 2018-2022 жылдары «Цифрлы Қазақстан» бағдарламасын іске асыруда («Цифрлық Қазақстан»мемлекеттік бағдарламасы, 2017) [1]. Осы тұрғыдан Елбасы “Төртінші өнеркәсіптік революция жағдайындағы дамудың жаңа мүмкіндіктері” атты Жолдауында: “…Жоғары білім беру ісінде жасанды интеллектпен және «үлкен деректермен» жұмыс істеу үшін ақпараттық технологиялар бойынша білім алған түлектер санын көбейту керек” деп (Н.Ә.Назарбаевтың жолдауы, 2018) [2], болашақ педагогикалық мамандардың әлемдік стандарт бойынша цифрлық технологияны жеткілікті деңгейде меңгеруі қажеттігіне аса мән берген.

COVID-19 әлемдік деңгейде бағытты, ойды, ойлауды өзгертуге, әсіресе, білім саласындағы аудиториялық міндетті оқу орнының монополиялық басымдығын қашықтықтан оқыту форматына ауыстыруға мәжбүрледі. Оқшаулаудың енгізілуі білім беру жүйесіне кейбір өзгерістер енгізді, яғни, сабақтар қашықтықтан өткізілді. Ал ауысу өте тез, бейімделу қабілеті төмен болғандықтан, туындаған көптеген мәселелер болды. Қашықтықтан оқу форматына көшу ерекше жағдайларға байланысты болғанымен, оның оң нәтижелері де бар. Біріншіден, студенттер білімді өздерінің қажеттіліктері мен жеке қасиеттерін ескере отырып, өз бетінше іздеуге, алуға дағдылана бастады. Көптеген оқу орындары қол жетімді қосымшаларды пайдаланады, Google Hangouts немесе Zoom арқылы сабақтар өткізеді, сонымен қатар оқуға интерактивті жұмыс парақтары мен бейне сабақтар жібереді. Студенттер

өз жобаларын Google Classroom, Zoom, Google Meet және т. б. сияқты көптеген қосымшалар арқылы әріптестерімен талқылайды.

Цифрлық оқыту АКТ элементтерін қамтиды, мысалы, қашықтан үйлестіру, электрондық пошта, вебинарлар және эфирлік сабақтар, интеллектуалды дауыстық жауап жүйесі және т.б. Бірте-бірте бүкіл әлемде цифрландыру жүріп жатыр, және білім беру жүйесі-бұл сандық технологиялардың ең үлкен бағыттарының бірі (Магомадов В. С., 2019) [3].

Зерттеу әдістері

Білім алушылардың ақпараттық-интеллектуалды құзыреттілігін қалыптастыру мақсатында біз білім беруді 3 кезеңге бөліп қарастырдық.

Бірінші кезең «Білім» «Мен не үшін және қалай істейтінімді білемін»

Білім алушылардың «Білім» кезеңінде ақпараттық-интеллектуалды құзыреттілігін қалыптастыру үшін келесі***: білімнің ұтқырлығы, икемділік әдісі*** және ***сыни ойлау*** критерийлерін қарастырдық. Бұл кезең дәріс және семинар сабақтарды қамтиды.

Екінші кезең «Дағды» (Мен жасай аламын және жасаймын)

«Интеллектуалды іс-әрекеттің» екіінші кезеңінде ситуациялық тапсырманы орындау үшін студенттер орындау деңгейін ақпараттық, импровизациялық, эвристикалық деп бөліп, ***ақпараттық деңгейге*** зертханалық жұмысты, ***импровизациялық деңгейге*** студенттің оқытушымен өзіндік жұмысын (СОӨЖ) және ***эвристикалық деңгейге*** студенттің өзіндік жұмысын (СӨЖ) орындауын қарастырдық.

Үшінші кезең «Жоба» (Мен жасай алатын жобалар)

Тақырыпты игеру және оны зерттеу шеңберінде ситуациялық тапсырманы орындау бойынша болашақта жасалатын жобаларын ұсыну. (P. Seisenbekova, A. Shayakhmetova and M. Othman, 2019) [4]

Желілік технологияларды қолданумен цифрлы білім берудің типтік ерекшеліктері - бұл икемділік, ұтқырлық, өндіріс қабілеттілігі, диалогтық және интерактивтілік, медиа ағындарды қабылдауға бағдарлау. Осының барлығы ақпараттық-интеллектуалды құзыреттілікті қалыптастыруға ықпал етеді (Филимонова О.В., 2016) [5].

Интеллектуалды оқыту ортасы ең алдымен оқытушы мен білім алушыға үлкен еркіндік береді. Бұл екеуінің де тұлғалық мүмкіндіктерін жүзеге асыруына қолайлы. Тұлға болып қалыптасуына қолайлы. Тұлға деген өз-өзіне нақты мақсат қойып, өздігінен жүйелі әрекет ете алатын, өз әрекетіне өзі жауап бере алатын адам. Тұлға деген адами да, кәсіби де деңгейі өте жоғары, толыққанды өмір сүретін адам (Носкова Т. Н., Павлова Т. Б., Яковлева О. В., 2018) [6].

Әдебиеттерге шолу

Құзыреттілік түсінігі көп қырлы әртүрлі ұғымды білдіреді. Қандай да бір жаңа дүние пайда болса оның міндетті түрде құзыреттілігі болады деген тұжырым жасауға болады. (Derek Bok. 2021) [7].

Елімізде оқушылардың ақпараттық құзырлылықтарын қалыптастырудың теориялық негіздері туралы К.С.Құдайбергенова, студенттердің ақпараттық құзырлылық негіздерін қалыптастырудың педагогикалық шарттары туралы С.Н.Исабаеваның, оқушылардың құзырлылығын қалыптастырудағы ақпараттық технологиялардың орны мен маңызы жайлы Е.Ы.Бидайбеков, Г.Б.Камалова, Б.Д.Сыдыков, Ж.А.Қараевтың, С.М. Кеңесбаев, С.Т.Мұхамбетжановаңың зерттеу жұмыстарынан көруге болады.

Оқу процесінде білім алушылардың интеллектуалды және тұлғалық дамуының өзара байланысының идеялары К.А. Абулханова-Славская, Б.Г. Ананьева, О.К. Тихомирова еңбектерінде кездеседі. Жалпы жеке тұлғаның дамуында интеллектуалды қабілеттерінің рөлі ерекше екендігі мына ғалымдардың еңбектерінде көрсетілген Ж.Пиаже, В.Н. Дружинин, М.И. Дьяченко, Л.А. Кандыбович, А.Н. Леонтьев және т.б.

Ресей ғалымдары: Л.Е.Панфилова, Т.Е.Матвеева, С.А.Сапон, И.В.Фролова, О.В.Филимонова өз еңбектерінде ақпараттық-интеллектуалды құзырлық ұғымына анықтама бере отырып, мектеп оқушыларының ақпараттық-интеллектуалды құзыреттілігін қалыптастыруды қамтамасыз ететін дамып келе жатқан білім беру жүйесін теориялық және эксперимент түрінде негіздеген.

«Құзыреттілік – белгілі бір пәнді оқыту процесінде қалыптасқан білім, дағды, ептілік жиынтығы, сондай-ақ, белгілі бір іс-әрекетті жүзеге асыруға қабілеттілік. Алғашында бұл ұғым тіл үйренуге қатысты пайда болған (Anamova R., 2020) [8].

Л.Г.Панфилова, С.А.Сапон және Т.Е.Матвеева өз еңбектерінде ең алғаш болып ақпараттық-интеллектуалды құзырлық ұғымына анықтама бере отырып, мектеп оқушыларының ақпараттық-интеллектуалды құзыреттілігін қалыптастыруды қамтамасыз ететін білім беру жүйесін теориялық және эксперимент түрде негіздеген болатын. Яғни, ақпараттық-интеллектуалды құзыреттілік - оқу-танымдық іс-әрекеттегі мәселелер мен міндеттерді дұрыс шешу үшін алынған ақпаратты тиімді пайдалану деп көрсеткен (Панфилова Л.Г., Матвеева Т.Е., Сапон С.А., 2013) [9].

Зерттеу нәтижелері және оларды талдау

Эксперименттік зерттеуге Абай атындағы Қазақ Ұлттық университетінің 3-курс ИОК 181 тобының бірінші топша студенттерінің 8 студенті эксперимент тобы ретінде, екінші топшасындағы 8 студент бақылау тобы ретінде алынды. Барлығы 16 студент эксперимент жұмысына қамтылды. Ол педагогикалық эксперименттің толыққанды, табиғи өтуіне мүмкіндік берді. Эксперимент шеңберінде нәтижелер мен қорытындыны дұрыс бағалау үшін ықтимал-статистикалық әдістер неғұрлым тиімді болды.

Эксперимент барысында эксперимент тобы және бақылау тобының студенттері оқу жетістіктерін критериалды бағалау бойынша ақпараттық-интеллектуалды құзыреттіліктерін салыстыру үшін тәуелсіз Стьюденттің t-критерийін қолданып есептейміз.

Қадам 1. 1-кесте – Эксперимент және бақылау топтарының мәндерін енгіземіз.

ИОК 181 Эксперимент тобы		ИОК 181 Бақылау тобы	
Аты-жөні	Балл	Аты-жөні	Балл
1. Мамытбек Әйгерім	93	Мустафин Сабыржан	76
2. Ергеш Нұрсұлтан	83	Сартаева Гүлімай	65
3. Есіркеп Сәния	91	Сагидуллаева Айнура	80
4. Жанболатұлы Нұрдос	88	Сүлейменқан Асема	76

5. Қасым Айдана	91	Тасубайұлы Асылбек	81
6. Қуанышбек Бекжан	96	Тасқұл Лаура	83
7. Көшербаев Нұржан	81	Тұрдалы Сандуғаш	50
8. Орынбасар Ұлданай	76	Сатбай Бакдаулет	45

Қадам 2. Тәуелсіз топтарға арналған **Стьюденттің t-критерийі** екі тәуелсіз топтардың орташа мәндерін салыстыру үшін қолданамыз

Тәуелсіз топтарға арналған Стьюденттің t-критерийі:

$$t_e = \frac{|M_1 - M_2|}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}$$

мұндағы M_1— бірінші топтың орташа арифметикалық мәні; M_2— екінші топтың орташа арифметикалық мәні; σ_1—бірінші топтың стандартты ауытқуы; σ_2— екінші топтың стандартты ауытқуы; n_1— бірінші топтағы студенттердің саны; n_2— екінші топтағы студенттердің саны.

Қадам 3. Орташа арифметикалық - бұл үлестірімдегі барлық мәндердің олардың санына бөлінген жиынтығы. **Орташа арифметикалық** ортыны мына формуламен анықтаймыз.

$$M_x = \frac{\sum x_i}{n}$$

$$M_1 = \frac{93 + 83 + 91 + 88 + 91 + 96 + 81 + 76}{8} = 87{,}38$$

$$M_2 = \frac{76 + 65 + 80 + 76 + 81 + 83 + 50 + 45}{8} = 69{,}5$$

Қадам 4. Стандартты ауытқу - дисперсияның оң квадрат түбірі.

Стандартты ауытқудың формуласы:

$$\sigma_x = \sqrt{D_x} = \sqrt{\frac{\sum (x_i - M_x)^2}{n - 1}}$$

$$\sigma_1 = \sqrt{45{,}98} = 6{,}78$$

$$\sigma_2 = \sqrt{215{,}71} = 14{,}68$$

Қадам 5. 2-кесте – тәуелсіз топтарға арналған Стьюденттің t-критерийі бойынша есептеу жүргіземіз.

№	Эксперимент (Э) және Бақылау (Б)	Орташа мәннен ауытқу	Квадратты ауытқу

	топтарының алған баллдары					
	Э.1	Б.2	Э.$x_i - M_1$	Б. $x_i - M_2$	Э.$\sqrt{D_1}$	Б.$\sqrt{D_2}$
1	93	76	5.62	6.5	31.5844	42.25
2	83	65	-4.38	-4.5	19.1844	20.25
3	91	80	3.62	10.5	13.1044	110.25
4	88	76	0.62	6.5	0.3844	42.25
5	91	81	3.62	11.5	13.1044	132.25
6	96	83	8.62	13.5	74.3044	182.25
7	81	50	-6.38	-19.5	40.7044	380.25
8	76	45	-11.38	-24.5	129.5044	600.25
Қосындысы:	699	556	-0.04	0	321.8752	1510
Орташа мәні:	87.38	69.5				

$$t_e = \frac{\lfloor 87{,}38 - 69{,}5 \rfloor}{\sqrt{\frac{6{,}78^2}{8} + \frac{14{,}68^2}{8}}} = \frac{17{,}88}{5{,}72} = 3{,}1$$

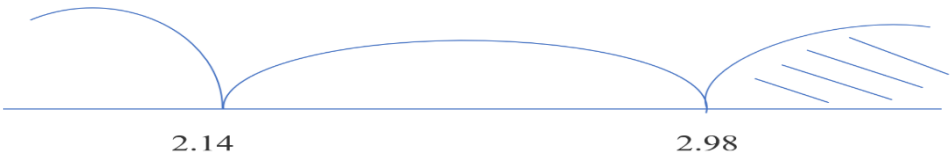
Нәтижесі: $t_e = 3.1$

Қадам 6. Қорытынды жасаймыз.

Тәуелсіз топтарға арналған Стьюденттің t-критерийі $t_e = 3.1$ ке тең және кестедегі Стьюденттің t-критерийі мәні p = 0,05 бойынша

3-кесте – Сындарлы мәндер:

$t_{см}$	
p≤0.05	p≤0.01
2.14	**2.98**



Маңызды емес аймақ ***Маңызды аймақ***

1-сурет – маңыздылық осі:

Алынған t (3.1) эмпирикалық мәні маңызды аймақта. Сондықтан, екі статистикалық топтың орташа арифметикалық шамалары арасындағы айырмашылық статистикалық мәнді болып табылады. Алынған нәтижелер экспермент тобындағы білім алушылардың оқу жетістіктерін критериалды

бағалаудың мотивациялық көрсеткіштерінің жоғары дамығанын көрсетеді. Сонымен қатар, эксперименттік зерттеу жұмысына жүргізілген математикалық-статистикалық талдау нәтижесі дамытушы эксперимент барысындағы эксперименттік және бақылау тобындағы алынған нәтижелердің орташа арифметикалық шамалары арасындағы айырмашылықтардың статистикалық мәнділігін көрсетті. Зерттеу барысында алынған нәтижелерден эксперименттік жұмыстың тиімділігі және қойылған болжамның расталғандығы жайлы бекітуге болады.

Қорытынды

Болашақ информатика мұғалімдерінің ақпараттық-интеллектуалды құзыреттілігін қалыптастыру үшін білім беруді цифрландырудың мүмкіндігі зерттелді. Болашақ информатика мұғалімдерінің білім беруді цифрландыру жағдайындағы ақпараттық-интеллектуалды құзыреттілігін қалыптастырудың жалпылама алгоритмі жасалды. Болашақ информатика мұғалімдерінің ақпараттық-интеллектуалды құзыреттілігін дамыту бойынша оқыту технологиясының артықшылықтары көрсетілді және критериалды бағалау бойынша білім алушылардың білім жетістіктері бағаланды. Тәуелсіз Стьюденттің t-критерийі бойынша эксперимент жұмыстары жүргізілді. Зерттеу барысында алынған нәтижелерден тәуелсіз Стьюденттің t-критерийі бойынша эксперименттік жұмыстың тиімділігі және қойылған болжамның расталғандығы бекітілді.

Әдебиеттер

1. «Цифрлық Қазақстан»мемлекеттік бағдарламасы. http://mic.gov.kz/kk/pages/cifrlyk-kazakstanmemlekettik-bagdarlamasy. 2017 жылғы 12 желтоқсан.

2. Қазақстан Республикасы Президенті Н.Ә.Назарбаевтың “Төртінші өнеркәсіптік революция жағдайындағы дамудың жаңа мүмкіндіктері” атты Жолдауы. 2018 жылғы 10 қаңтар. http://www.akorda.kz/kz

3. *Магомадов В. С.* Использование технологии AR как инструмент образования // В сборнике: Современная мировая экономика: проблемы и перспективы в эпоху развития цифровых технологий и биотехнологии. 2019. С. 184-185.

4. *P. Seisenbekova, A. Shayakhmetova and M. Othman,* The Use of The Bayesian Approach in the Formation of The Student's Competence in the ICT Direction. 2019 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2019 - Proceedings 2019. С. 85-90. DOI:10.1109/I2CACIS.2019.8825060

5. *Филимонова О.В.* Разработка технологии формирования информационно-интеллектуальной компетентности студентов технического вуза // Современные проблемы науки и образования. – 2016. – № 4.; URL: http://www.science-education.ru/ru/article/view?id=24816.

6. *Носкова Т. Н., Павлова Т. Б., Яковлева О. В.* ИКТ-инструменты профессиональной деятельности педагога: сравнительный анализ российского и европейского опыта // Интеграция образования. - 2018. - Т. 22, № 1. - С. 25-45.

7. *Derek Bok.* Improving the Quality of Education. 2017. https://www.insidehighered.com/views/2017/09/21/how-improve-quality-higher-education-essay [16.01.2021]

8. *Anamova R., Bykov L., Kozorez D.* Algorithm for Designing Professional Retraining Programs Based on a Competency Approach // Journals Education Sciences. 2020. 10(8). 1-9.

9. *Matveeva T.E., Sapon S.A., Panfilova L.G.* Technology for the development of information and intellectual competence - a modern means for the implementation of the requirements of the Federal State Educational Standard in school education // Scientific and methodological electronic journal "Concept". - 2013. - Т. 5. - P. 116–120. - URL: http://e-koncept.ru/2013/54024.htm.

MATHEMATICAL MODELING OF BIOREACTOR PROCESS CONTROL

Shakerkhan K. O., Meshechkin V. V.
e-mail: kapan-shakerkhan@mail.ru
Kazakh Humanitarian and Law Innovation University, Kazakhstan

Annotation. *This article presents a comparison of biogas plants for waste processing of various modifications, advantages and disadvantages, as well as a description of a biogas plant of its own design of a horizontal type, taking into account the local climatic and economic conditions of the development of farms in Kazakhstan. The article discusses the use of our patented pneumatic motor for mixing bio-waste, a bioreactor of our own production and describes the analysis of the development of biogas technologies in the countries of the far and near abroad. The analysis of the mathematical model is carried out. Several directions of mathematical modeling of anaerobic digestion processes are considered. Such models based on the equations of chemical reactions, scientific works of Buswell, Muller, Boyle, etc. Models based on empirical dependencies, the work of Safili, Westerman. Models based on kinetic dependencies, on the concentration of the substrate and cells, on the inhibition process, for example, the work of Mono, Konto, Moser, Chen and Hashimoto.*

Keywords: *biomethane, biogas plant, bioreactor, biowaste, mathematical modeling, regression analysis, correlation*

In many countries, much attention is paid to the problem of obtaining and using biogas. In a short time, a whole industry for the production of biogas has emerged in many countries of the world. China is the leader in the development of the biogas industry. Since the mid-70s of the XX century, a National program for obtaining biogas from animal waste has been operating in this country. Currently, there are 10 million farm methane tanks in operation. In addition, there are 40,000 biogas plants operating in China, 24,000 treatment plants producing biogas, which ensures the operation of 190 power plants. China is an exporter of biogas and engines based on it.

The European Commission has identified bioenergy as an independent direction of common energy, which was confirmed at the Pan-European Conference on Bioenergy in October 2003 in Budapest.

The main advantages of biogas are its renewability, the availability of local sources of raw materials for fuel production, reducing the greenhouse effect and environmental damage from organic waste collection systems, providing an environmentally closed energy system. Table 1 shows data on the production of biogas in the world. [1, 2, 5, 9]

Table 1. Biogas production in the world

Country	**The volume of biogas production per year, million m^3**	**The total capacity of the biogas-powered plant Mwt**
USA	500	200
Great Britain	200	80
France	40	16

Russia	58	-
Qazaqstan (potential opportunities)	15	-

The table shows that in the United States, currently, the annual volume of biogas production is 500 million m^3. A significant part of it goes to power plants. The total electric capacity of biogas-powered plants is about 200 Mwt.

There are more than ten large biogas plants operating in the United States, one of which (with three feedlots for 110 thousand heads) supplies the produced biogas to the gas distribution network of Chicago. In addition, installations for using waste on small cattle farms with a cattle population of up to 150 heads have become widespread in the United States.

In the UK, about 200 million m^3 of biogas is produced per year. The total capacity of the UK's bioelectric power plant is about 80 Mwt.

France produces about 40 million m^3 of biogas per year. At one of the landfills near Paris, a bio-power plant was built using biogas, the emission of which is 1.5 thousand m^3 per day.

Germany is the leader in the production of biogas in Europe. The country aims to reduce carbon dioxide emissions by 40% and phase out nuclear energy by 2020. The government's acts, which set out strategies to reduce emissions, include national goals for the production of biomethane – 6 billion cubic meters of gas per year until 2020 and 10 billion cubic meters of gas per year. Cubic meters per year by 2030. In this regard, a further significant expansion of German biogas production is expected.

The Danish government provides significant tax incentives for biogas producers: about 20% of capital investments for centralized biogas and 30% for individual plants or installations. The total annual energy capacity of Danish biogas producers, obtained from all sources, is currently up to 4PJ. It is planned to further increase its production to 6PJ. Currently, there are 18 biogas plants in operation in Denmark, capable annually processing 1.2 million tons of biomass (75% of animal waste and 25% of other organic waste), giving up to 45 million m^3 of biogas, which is equivalent to 24 million m^3 of natural gas. [1, 2, 3, 5, 11]

There is no national program to support the construction of biogas plants in Russia, nor is there a single centralized biogas plant. At the same time, there are models of small biogas plants of domestic production on the domestic market, intended for use in personal subsidiary and farm farms.

The Factor Ltd Company (Moscow) has developed and implemented a prototype of a biogas plant at the Balakhninskaya poultry farm (Nizhny Novgorod region). With a reactor capacity of 5 m^3, it is able to process 1 ton of manure per day and produce up to 60 m^3 of biogas. In the near future, the company is ready to start mass production of biogas plants with reactors with a capacity of up to 500 m^3.

JSC "Center "EcoRos" in 1994, at the livestock complex of cattle "Poyarkovo", JSC "Agrofirma "Iskra" of the Solnechnogorsk district of the Moscow region, an autonomous power unit-module BIOEN1 for waste processing of 20-25 heads of cattle was put into operation (Figure 1). [2, 4, 18]

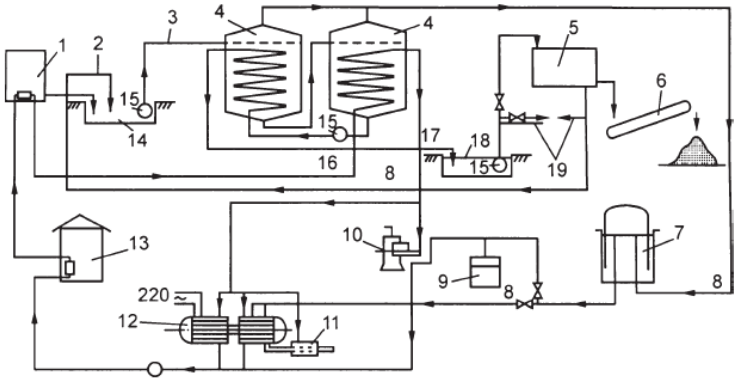


Fig. 1. Technological scheme of an autonomous bioenergetics block module BIOEN-1 is equipped with four digesters with a total capacity of 8.8 m3, four tanks with "wet" type - 12 m3, electric power 4 kW (based on commercially available generator AB-4T/400-M2 Viazemsky electromechanical plant of Smolensk region, documentation of JSC "Agrodizel", Moscow), the heating gas fired unit boilers-23, 2-1 heat capacity of 23 kW, commercially available Zhukovsky machine-building plant (Zhukovsky town of Moscow region), flameless infrared gas burner heat output 5 kW household gas stoves.

The biogas industry is also developing in Kazakhstan, although it cannot yet compete with other areas of renewable energy. Nevertheless, the share of biogas energy in 2019 amounted to 18 million kWh or 0.75% of all RES electricity. This energy was generated by three biogas plants (BGS) with a total capacity of 2.42 MW, which are monitored by the Ministry of Energy of the Republic of Kazakhstan on a quarterly basis. Since this year, this list includes another BGS-Water Resources-Marketing LLP with an installed capacity of 0.4 MW at the sewage treatment plants of Shymkent. Thus, according to the Ministry of Energy, 2.82 MW of biogas capacity will be monitored in 2020. One of those included in the list – a 1 MW biogas station built from railway tanks – belongs to the Karaganda agro-industrial complex "Volynsky" LLP. The raw material for its operation is pig farm waste; the generated electricity supports the operation of the fish shop of the complex. The biogas plant for 0.35 MW of “Karaman-K” LLP is located in the Kostanay region and operates on the waste of a cattle farm; the generated electricity is directed to its own needs. The development of the project and delivery of the equipment of this station was carried out by LLC "Zorg biogas Ukraine". The same supplier provided similar services to Karaganda LLP "Agrofirma Kurma" for the construction of BGS with a capacity of 1.07 Mwt. [6, 8]

Currently, biogas plants with various design and technological features have been developed. There are industrial and artisanal installations. Industrial installations differ from artisanal ones by the presence of mechanization, heating systems, homogenization, and automation. Types of biogas plants are classified according to the methods of loading raw materials, methods of collecting biogas, according to the materials used for their construction, the use of additional devices, the horizontal or vertical location of the reactor, underground or ground construction. Two-stage and one-stage biogas complexes are used. The single-stage technology is used for most substrates and such a technology can be considered basic. According to the number of stages of the installation process, there are

single-stage, two-stage and multi-stage. Single-stage installations consist of a single bioreactor, in which the complete fermentation of biomass takes place. In two-stage systems, the process takes place in the main fermentation bioreactor and in the final fermentation and sludge deposition reactor. Multi-stage systems include a different number of basic fermentation bioreactors and fermentation reactors.

According to the operating mode, continuous, semi-continuous and periodic installations can be distinguished.

Batch plants consist of a single bioreactor, which is fully loaded with the initial substrate, and then completely emptied after a certain time of the process. In semi-continuous mode installations, the process of obtaining biogas takes place in two or more reactors that operate in turn.

In the continuous mode, the substrate is fed into the bioreactor continuously or at short intervals, while the corresponding volume of the fermented substrate is removed. Installations operating in continuous mode are characterized by stability and high performance compared to other modes.

According to the position of bioreactors, there are vertical, horizontal and inclined locations. The choice of the reactor location depends on the operating mode and the availability of free territory. In our case, we use a bioreactor of a horizontal type, semi-underground location with a continuous operation mode. Such a bioreactor allows you to save energy on mixing and keep warm in cold weather conditions.

In biogas plants, bioreactors of oval, cylindrical and cubic shapes are used. Our proposed bioreactor is a single-stage, cylindrical tank. Cylindrical tanks are much more effective in reducing the energy consumption for mixing, unlike oval and cubic ones, which is confirmed by most laboratory studies.

Also, biogas plants are distinguished by the method of heat supply and the method of mixing. The heat supply necessary for the process can be carried out in direct and indirect ways. For our bioreactor, we use an indirect method, since the direct method is performed directly by supplying hot water or steam under pressure to the fermentation mass. To heat the biomass in this way, the installation of a steam generating system is required, which leads to additional costs. In addition, when steam or water is supplied, an uneven temperature distribution occurs in the reactor, resulting in overheating of the biomass [10].

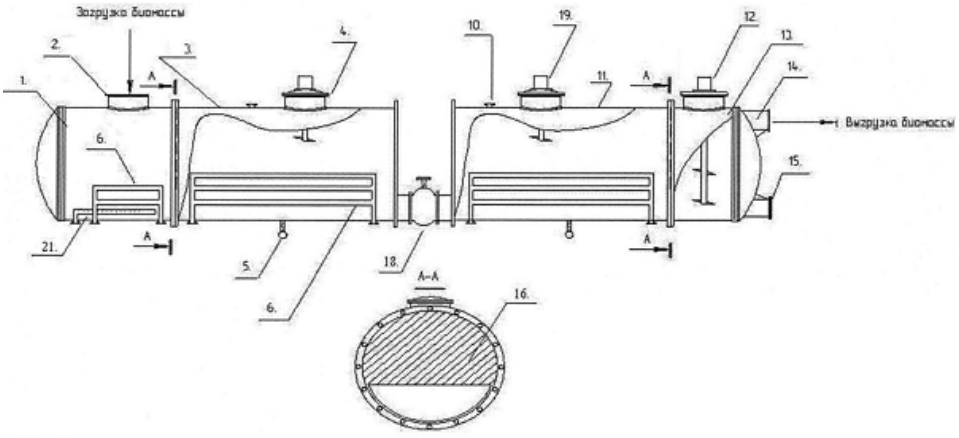


Fig. 2. Diagram of the simplest biogas horizontal installation

Biogas plant (see fig. 2) offered by us for small farms. The reactor volume is from 16 m3, designed for processing 500-1000 kg of manure per day. The plant contains several components to ensure the processing of manure and the production of biofertilizers and biogas. And it works in a mesophilic temperature regime from 20 ° C to 35 ° C. The biogas produced by the plant is immediately sent for use in power plants. The processed mass is removed from the reactor through the discharge pipe at the time of loading the next portion of raw materials or due to the pressure of biogas. The discharged fermented mass falls into a temporary storage tank, which should be at least the volume of the reactor [7, 8].

For the reality of Kazakhstan, taking into account economic and climatic factors, we have invented a domestic bioreactor. The bioreactor, made of a tubular shape, is located horizontally and is divided into three sections: loading, working and unloading, the working section consists of one or more modules, in each module of the working section there are mounted agitators with a drive and a heat exchanger, characterized in that each module is equipped with a float device in which a stirrer with a drive is mounted with the possibility of rotation relative to the horizontal axis, and in the upper part of each module a trolley with a drive is installed on horizontal guides, to which a float device is connected (integrated) by means of vertical rods (see fig. 3).

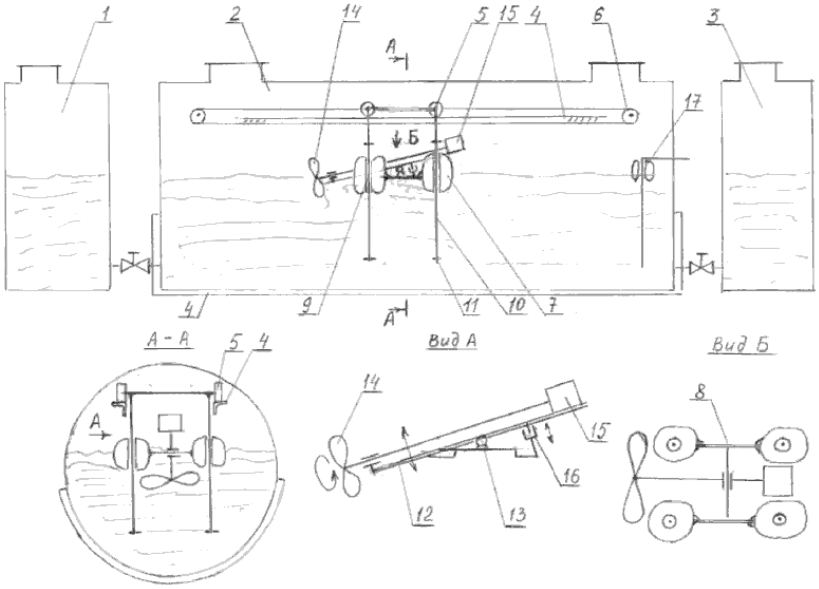


Fig. 3. A horizontal bioreactor with a float mixing device on a pneumatic motor operating on compressed air.

Технический результат достигается за счет того, что в конструкцию биореактора вводится дополнительный элемент в виде поплавкового устройства, в которое монтируется мешалка с приводом, с возможностью перемещения вдоль биореактора и поворота относительно горизонтальной оси в вертикальной плоскости [6, 7].

На рисунке 5 изображен биореактор с одним модулем:
1 - загрузочный сектор;
2 – рабочий сектор (модуль);
3 – разгрузочный сектор;

4 – теплообменная рубашка;
5 – тележка;
6 - привод тележки;
7 - поплавок;
8 – горизонтальные тяги;
9 – втулки;
10 – штанга вертикальная;
11 – ограничители;
12 – рычаг;
13 – ось рычага;
14 – мешалка;
15 – привод мешалки;
16 – гидро (пневмо) цилиндр;
17 – датчик уровня.

Биореактор состоит из трех секций: загрузочной 1, рабочей 2 и разгрузочной 3 (рисунок 5).

Рабочая секция может состоять из нескольких модулей. Модуль в нижней части имеет теплообменную рубашку 4.

В каждом модуле в ее верхней внутренней части смонтированы тележка 5 с приводом 6. Внутри каждого модуля на поверхности биомассы располагается поплавковое устройство, состоящее из поплавков 7 жестко скрепленных между собой горизонтальными тягами 8, при этом каждый поплавок 7 посредством втулок 9 подвижно встроен в вертикальную штангу 10. Вертикальные штанги 10 снабжены ограничителями 11перемещения поплавков 7 вдоль штанг.

На горизонтальных тягах 8 поплавкового устройства на рычаге 12 с осью 13 смонтирована мешалка 14 с приводом 15. Рычаг 12 снабжен гидро (пневмо) цилиндром 16. Для контроля уровня биомассы внутри каждого модуля имеется датчик уровня 17 электрически связанный с системой управления гидро (пневмо) цилиндром 16.

Перемешивание биомассы в каждом модуле происходит следующим образом.

Мешалка 14 с приводом 15, установленная на поплавковом устройстве, перемешивает биомассу по всей длине модуля, перемещаясь вдоль нее посредством тележки 5, которая может двигаться, например, с помощью трособлочного привода 6. Вертикальные штанги 10 обеспечивают устойчивое перемещение поплавкового устройства вдоль модуля. Ограничители 11 не позволяют поплавковому устройству опуститься ниже критической отметки, при которой мешалка могла бы задевать стенки модуля.

Мешалка 14 с приводом 15, проворачиваясь с помощью гидро (пневмо) цилиндра 16 относительно горизонтальной оси 13 позволяет перемешивать биомассу по всей высоте модуля.

Угол поворота рычага 12 с размещенной на ней мешалкой 14 с приводом 15 относительно горизонтальной оси 13 координируется в зависимости от уровня биомассы в рабочей секции 2 с помощью датчика уровня 17.

Таким образом, изобретение позволяет повысить качество перемешивания биомассы по всему объему модуля биореактора, сократить энергозатраты на его работу. А подземное расположение предусматривает горизонтальную конструкцию биореактора из-за очевидно меньших материальных затрат по сравнению с малой надежностью и неэффективностью маловысотной вертикальной конструкции.

Кроме того, по нашим предварительным расчетам, железобетонная конструкция в условиях Казахстана оказывается в 1,5-2 раза дешевле стальной.

В результате анализа рынка биогазовых установок нами были установлено следующее: в Казахстане на сегодняшний день нет предприятий, выпускающих биогазовое оборудование (а тем более комплексы). Зарубежное оборудование очень дорогое, его не могут позволить себе купить даже относительно крупные фермерские хозяйства (около 1000 голов КРС). Например, стоимость биогазового комплекса в Костанайской области составила 400 млн. тенге, то есть более 1 млн. долларов США для фермерского хозяйства, где в наличии порядка 1000 голов к.р.с. Важно заметить, большинство поставщиков БГУ за рубежом, включая РФ, как и индивидуальные предприниматели в РК [19], широко рекламируют и продают БГУ (причём дорого, около 1300 долларов США за 1 $м^3$ биореактора), не включая в комплект такое важное и необходимое для нормального осуществления технологического процесса оборудование как измельчитель сырья. Измельчители нашей разработки [3] эффективны, практичны и недороги в сравнении с зарубежными аналогами (например, германский измельчитель средней производительности имеет стоимость порядка 13000 евро). Также не включаются в комплект в большинстве случаев система очистки биогаза и другое оборудование. Кроме того, часто встречаются БГУ с неэффективным энергопотреблением перемешивающего устройства (до 3,4 кВт на 1 $м^3$ объёма биореактора). [13, 14]

На этом фоне предлагаемая разработка биореактора представляется действительно эффективной и максимально учитывающей экономические и климатические особенности региона.

Наличие оптимальной и адекватной математической модели позволяет оценить анаэробный процесс переработки отходов со всех его сторон, без проведения полномасштабных экспериментов, где соблюдаются пределы указанных и принятых ограничений. Актуальной задачей математического моделирования процесса метаногенеза является разработка универсальной модели, которая могла бы учитывать все параметры и факторы, связанные с процессом анаэробного брожения субстрата.

К настоящему времени математическое моделирование процесса анаэробного сбраживания рассматривается в нескольких направлениях.

Основой первого направления являются модели, основанные на уравнениях химических реакций. К ним относятся работы Басвелла, Мюллера, Бойля и других. Например, Басуэлл и Мюллер берут модель в качестве основы для определения количества произведенного биогаза в зависимости от исходного субстрата, а именно от химического состава:

$$C_n H_a O_b + (n - \frac{a}{4} - \frac{b}{8}) H_2 O \leftrightarrow \left(\frac{n}{2} - \frac{a}{8} - \frac{b}{4}\right) CO_2 + \left(\frac{n}{2} + \frac{a}{8} - \frac{b}{4}\right) CH_4 \quad (1)$$

где, $C_n H_a O_b$ - органическое вещество, H_2O - вода, CO_2 - углекислый газ, CH_4 - метан, a, b, n – безразмерные коэффициенты

Второе направление состоит из моделей, основанных на эмпирических зависимостях. В тоже время эти модели не учитывают параметры, которые влияют на конечный выход биогаза, и поэтому не раскрывают подробно процесс разложения органического вещества. Работы Сэфили и Вестермана предлагают эмпирическую

зависимость выхода метана от температуры анаэробного сбраживания отходов в психофильном режиме:

$$CH_4 = 0{,}216 + 0{,}00934 * T \quad (2),$$

где CH_4 – выход метана, $м^3/кг$, Т – температура процесса сбраживания, ^0C.

Третье направление включает модели, основанные на кинетических зависимостях моделей Моно и Конто. Моно описывает процесс анаэробного разрушения ферментированного субстрата в зависимости от удельной скорости роста микроорганизмов:

$$\mu = \mu_M \frac{S}{K_s + S} (3)$$

где, $\mu_м$ – максимальный удельный темп роста микроорганизмов, $сут^{-1}$; K_S – константа Моно, при которой темп роста составляет 0,5 от максимума.

На основе модели Моно Эндрюс, Мозер и другие разработали свои модели. В их работе также описывается выход биогаза в зависимости от концентрации субстрата, но с введением дополнительной функции в формулу как ингибирование у Эндрюса и с введением сигмоидального фактора в Мозер. Вышеприведенные формулы являются лишь частью, которая характеризует биологическую фазу:

$$\frac{dx_1}{dt} = \frac{F}{V}(X_0 - X_1) + \mu * X_1 - k_T * T_{x1} (4)$$

$$\frac{dS_1}{dt} = \frac{F}{V}(S_0 - S_1) - \frac{\mu}{Y_{\frac{X}{S}}} * X_1 (5)$$

$$\mu = \frac{\mu_{XX}}{1 + \frac{K_S}{HS} + \frac{HS}{K_1}} (6)$$

где X_0, X_1 – концентрация микробной популяции на входе и на выходе соответственно, $кг/м^3$; F,V – скорость подачи субстрата и объем субстрата в реакторе, $м^3/с$; μ - удельный темп роста микроорганизмов, $сут^{-1}$; k_T – коэффициент токсичности, $сут^{-1}$; T_{x1} – концентрация токсического вещества, $кг/м^3$; S_0, S_1 – концентрация ацетата на входе и на выходе, соответственно, $кг/м^3$; $Y_{x/s}$ – экономический коэффициент, характеризующий рост микробной популяции по мере потребления субстрата; HS – концентрация уксусной кислоты, $кг/м^3$; K_1 – константа ингибирования роста микроорганизмов уксусной кислоты, $кг/м^3$.

Модель Конто описывает скорость роста микроорганизмов в зависимости от концентрации субстрата и клеток бактерий. Отличительной особенностью модели Моно является учет процесса ингибирования:

$$\mu = \mu_м \frac{S}{K_S X + S} (7)$$

где X – концентрация клеток бактерий.

На основе модели Конто была разработана модель Чена и Хашимото. Чтобы определить скорость выхода биогаза в математической модели, основные

параметры процесса анаэробной ферментации были введены как отдельные функции:

$$V = \frac{B_0 S}{\tau} * (1 - \frac{k}{\mu_m \tau - 1 + K}) \quad (8)$$

где B_0 – максимальный выход метана за сутки из 1 кг органического вещества, $м^3$ CH_4/кг;

S – концентрация субстрата, кг/$м^3$; τ – продолжительность сбраживания, сут; К – кинетический параметр. Здесь параметр $\mu_м$ = 0,013 Т – 0,129.

Все приведенные выше модели учитывают выход биогаза (качество анаэробного процесса) на основе химического состава и массы исходного сырья, количества и скорости роста микроорганизмов или продолжительности ферментации. [15, 16, 17]

Также имеются предложенные модели Друзьяновой В.П., которая описывает среднюю скорость всплытия пузырьков газа из биореактора при психрофильном режиме:

Уравнение скорости всплытия биогазового пузыря

$$\vartheta_n = \frac{e^{\frac{t(\sqrt{l^2-4ac})}{b}(l-\sqrt{l^2-4ac})-l-\sqrt{l^2-4ac}}}{2a(1-e^{\frac{t(\sqrt{l^2-4ac})}{b}})} \quad (9)$$

Тем самым определяя, скорость всплытия пузырьков газа и их количества, и образующиеся осадки, можно определить мощность при спонтанном перемешивания и далее спрогнозировать объем ожидаемого биометана в ферментаторе:

Мощность спонтанного перемешивания

$$N_{сп} = m_{суб} g(\vartheta_n + \sqrt{\frac{4gd(\rho_T - \rho_{ж})}{\xi \rho_{ж}}}) \quad (10)$$

$m_{суб}$ - масса субстрата, ϑ_n - скорость всплытия пузырька, ξ - коэффициент лобового сопротивления, ρ_T - плотность твердой частицы, $\rho_{ж}$ - плотность жидкости, d – диаметр пузырька, g – ускорение свободного падения.

Существует модель Егоровой Е.Н., которая учитывает зависимость образования продукта метаболизма от скорости массообмена субстрата и скорости продуктов метаболизма, как основные факторы, интенсивно воздействующие на процесс эффективной деструкции органического навоза. Таким образом можно говорить, что выход биогаза определяется перемешиванием субстрата:

$$\nu_б = \int(N_{перем}) \text{, (10) где}$$

$N_{перем}$ – мощность перемешивания в метантенке

Мощность перемешивания $N_{перем}$, по матмодели Егоровой Е.Н. необходимую на перемешивание субстрата внутри метантенка, определяется с учетом необходимого количества лопастей, крутящего момента на валу мешалки, коэффициента лобового сопротивления, плотности субстрата и т.п.:

$$N_n = (M_{кр} * \omega) * Z_л = \left(\frac{C_x \rho \omega^3 a b^4}{8} \right) * Z_л, \quad (11)$$

где
$M_{кр}$ – крутящий момент, возникающий на валу мешалки, Н*м;
C_x – коэффициент лобового сопротивления лопастей;
ρ – плотность перемешиваемой среды, кг/м^3;
ω - угловая скорость вращения мешалки, с$^{-1}$;
$Z_л$ – количество лопастей, ед;
a – высота лопасти, м;
b - высота лопасти, м.

В моделях Друзьяновой В.П. и Егоровой Е.Н. описаны обобщающие модели, полученные в лабораторных установках. В первом случае для определения выхода биогаза в зависимости от мощности биореактора при психрофильном режиме, а во втором случае в зависимости от мощности перемешивания в метантенке. Но все эти математические модели, сложно применяемые в промышленных масштабах для точного прогнозирования выхода биогаза с учетом различных параметров. [18, 19]

В нашей исследовательской работе по анализу оптимальной математической модели для более точного прогнозирования выхода биогаза при анаэробном брожении были использованы статические данные из биогазовой станции с. Курма, Карагандинской области и аналитические данные получены на примере биогазовой станции в провинции Манитоба, Канада. В предложенную нами в математическую модель, для ее широкого использования в промышленных масштабах и практического применения, использованы от 20 и до 26 различных параметров, существенно влияющих на качество анаэробного брожения, и соответственно на высокий результат выхода биогаза. Предлагается включить такие параметры в математическую модель, как показатели макро и микроэлементов (K-калий, Na-натрий, Ca-кальций, Mg-магний, Fe-железо, Cu-медь, Zn-цинк, Ni-никель, Co-кобальт, Mo-молибден, Cr-хром, Cd-кадмий), показатели C-углерода, N-азота, P-фосфор, C/N-соотношение углерода к азоту, L-концентрация питательных веществ, n-степень измельчения, VFA-содержание жирных кислот, τ-период брожения, m-масса субстрата, t-температура, pH-показатель кислотности, φ-влажность, S-сера, H_4N+ - аммоний. [20]

Из полученных стат.данных сформировали свою математическую модель с учетом предложенных параметров, оказывающих влияние на анаэробное брожение. Из всех изученных моделей для анаэробного брожения, нами предложена линейная регрессионная модель. Т.к. в ходе экспериментальных и математических исследований выяснилось, что данная модель является более практичным и эффективным при широком промышленном производстве биогаза. Выделяют несколько разновидностей регрессий: линейная, гиперболическая, множественная,

логарифмически линейная, нелинейная, обратная, парная. Экспериментальные исследования показывают, что влияние различных параметров на выход биогаза имеет линейную зависимость.

Предложенная нами математическая модель представляет собой линейное дифференциальное уравнение эмпирических соотношений каждого параметра, полученное путем регрессионного анализа. Модель линейной регрессии имеет следующий вид (см. формула 12):

$$y = a_0+a_1x_1+a_2x_2+\ldots a_nx_n \quad (12)$$

В данном уравнении:

- *Y* – переменная, влияние на которую нужно найти;
- X – факторы, влияющие на переменную;
- A – коэффициенты регрессии, определяющие значимости факторов;
- N – общее количество факторов.

Литература

1. Barbara Edery, Heinz Schultz. Biogas plants. Practical guide. Pages 1996 - 268. http://libed.ru/knigi-nauka/350087-1-barbara-eder-haync-shulc-biogazovie-ustanovki-prakticheskoe-posobie-osnovi-planirovaniya-stroitelnie-raboti-t.php

2. Vedenev A. G., Vedeneva T. A.-B.: A guide to biogas technologies. - "ДЭМИ", 2011 - 84 p. http://www.fluid-biogas.com/wp-content/uploads/2020/03/Rukovodstvo-biogas_2017.pdf

3. Iskakov S. K. Mobile biogas plant. // Энергосовет – 2015. – №4 – С. http://www.energosovet.ru/bul_stat.php?idd=551

4. Biomass as a renewable energy source. https://esa-conference.ru/wp-content/uploads/files/pdf/Kozlov-YUrij-Pavlovich.pdf

5. Development of an industrial-scale bioreactor in the context of a global pandemic. Shakerkhan K. O.Meshechkin V. V.Sagindykov K. M.Konyrkhanova A. A.Abilmazhinov E. T. IOP Conference Series: Earth and Environmental Science (2021). DOI:10.1088/1755-1315/723/4/042034

6. Prospects of biogas production in Kazakhstan. https://cyberleninka.ru/article/n/perspektivy-proizvodstva-biogaza-v-kazahstane/viewer

7. Биогазовая установка https://kazpatent.kz/images/bulleten/2018/gazette/ru201819/html/b0025684.htm

8. Казахстанская биогазовая энергетика. https://eenergy.media/2020/03/11/kak-razvivaetsya-kazahstanskaya-biogazovaya-energetika/

9. Китайская система стимулирования биогазовой энергетики. https://agroserver.ru/articles/1831.htm

10. Классификация биогазовых установок по конструктивным и технологическим признакам. https://cyberleninka.ru/article/n/klassifikatsiya-biogazovyh-ustanovok-po-konstruktivnym-i-tehnologicheskim-priznakam/viewer

11. Energetic and economic analysis of biogas plant with using the dairy industry waste. Kozłowski K.Pietrzykowski M.Czekała W.Dach J.Kowalczyk-Juśko A.Jóźwiakowski K.Brzoski M.Energy (2019). DOI: 10.1016/j.energy.2019.06.179

12. A Hybrid Method for the Development of Mathematical Models of a Chemical Engineering System in Ambiguous Conditions. B.B. Orazbayev, E.A. Ospanov, K.N., Orazbayeva,

L.T.Kurmangazieva //Mathematical Models and Computer Simulations. Moscow, Russia. 2018 – Vol.10, Issue 6. – pp. 748-758 DOI: 10.1134/S2070048219010125

13. Analysis of heat loss of a biogas anaerobic digester in weather conditions in poland. Teleszewski T. J.Z˙ukowski M. Journal of Ecological Engineering (2018). DOI: 10.12911/22998993/89660

14. Digitalization and innovative development of mining processes. Stenin D.Stenina N.Akanov A.Sagindikov K. E3S Web of Conferences (2019). DOI: 10.1051/e3sconf/201910503012

15. Mathematical modeling and decision-making on controlling modes of technological objects in the fuzzy environment. B.B.Orazbayev., Y.A. Ospanov, K.N.Orazbayeva, N.S Mukataev, A.I. Demyanenko // Proceedings of the 12th World Congress on Intelligent Control and Automation. (WCICA) Guilin, China. 2016. – pp.103-109 DOI: 10.1109/WCICA.2016.7578783

16. Control of Fuzzy Technological Objects Based on Mathematical Model. B.B. Orazbayev, Y.A. Ospanov, K.N. Orazbayeva, T. Gancarzyk, A. Shaikhanova // 16th International Conference on Control, Automation and Systems (ICCAS 2016). – Gyengju, Korea, 18–19 October 2016. –P. 1487–1493. DOI: 10.1109/ICCAS.2016.7832501

17. Review of the mathematical description of the process of methanogenesis in a bioreactor. M.B. Tlebaev, N.K. Kalinchun, D.U. Mamataeva. International scientific journal (ISSN 2072-0297) № 4.1(138.1)/2017. http://www.rusnauka.com/pdf/246610.pdf

18. Energy-saving technology for processing cattle manure. Dissertation work / Ulan-Ude / 2016, V.P. Druzyanova. https://www.esstu.ru/uportal/dissertation/downloadFile.htm?type=dissertation&typeId=499

19. Substantiation of the parameters of a small-volume digester with a stirring device for the conditions of the Republic of Sakha (Yakutia). Dissertation work / Blagoveshchensk / 2017, E.N. Egorova. https://www.dissercat.com/content/obosnovanie-parametrov-metantenka-malogo-obema-s-peremeshivayushchim-ustroistvom-dlya-uslovi

20. Parameters of the distributed databases of information systems when splitting data with application of algorithms of multidimensional parity. Karipzhanova A. Z.Sagindykov K. M.Gudov A. M.Dimitrov K. News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences (2019). DOI:10.32014/2019.2518-170X.128

DESIGNING AND ADMINISTERING A WEB APPLICATION CREATED WITH ASP.NET CORE TECHNOLOGY

Svanov A., Kintonova A.
asylsvanov@mail.ru
aliya_kint@mail.ru
L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan

Abstract. *Modern computer technologies are constantly developing and improving. This article discusses the basic issues of administering a web application created on the ASP.NET Core platform. Many business leaders and software developers do not make the right decisions, spending a lot of time choosing a particular web technology. The article also describes the technologies used in the process of creating and administering an enterprise web application.*

Keywords*: Web-application administration, ASP.NET Core technology, MVC design pattern, business processes optimization.*

Introduction. The main goal of the state program "Digital Kazakhstan", adopted in the country in 2019, is to improve the quality of life of the population by increasing the pace of economic development and the use of digital technologies. Recently, the popularity of web applications is growing. Because today many Internet resources are among them. Web applications work on the Internet using a web server, similar to the "client-server" structure.

Optimization and automation of business processes plays an important role in digitizing industries, increasing productivity, restructuring infrastructure, forecasting business needs, building a creative society and introducing new realities and innovations. Demonstrate the role of web applications in providing online business opportunities for businesses in a digitalizing country.

The purpose of the research work: to create a web platform for automating the work of enterprise employees and optimizing the workflow using the Asp.net core MVC framework. Develop skills in the theoretical and practical use of new web technologies in the development of web applications.

To achieve the purpose, the following research *tasks* were set:

1. Analysis of web resources.
2. Description of the functionality of the corporate web resource.
3. Explore the capabilities of the Asp.Net Core framework.
4. Development of a web resource for employees of Digital Agency LLP using the Asp.Net Core framework.

Object of research: Researching and exploiting opportunities for developing enterprise web resources of the ASP.NET Core platform. The practical significance of the research is the creation of a web application using the MVC core of Asp.net to automate the work of employees and optimize the workflow.

ASP.NET Core technology. ASP.NET Core is a platform offered by Microsoft that allows you to create different types of Web applications. With ASP.NET Core it is possible to create large portals and applications from small resources. This platform is a

continuation of the development of the ASP.NET platform. This is not just a new version or release, we can say that the release of Core is a revolution in the history of the platform and its qualitative transformation. ASP.NET Core is now a fully open source framework and all source files are available on GitHub [1-2].

So, with ASP.NET Core, we can create cross-platform applications. Although Windows is still a priority in the development and use of applications, we are no longer limited to this operating system. That is, we can run web applications not only on Windows, but also on Linux and Mac OS.

Depending on the modularity of the frame, all the necessary components of the web application can be downloaded as separate modules through the Nuget package manager. In addition, unlike previous versions of the platform, there is no need to use the System.Web.dll library [3].

ASP.NET Core includes the Web API system and the MVC system, which combines the functionality of web pages. Earlier versions of the platform included these technologies separately, so there were many repetitive features. Now they are integrated into one ASP.NET Core MVC programming model. Along with the integration of these technologies into one model, a number of new additional features have been added to the MVC. One of these features is tag-helpers, which allow you to continuously integrate html syntax with C # code.

ASP.NET Core is characterized by its versatility. The framework is made up of a set of relatively independent components. We can use the built-in implementation of these components, or we can expand them using an inheritance mechanism, or we can even create and use our own components with our own functionality [4].

A new HTTP conveyor based on Katana components and OWIN specifications is now used to process requests. Its modularity makes it easy to add your own components. In conclusion, we can distinguish the following main differences between the previous versions of ASP.NET Core and ASP.NET:

– Distribution of platform packages through NuGet;

– Cross-platform: ability to create and use ASP.NET applications on Windows, Mac and Linux;

– New lightweight and modular HTTP request conveyor;

– Ability to use the application both in IIS and as part of its own process;

– Use of the main .NET platform and its functionality;

– Light cloud configuration;

– Possibility of expansion;

– Comprehensive support for the creation and use of NuGet packages;

– Unified web stack that combines Web UI and Web API;

– Development as an open source, open to change;

ASP.NET Core MVC has released a fully clear, standard-compliant structure. Its built-in tag assistants produce results that meet the standards, but there is a significant philosophical change compared to web forms. Instead of HTML, which is not convenient for you to manage, ASP.NET Core MVC invites you to create simple views decorated with CSS. Of course, if you want to add complex UI elements, such as date selection or a few ready-made widgets for cascading menus, ASP.NET Core MVC has no special requirements and this approach makes it easier to use the best option. For example, it is very easy to insert client libraries such as jQuery, Angular, React or Bootstrap CSS. ASP.NET Core MVC integrates well with these libraries, so it includes templates for launching new projects from Microsoft. ASP.NET Core MVC is compatible with HTTP.

You have the ability to control requests between the browser and the server, so you can customize the user interface to your liking.

MVC design pattern. This technology is a ready-made template or template for solving common problems in the field of software development. That is, the program is an architectural design that provides developers with their own solution to a problem that is repeatedly encountered in a particular context. This technology appeared in the 70s of last century. Typically, these code solutions are not the final ones, they are simply examples of problem solving in different situations. Object-oriented templates represent relationships, as well as relationships between classes and objects, and they are not limited to the final classes and objects. Templates used only in that language, according to the specifics of a particular language, are considered low-level design templates and are called idioms. It is not universal because it is used in a specific language or programming platform.

High-level design templates are also widely used. They include a large software system architecture. Algorithms are also considered templates, although they are considered computational templates, not design templates, because they are used in computational problems [5].

While MVC is a great platform for creating websites, it also has great status for creating web APIs. It has the ability to create services that are available to most customers, including applications for browsers and mobile devices. The platform supports HTTP content matching with local support for formatting data as JSON or XML. There are link features to support hypermedia. Supports the allocation of resource-independent resources to share web APIs between multiple web applications.

When implementing the Model-View-Controller architecture, some design patterns are used. The main ones are: controller, strategy, linker and others. The model is an independent component - any changes to the controllers or view have no effect on the model. The controller and appearance are relatively independent components. This way, you can access a specific controller using a view and create views from the controller, but often you can change them yourself. ASP.NET Core MVC has released a fully comprehensible, standards-compliant framework. Its built-in tag helpers release results according to standards, but there are significant philosophical changes compared to web forms. Instead of HTML, which is not convenient for you to manage, ASP.NET Core MVC invites you to create simple CSSS-styled views. Of course, if you want to draw complex UI elements, i.e. a date or a few pre-made widgets for cascading menus, ASP.NET Core has no special requirements for MVC and this approach makes it easier to use the best option.

In MVC, the letter M represents the model, and it is an important part of the application. A model is an image of the objects, processes, and rules of a particular subject that define a topic known as the domain of the application. The model in an MVC application represents the state of the application and the business logic or operations performed with it. In the MVC architecture, the view displays only the data, while the controller processes the input data and responds to the user's actions. Business logic must be included in the model along with input logic to maintain the status of the application. The model, often referred to as the domain model, contains C # objects (called domain objects) that form the domain of the application and manage them [6-7].

Views and controllers give domains customers access to subject area data, and a well-designed MVC application starts with a well-thought-out model and has a centrally strong connection between the controllers and views that are added later.

Building web applications while summarizing Asp.Net in large logic programs also makes the model easier to work with by introducing a ViewModel element. Retrieving and writing data from the database is done using the Entity Framework. Asp.Net, in addition, the MVC framework will certainly appeal to users not only for its convenient architecture, but also for its versatility in software development and ease of access to other services.

Designing and administering. First we create all the models (tables) we need. To link these models to the controller, we need to create a context file. The IdeaDbContext context file helps us connect to the database. Since the database has not yet been created, we call the Database.EnsureCreated () method in the IdeaDbContext constructor. Using this method, we create a table in the database based on the described models. Before sending the program for execution, we enter the settings to connect to the database server in the file appsettings.json. Server = (localdb)\\mssqllocaldb; Database = ideadb.

We create our first method called Index. This method looks at the home page of the web application and responds to the action on it. Return View (ideas.ToList ()) to run the Index; write the code. This code gives us an index method that lists the ideas table as a list. We just need to adjust the view to get it out. To do this, we create a web page from the Views folder according to the owner of the index. This place is for writing simple HTML code. That allows you to create a view of the site. After writing the required code, you can try to implement the project. As you can see in Figure 5, 15 models and as many tables have been created. Each table stores its own information. For example: like, dislike, like a comment, a table of ideas, questions, answers, etc. Let's look at the scene before moving on to the controller. Create a view code with simple HTML code and CSS elements. We use the help of "master pages" to create a scene. That is, we need to avoid rewriting the code on each page. Here we describe and describe the common design elements. For example, navigation panels and libraries. When it comes to libraries, these are the files you need to embellish the elements of the web view. This data is stored in the _Layout.cshtml file.

To create views, we use the Bootstrap 4 frontend framework. This framework offers a free set of tools for creating websites and web applications. They include design templates for other components of the web interface, including HTML and CSS typography, web forms, buttons, bookmarks, navigation blocks, and JavaScript extensions. Bootstrap uses modern elements in the field of CSS and HTML. Therefore, older browsers may have problems opening. Bootstrap has often been used to create mobile versions of websites. Because Bootstrap is very effective in creating pages that can be quickly adapted to both computers and mobile devices.

To associate the view with the model, we write the code string @model IEnumerable <Prk.Idea.Models.MIdea> at the beginning of the view. This allows us to get data from the table of ideas. We can divide the page into several parts. On the left we will have function buttons (Figure 9). There are buttons for filtering data according to several categories. Each button is associated with an action according to the filter type.

We take the required table in context and use the Include () built-in method to get each required field in that table. This method means adding data. To determine which idea should be retrieved from the database when opening this page, the method should be given the number of the idea when you click the open idea button in the view on the original Index page. We do this through @ViewBag. This is an integrated method of Razor Pages.

We will give the number of the required idea via @ViewBag. The idea number is written to the id parameter as specified in the public IActionResult Details (int? Id) {} method parameter. It will be much easier to apply the desired idea in the future. This is done using a tag-helper. This solves the problem of data acquisition.

The ability to add an idea to the site opens as a modal page. Adding an idea may or may not show the author of the idea. But in the database, the administrator will see the author of the idea. It consists only of a field that accepts a value of 0 or 1, which determines whether it is hidden or not hidden in another field. This is a measure to identify violators on the site.

Conclusions. During this research, new technologies and methods for developing web applications were proposed. The work analyzes the types and structures of web resources and reveals the topic of web-resource development. Examples of the use of new programming features, including: Asp.Net Core MVC frame and the latest versions of Entity Framework, Identity 2.0, Boootstrap 4.3 technologies are shown and summarized. Objectives of the research were performed: analysis of web-resources, described the needs of digital agency staff and tasks to perform the web-resource and its functionality, proposed the design of the architecture of the web-resource, demonstrated the process of creating a web-resource (web-application). description is provided.

The Asp.Net Core platform offers new, up-to-date solutions for creating web applications. The creation and management of logic is easily carried out independently through the division of responsibilities. Client-server technology is optimized as a result of linking with the controller in the "model-view-controller" architecture. Entity Framework technology simplifies the work with large databases due to asynchronous data output and code-first.

The practical significance of the research is that the research and analysis in this work makes a significant contribution to the development of web applications and plays an important role in the digitization of industries in the country, increasing productivity and innovation in business.

References.

1 Asp.Net Core MVC Framework. - https: //ru.wiqipedia.org/wiki/ASP.NET_MVC_ Framework (12.04.2020).

2 Wolfson B. Flexible project management and products. - Saint Petersburg: Peter, 2015 - 144 p.

3 Freeman A. ASP.NET Core MVC with C # Examples for Professionals. - St. Petersburg. : LLC "Alpha-kniga", 2017. - 992 p.

4 ASP.NET Core - a new epoch in the development of ASP.NET. - https://metanit.com/sharp/aspnet5/1.1.php (19.04.2020).

5 Murat J., Alex F .. Pattern design for professionals. - Saint-Petersburg: Peter, 2016. - 240 p.

6 Gamma E., Helm P., Johnson P., Vlissides J.; Receptions of object-oriented design. Pattern design. - SPb: Peter, 2019. - 368 p.

7 ASP.NET Core MVC. Official documentation of Microsort Docs.- https://docs.microsoft.com/ru/aspnet/core/mvc/overview?view=aspnetcore-3.1 (15.05.2020).

SATELLITE MONITORING ARABLE LAND OF XINJIANG CHINA ON BASE OF NDVI-C6 AND LST-C6 FEWS NET DURING 2002-2021

Terekhov A.G., Abayev N.N.
e-mail: aterekhov1@yandex.ru
Institute of information and computing technology MES, Kazakhstan

Abstract. *The use of water resources of the cross-border (China-Kazakhstan) River Kara-Ertis in the interior of the Dzungarian plain determines the relevance of this research. The Normalized Vegetation Difference Index (NDVI) and Irrigation Cooling Effect (ICE) were used to assess the state of crops and the efficiency of agricultural water use in 2002-2021. The FEWS NET data portal was source of NDVI and LST data with 10 days renew. The trends of increasing NDVI and ICE values on first decade of July over the past 20 years are revealed. This indicates an improvement of the cropping practice and irrigation performance of arable land in the Northern foothills of the Eastern Tien Shan (China). Thus, it can be concluded that water use by transboundary River Kara-Ertis in the interior Dzungarian plain has been in a growing phase over the past 20 years.*

Introduction

The arid climate and the rising water consumption in Central Asia create the issue of regional water security. One of the components of water security concerns the issue of water allocation of transboundary river outflow and, in particular, the River Black Irtysh. The upper reaches of this river belong to the Xinjiang, China and the lower part belongs to Kazakhstan. In the period of 1999-2007, the channels of inter-basin water transfer: Black – Irtysh – Karamay (1999); and Black Irtysh-Urumqi (2007) were built in Xinjiang. This water transport infrastructure transfers the water resources of the cross-border River Black Irtysh 400 km to the South, to the Northern foothills of the Eastern Tien Shan, where they are used for various needs, including agricultural irrigation in the interior of the Dzungarian plain. In the continental, arid climate of Central Asia, crop production is possible only when the land is watered. Available water resources of territories, in general, depend on the characteristics of seasonal large-scale atmospheric circulation and conditions for winter snow accumulation. For Kazakhstan, as a country of the lower part of the cross-border river basin, objective information about agricultural water consumption in the Xinjiang and its long-term trends is of great interest.

Remote sensing data provides a wide range of possibilities for recording various parameters related to irrigation agriculture [1,2]. Irrigation farming in arid climates significantly changes the spectral characteristics of the underlying surface. There appears a developed vegetation cover with regular seasonal dynamics. Long-term monitoring of vegetation indices, for example Normalized Vegetation Difference Index (NDVI), allows us to judge changes in the area of crops and provides information about the crop states [3] and their productivity [4,5]. Irrigation of arable land leads to moistening of the surface layer of the soil and the development of vegetation. This process is accompanied by evapotranspiration [6], a decrease in the surface temperature (Land Surface Temperature (LST)) and rising ground water levels [7]. In practice, more often used effect of reducing the temperature of irrigation arable land (Irrigation Cooling Effect (ICE)), which is usually used in climate or meteorological research [8-10]. During irrigation, water evaporation occurs both from above-ground biomass and from capillaries of the soil layer. The value

of ICE is closely related to irrigation efficiency. Thus, ICE can act as a parameter that characterizes irrigation performance.

The purpose of this research was long-term (2002-2021) monitoring and analysis of NDVI and ICE values for river basins of the Xinjiang region of China, which are located on the Northern slope of the Eastern Tien Shan. For the analysis, arable lands located in the zone of influence of the Black Irtysh – Dzungarian plain water transport system were selected, which are watered, including cross-border (China-Kazakhstan) resources of the River Black Irtysh.

Test site territory

Kazakhstan is the largest country in Central Asia with an area of 2.72 million km2 (9th place in the world). In the South-East, Kazakhstan borders the Xinjiang (China) from whose territory Kazakhstan receives several large for Central Asia cross-border rivers, including the River Kara-Ertis with the annual runoff on the China-Kazakhstan border is 8 km^3. In the period of 1999-2007, the irrigation system of the Kara-Ertis – Dzungarian plain was built, consisting of two branches, Kara-Ertis – Karamai and Kara-Ertis – Urumqi. Thus, at present, the waters of the cross-border Kara-Ertis river reach the Northern foothills of the Eastern Tien Shan, where they are used for irrigation of arable land. The objects in this research were arable lands of three river basins of the Northern slope of the Eastern Tien Shan: River Bolo-Tala; River Kuitun; and the River Manas; Fig. 1. For the analysis, three contours were identified that included the irrigation arable land of the respective river basins.

Materials and methods

MODIS data is a useful source of information for describing the state of irrigation agriculture in Central Asia [11]. The product "Temporarily smoothed NDVI" USGS/EROS/FEWS NET in e-Modis NDVI C6 format (https://earlywarning.usgs.gov/fews/search/Asia/Central%20Asia), with a resolution of 250 meters and a 10-day renewal available on the territory of Central Asia, fig. 1a. Processing NDVI scenes when creating seasonal series of e-Modis NDVI C6 values has a strategy for calculating the upper envelope, which minimizes the impact of interference from cloud cover. It was expected that the high quality of the e-Modis NDVI C6 scenes would allow obtaining correct estimates of the long-term dynamics of the vegetation index in the selected contours of agricultural areas when using one covering per season. To describe the state of agricultural vegetation within the selected contour, we used the 19th decade (July 1-10) of each year, the period when most crops have a seasonal maximum phase of green biomass.

The temperature of the underlying surface (soil+vegetation) was characterized using MODIS satellite data "Land Surface Temperature (LST), Collection 6". There are a large number of variants of this product combined under the domain name MOD11. Assessment of the surface temperature of arable land and surrounding areas is interfered by cloud cover. However, when solving seasonal monitoring tasks, there is no need for a high coverage frequency. We used the Famine Early Warning system NET (LST-C6 FEWS NET) product available on the data portal (https://earlywarning.usgs.gov/fews/). The product has an archive since 2002, a spatial resolution of 5 km and a 10-day renewal. These characteristics are sufficient to solve the research tasks.

Irrigation Cooling Effect (ICE) in arid climate in irrigation farming zones is a gradient between the temperature of the underlying surface in an agricultural oasis and the surrounding dry areas. The highest air temperatures and low humidity in Central Asia occur in July-August. The third decade of July was selected for monitoring ICE in agricultural areas, i.e. the time is near with NDVI monitoring. The ICE value for each analyzed contour was a characteristic of seasonal water availability of arable land.

Thus, from the NDVI C6 and LST C6 FEWS NET product databases for the period July 1-10 and July 21-31, 2002-2021, the time series was formed for three contours that include the arable lands of the Bolo-Tala, Kuitun and Manas river basins. These time series characterized the dynamics of changes in the agriculture practice and water availability of arable land in river basins. A standard linear regression mathematical tool was used to assess the direction of trends.

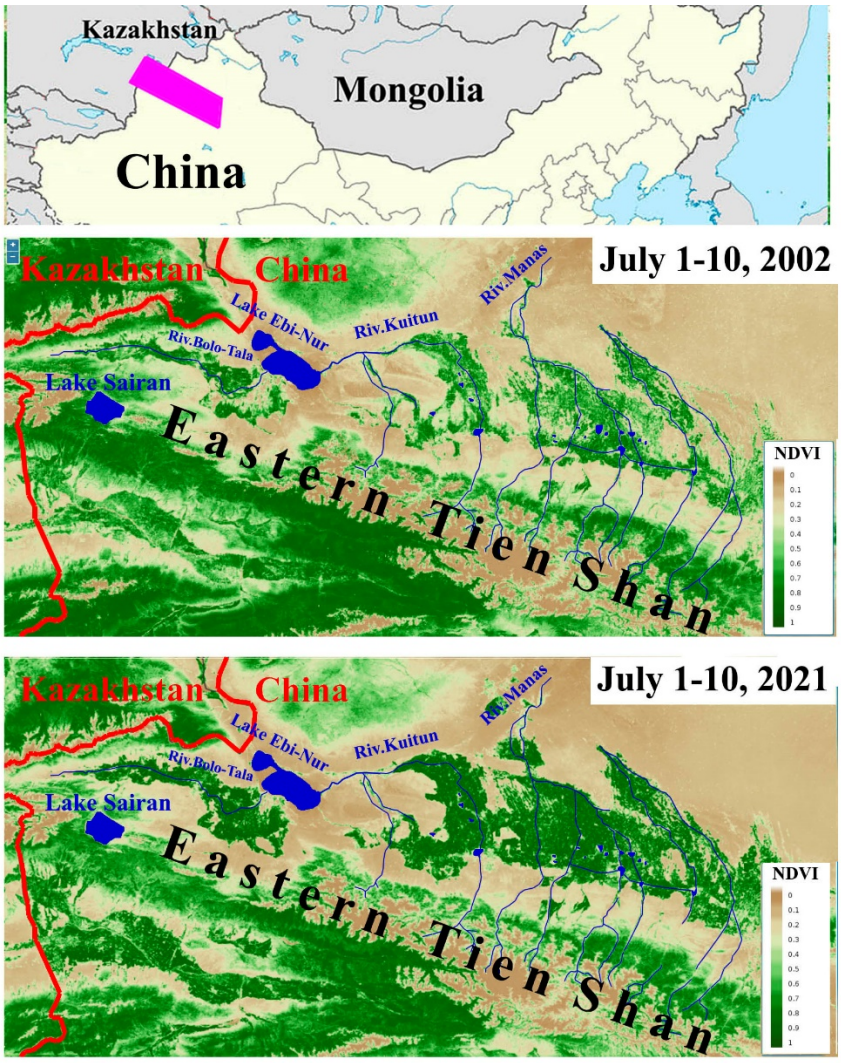


Fig. 1. The examples of satellite scenes NDVI C6 FEWS NET on 1 decade of July 2002 and 2021 year

Results

The Fig. 2 shows the long-term (2002-2021) evolution of arable land parameters, in particular the values of the vegetation index NDVI (July 1-10) and the values of the cooling effect of irrigation ICE (July 21-31) for three river basins of the Northern slope of the

Eastern Tien Shan: River Bolo-Tala: River Kuitun; and River Manas. The calculated linear regression trends show an increase in the values of both parameters. The confidence of the linear approximation of trends varied from 0.51 to 0.94, Fig. 2.

Discussion

The considered arable lands of the River Bolo-Tala, River Kuitun and River Manas basins had pronounced trends for improving the crop state in the period 2002-2021 years. The positive trend of the values of the vegetation index NDVI was expressed more significantly. The accuracy of the approximation varied from 0.84 (River Bolo-Tala basin) to 0.94 (River Kuitun basin), Fig.2. The ICE value increase was weaker. The accuracy of the approximation varied from 0.50 (River Bolo-Tal basin) to 0.77 (River Kuitun basin). The ICE value is also affected by the season humidity. In dry and hot seasons, ICE values are greater than in cold and wet ones, which masks the many years trend.

In the period 2002-2021, the level of agricultural practice in the Northern foothills of the Eastern Tien Shan increased significantly. Improvement of crop state also indicates that there are no problems with water availability of irrigated arable land.

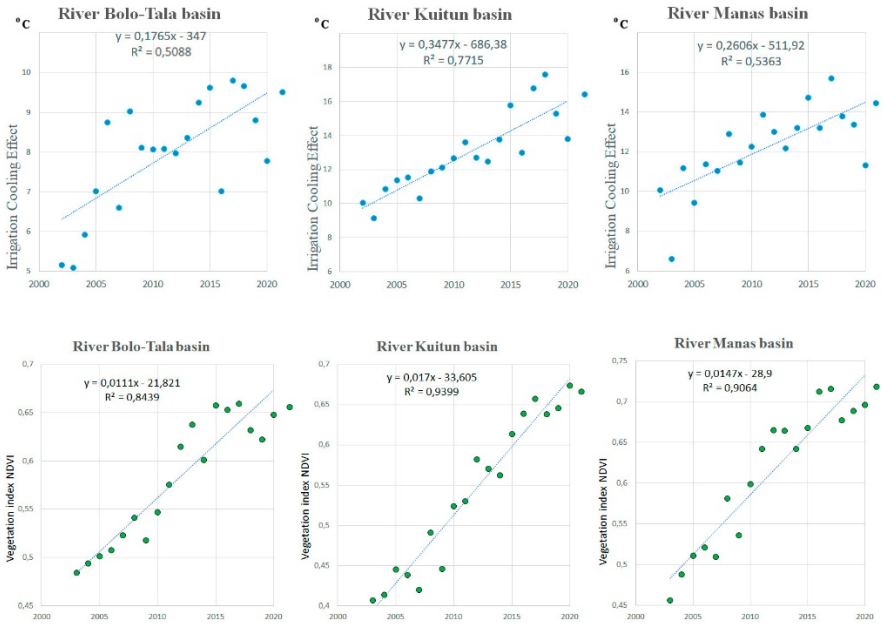


Fig. 2. Dynamics of average values of ICE (3 July's decade) and NDVI (1 July's decade) for arable lands of the Bolo-Tala, Kuitun and Manas river basins (Xinjiang, China) during 2002-2021 years

Conclusions

Satellite monitoring of irrigation arable land in the Northern foothills of the Eastern Tien Shan in the basins of the River Bolo-Tala, River Kuitun and River Manas in the period 2002-2021 showed no signs of stagnation or degradation of agricultural vegetation, which would obviously be associated with water deficit. In the coming years, the trend towards improving agricultural practices may obviously continue, since the potential of water resources has not yet been exhausted. The volume of water uses by cross-border river resources in the interior Xinjiang (China) and in particular the River Kara-Ertis, in the Northern foothills of the Eastern Tien Shan may grow in the future.

Acknowledgment

This research is funded by the Ministry of Education and Sciences, Republic of Kazakhstan (Grants: AP09562387).

References

1. Yakushev, V., Dubenok, N., Loupian, E. Earth remote sensing technologies for agriculture: application experience and development prospects// Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa. 2019.- Vol.16, N. 3.- P.11-23. doi: 10.21046/2070-7401-2019-16-3-11-23.

2. Dalezios, N., Spyropoulos, N., Dercas, N., Psomiadis, E. Remotely Sensed Methodologies for Crop Water Availability and Requirements in Precision Farming of Vulnerable Agriculture// Water Resources Management, 2019.- Vol.33, N.4.- P.1499-1519. doi: 10.1007/s11269-018-2161-8.

3. Terekhov, A., Abayev, N., Lagutin, E. Diagnostics of water availability for agricultural crops in Xinjiang (China) in 2003–2019 based on eMODIS NDVI C6 data// Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa. 2020.- Vol.17, N.1.- P.128-138. doi: 10.21046/2070-7401-2020-17-1-128-138.

4. Stepanov, A., Makogonov, S., Tolpin, V. Assessment of soybean yield in the Far East using regression models based on remote sensing data// Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa. 2019.- Vol.16, N. 6.- P.194-198. doi: 10.21046/2070-7401-2019-16-6-194-198.

5. Botvich, I., Emelyanov, D., Larko, A., Malchikov, N., Ivchenko, V., Demyanenko, T., Shevyrnogov, A. Estimation of the spatial distribution of spring barley yield (Krasnoyarsk Territory) from ground and satellite spectrophotometric data// Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa, 2019.- Vol.16, N. 5.- P.183-193. doi: 10.21046/2070-7401-2019-16-5-183-193.

6. Muzylev, E., Startseva, Z., Zeyliger, A., Ermolaeva, O., Volkova, E., Vasilenko, E. Osipov, A. The use of satellite data on land surface and meteorological characteristics in modeling the water and heat regimes of large agricultural region// Sovremennye problemy distantsionnogo zondirovaniya Zemli iz kosmosa, 2019.- Vol.16, N. 3.- P.44-60. doi: 10.21046/2070-7401-2019-16-3-44-60.

7. Lagutin, E., Smolyar, V., Kojobaev, K., Terekhov, A., Edigenov, M. RK probabilistic hydrogeological map// News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, 2020.- Vol.2, N. 440.- P. 103-113. doi: 10.32014/2020.2518-170X.37**.**

8. Bamston, A., Schickedanz, P. The effect of irrigation on warm season precipitation in the southern Great Plains// J. Climate Appl. Meteor., 1984.- Vol.23.- P.865-888. doi: 10.1175/1520-0450(1984)023<0865:TEOIOW>2.0.CO;2.

9. Han, S., Yang, Zh. Cooling effect of agricultural irrigation over Xinjiang, Northwest China from 1959 to 2006// Environ. Res. Lett., 2013.- Vol.8, N.2.- 024039. doi: 10.1088/1748-9326/8/2/024039.

10. Yang, Q., Huang, X., Tang, Q. Irrigation cooling effect on land surface temperature across China based on satellite observations// Sci. Total Environ., 2020.- Vol.705.- 135984. doi: 10.1016/j.scitotenv.2019.135984.

11. Conrad, Ch., Dech, S., Hafeez, M., Lamers, J., Martius, Ch., Strunz, G. Mapping and assessing water use in a Central Asian irrigation system by utilizing MODIS remote sensing products// J. Irrig. Drain. Syst., 2007.- Vol.21.- P.197–218. doi: 10.1007/s10795-007-9029-z.

МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ОЦЕНКИ ЭКОЛОГИЧЕСКОГО УЩЕРБА ПРИ ЭКСПЛУАТАЦИИ ПЕРСПЕКТИВНЫХ РАКЕТ-НОСИТЕЛЕЙ

[1]Ермолдина Г.Т., [2]Алипбаев К.А., [1]Аден А.Е., [2]Оразалы Е.Е.,
[1]Бапышев А.М., [1]Суйменбаев Н.Б.
gulerm@mail.ru
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Алматинский университет энергетики и связи имени Г. Даукеева, Казахстан

Аннотация. *В статье рассмотрены методические подходы к эколого-экономической оценке и функциональному зонированию территории района падения отделяющихся частей ракет-носителя на основе информационно-прогностической системы. В работе определена структура баз данных, информационное взаимодействие между основными модулями этой системы и представлен методический подход при экономической оценке экологического ущерба. На основе исследования разработаны предложения по оптимизации территорий районов падения по себестоимости и восстановительных работ.*

Ключевые слова: *эколого-экономическая оценка, зонирование территории, операционно-территориальная единица, ракета-носитель, информационно-прогностическая система, база данных, район падения.*

1 Введение

При пусках ракет-носителей с космодрома Байконур трассы полета проходят по территории Республики Казахстан и Российской Федерации. Соответственно при аварии на территории Казахстана экологический ущерб определяется в соответствии с Казахстанским законодательством и условиями межгосударственных соглашений [1-3].

При определении размера экологического ущерба были выявлены недостатки нормативной базы, определяющей порядок его расчета применительно к рассматриваемым случаям. Исходными данными для определения ущерба являются технические характеристики носителя, разгонного блока и космического аппарата, данные о трассе вывода, телеметрическая информация о полете, характеристики местности, где произошло падение, результаты обследования места аварии. В реальной практике экологический ущерб определялся расчетным методом с учетом принятых допущений [4-5]. Изменение качества объектов окружающей среды (понижение бонитета почв, уничтожение растительности и др.) относится к экологическому ущербу. При определении ущерба в этом случае учитывается время, необходимое для естественного или искусственного (рекультивация территории) восстановления исходных свойств объектов окружающей среды.

Разработанная ФГУП «Центр эксплуатации наземной космической инфраструктуры» совместно с Географическим факультетом МГУ «Методика определения экологического ущерба при аварии ракет-носителей и межконтинентальных баллистических ракет на трассе вывода космических

аппаратов на орбиту» на основе практического опыта работ, имеет определенные недостатки и не может претендовать на ликвидацию пробелов природоохранного законодательства [6].

2 Постановка задач исследования

Особенность оценки экологического ущерба при падении ступеней ракеты-носителя заключаются в том, что эксплуатация ракет-носителей характеризуется неспецифическим воздействием практически на все компоненты экосистемы: гидросферу, атмосферу, литосферу, биосферу. При возникновении аварийных ситуаций последствия аварии непредсказуемы. Единственно, что реализуется при пусках ракет, это запрет на аварийное выключение двигателей на особо опасных участках полета. Это участки полета, на которых при выключении двигателя может произойти падение аварийного изделия на населенные пункты и опасные производственные объекты [6].

Сложность определения экологического ущерба при аварийном падении отработавших ступеней ракеты-носителя заключается в невозможности предварительного сбора характеристик территории, подверженной воздействию, и, соответственно, в многообразии возможных последствий падения отделяющихся частей ракет-носителя. Штатная эксплуатация в местах падений характеризуется образованием на месте падения второй ступени ракеты-носителя в результате взрыва воронок различного диаметры и глубины, нарушением растительного покрова, последствиями взрыва, а также следами пожара и проливов токсичного ракетного топлива.

При определении размера экологического ущерба необходимо учитывать множество различных вариантов нарушения ландшафтов.

Анализ научно-технических, теоретических и практических подходов к формированию стратегии управления природными ресурсами при эксплуатации ракет-носителей показал необходимость разработки информационно-прогностической системы для определения районов запуска и падений ракет-носителей на основе внедрения технологии управляемого спуска ракетного блока с учетом экономической и технической оценки эффективности и соблюдением требований экологической безопасности их эксплуатации. Реализация информационно-прогностической системы в конечном счете позволит определить возможности формирования доказательной базы для принятия решений о запуске и падений ракет-носителей (РН) сверхлегкого класса (СЛК) на территории Казахстана.

В основную концепцию при разработке информационно-прогностической системы определения районов запуска и падений РН СЛК включены вопросы автоматизации отчетности по запускаемым ракетам.

3 Разработка информационно-прогностической системы

Решению задачи оценки вредных воздействий на окружающую среду и прогноза распространения загрязнений в районах запуска и падений частей ракет, должна служить информационно-прогностическая система определения районов запуска и падений ракет-носителей сверхлёгкого класса при управляемом спуске с учетом требований экологической безопасности. Решение задачи минимизации техногенного воздействия и оценки прогнозируемого ущерба должно включать развитие информационно-прогностических систем с целью выработки научно-обоснованных рекомендаций по выбору точек запуска и прицеливания с учетом показателей районирования территории и себестоимости восстановительных работ.

Разработка информационно-прогностической системы начинается с детального анализа первичных данных. В основе создания системы лежит методология районирования и типологической классификации многомерных данных.

3.1 Информационно-прогностическая система

Информационно-прогностическая система предназначена для мониторинга территорий, отводимых под эксплуатацию ракет-носителей и является основой информационного обеспечения управления деятельностью по регулированию природопользования и охране окружающей среды при эксплуатации ракетно-космических комплексов.

С учетом целей и задач экологического мониторинга предлагается вариант построения функциональной структуры информационно-прогностической системы (рисунок 1).

Рисунок 1 – Онтология информационного взаимодействия информационно-прогностической системы

Функциональное назначение информационно-прогностической системы состоит в решении комплекса задач научно-технического обеспечения. В состав базы данных информационно-прогностической системы входят следующие подсистемы (рисунок 2):

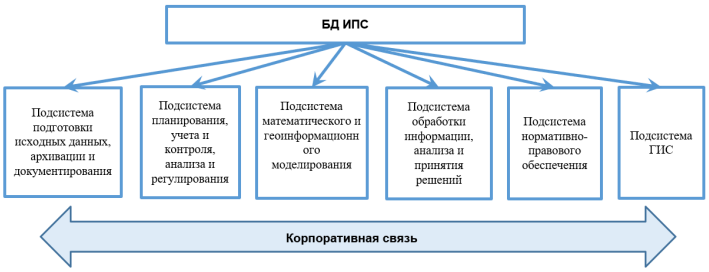


Рисунок 2 – Структура БД информационно-прогностической системы

1) Подсистема подготовки исходных данных, архивации и документирования

В подсистеме концентрируются исходные данные, содержащие перечень и количественные показатели (экологические характеристики), необходимые для обеспечения функционирования информационно-прогностической систем при штатной эксплуатации сверхлегких ракет и мини- космодромов. В их числе:

- характеристики экологического состояния окружающей природной среды,

- экологические характеристики изделий и объектов ракетно-космической техники;

- топографические и тематические карты;

- картографическая привязка объектов инфраструктуры и соответствующая характеристика объектов окружающей природной среды.

В соответствии с ними должны формироваться базы данных по указанным выше характеристикам при штатной эксплуатации и аварийных ситуациях. При этом типовыми аварийными ситуациями по отношению к окружающей среде являются:

- сбросы химических веществ в окружающую среду (вне рабочих зон) превышающие согласованные лимиты;

- пожары с выбросами в окружающую среду газов;

- выбросы (сбросы) радиоактивных веществ (при их наличии в составе РКК), превышающих нормы радиационной безопасности.

База данных подсистемы учета специфических воздействий РКД должна включать:

- БД календаря пусков средств выведения (дата и время пуска, используемый состав средств выведения, полезная нагрузка, параметры орбиты выведения);

- БД экологически значимых характеристик ракет-носителей (массово-габаритные, массы, типы и характеристики используемых топлив и других жидкостей, материалов и веществ), как для средств выведения в целом, так и для отдельных ступеней и отделяющихся частей ракет-носителя;

- БД экологически значимых технологий и характеристик используемого при проведении пуска технологического оборудования и объектов космодрома.

Учет специфических воздействий должен основываться на ведении календаря пусков ракет-носителей. Дата и время пуска, используемый состав средств выведения и параметры орбиты выведения практически полностью определяют объемы и географию воздействий и во многом условия распространения воздействий.

2) Подсистема планирования, учета и контроля, анализа и регулирования.

Планирование включает решение следующих задач:

- планирование экологических работ на каждый пуск в соответствии с планом запусков и технологическим планом подготовки и пуска ракет космического назначения;

- определение потребности в материальных ресурсах по осуществлению экологических работ;

- планирование метеорологического обеспечения;

- планирование работы экологических станций (при наличии);

- календарное планирование.

3) Подсистема математического и геоинформационного моделирования.

Подсистема предназначена для решения задач научно-технического обеспечения функционирования информационно-прогностической системы –

идентификация, оценка экологического риска, объем работ по ликвидации последствия, экономическую оценку экологического ущерба.

4) Подсистема обработки информации, анализа и принятия решений.

Подсистема должна обеспечивать принятие руководством различного уровня решений о модернизации ракет, возможных точках запуска ракет и падений отработавших ступеней, адекватных решений по оценке и прогнозированию последствий воздействий запусков сверхлегких ракет при штатной эксплуатации и возможных аварийных ситуациях.

5) Подсистема нормативно-правового обеспечения

Нормативно-методическая составляющая включает анализ информации по имеющимся методикам, нормативным документам по оценке экологического ущерба при эксплуатации РКК, включая аварийные ситуации и сверхнормативное загрязнение окружающей среды; средства документирования и представления результатов оценок воздействий, комплекс методических руководств и нормативных актов, регулирующих природоохранительные соотношения в сфере ракетно-космической деятельности.

6) Подсистема ГИС

Одной из основных задач ГИС является создание единого информационного пространства, которое может быть сформировано на основе использования современных геоинформационных технологий. Интеграционный характер геоинформационных систем (ГИС) позволяет создать на их основе мощный инструмент для сбора, хранения, систематизации, анализа и представления информации. Благодаря ГИС в полной мере реализуется возможность целостного, обобщенного взгляда на комплексные проблемы окружающей среды и экологии.

Основные блоки в структуре информационно-прогностической системы включают базы данных летательного аппарата, космодрома и района падения (рисунок 3).

Рисунок 3 – Основные блоки информационно-прогностической системы

3.2 Определение критериев экологического качества

Способ выделения оптимальной операционно-территориальной единицы (ОТЕ) опирается на существующих методах классификации. Под ОТЕ будем понимать земельные участки площадью S_i (i= 1, 2, 3 N). Так как любая экосистема

представляет собой систему, состоящую из сообщества живых организмов (биоценоз), среды их обитания (биотоп) и системы связей, осуществляющей обмен веществ и энергии между ними, то в качестве основных компонентов экосистем рассмотрим в роли биоценоза – растительность, биотопа - почву и водные объектов.

Характеристиками состояния растительности как правило являются разновидность растительного сообщества (флористический состав), густота (структура) растительного сообщества, проективное покрытие (соотношение площади в ландшафте) и фитомасса, а также показатели генеративности и пороков развития растительных организмов. Восстановление растительных сообществ характеризуются различным ежегодным приростом фитомассы, вследствие этого различным сукцессионным периодом.

Почвенный покров характеризуется многообразием почвенных разновидностей, обладающих различными физико-химическими свойствами. Поэтому целесообразным представляется обработка данных на основе почвенной карты с уже известными справочными данными. Оценка и градация ОТЕ по почвенному признаку предполагает определение бонитета почв согласно стандартным методикам бонитировки.

Наличие водотоков (водных объектов) свидетельствует о рисках миграции и широкого распространения загрязняющих веществ, поэтому наличие или отсутствие водотоков предполагает оценку ОТЕ согласно оценочной классификации: «наличие-плохо», отсутствие – хорошо».

Таким образом, оптимизация районов падений отделяющихся частей ракет-носителя предполагает выделение операционно-территориальных единиц по комплексу признаков следующих компонентов экотопа: а) растительности (состав, структура, проективное покрытие, фитомасса), б) почвы (крепость грунтов, бонитет типов почв), в) водные объекты (наличие либо их отсутствие).

3.3 Экономическая оценка экологического качества операционно-территориальных единиц

Ранжирование операционно-территориальных единиц целесообразно проводить по степени экологического качества, которое в значительной мере опирается на систему показателей состояния окружающей природной среды. Вариабельность операционно-территориальных единиц определяется системой показателей и сложностью рельефа, определяющих суммарный экологический ущерб и компенсации на восстановление первоначального состояния экосистемы.

Процесс комплексной оценки каждой природно-территориальной единицы в пределах расчетной зоны падения отработавшей ступени основан на учете показателей, характеризующих ее качество. Так, в качестве показателей, характеризующих экономическую оценку растительного покрова, предлагаются следующие критерии - состав, структура, проективное покрытие и фитомасса - Q_v, Q_s - Q_w.

Алгоритм выделения оптимальных типов ОТЕ (рисунок 4) предполагает следующее:

1) На исследуемую территорию накладывается регулярная или нерегулярная сетка из N участков с площадями S_i (i= 1, 2, 3 N). Каждый S_i представляет «мозаику» областей с определенным составом экотопа. Размер площадей S_i определяется однородными характеристиками растительного покрова.

2) На основе анализа данных инвентаризации, физико-географических и природно-ресурсных карт, паспортов РП, данных дистанционного зондирования,

методик оценки экологического воздействия формируют базу данных для оценки величин введённых критериев.

3) На основе введенных критериев Q_v, Q_s, Q_w для каждой S_i высчитывается экономическая стоимость:

3.1) Критерий качества растительного покрова

Оценка критерия Q_{Vi} представляет собой учет типа растительности, фитомассы Q_{vmi}(ц/га) и проективного покрытия Q_{ppri}(в %).

$$\sum_{i=0}^{n} Q_v = Q_{v_m} * Q_{v_s} * Q_{v_i} \quad (1)$$

Тип растительности определяется природно-климатической принадлежностью и зависит от флористического состава экотопа.

3.2) Для оценки величины почвенного критерия Q_{si}на основе известной шкалы, выделяется соотношение крепости пород и типов почв и дается среднее значение.

j] определяется оценочная стоимость C_{Si} и, соответственно, вычисляется оценка затрат на восстановление ущерба по критерию Q_{si}:

3.3) Критерий бонитета должен проводится на основе стандартных методик.

Q_{bi} оценивается по аналогии с вышеперечисленными.

3.4) Наличие водотоков определяется положительной или отрицательной величиной.

4) Суммарный показатель стоимости $C_{\sum i}$ восстановления ущерба в выделенной ОТЕ площадью S_i от воздействий указанных выше фактов является суммой стоимостей всех указанных критериев.

$$\sum_{i=0}^{n} C_i = Q_v + Q_s + Q_{n_i} \quad (3)$$

5) Выбор оптимальной зоны для падения ОС осуществляется из условия *min* $C_{\Sigma i}$ ОТЕ

Таким образом, методика позволит выполнять следующие функции:

– учет информации о литогенной основе, рельефе, типах почвогрунтов;

– подготовку информации о состоянии растительного покрова на основе архивных картографических данных и космоснимков;

– подготовку информации о сезонности и анализ климатических данных;

– анализ справочных данных о пожарной безопасности по показателям горючести и воспламенения;

– учет и экономическая оценка мероприятий по ликвидации последствий падений ОС в РП;

– классификацию однородных групп объектов и анализ результатов зонирования РП.

Рисунок 4 – Методология выделения операционно-территориальных единиц

Таким образом автоматизированная оценка экологического ущерба на основе разрабатываемой информационно-прогностической системы представляется целесообразной и позволяет провести двустороннюю оценку –оценку экологического ущерба и оценить стоимость восстановительных работ на основе классификации операционно-территориальных единиц.

Заключение

Экологическая безопасность космической деятельности предоставляет собой серьезную научную проблему обеспечения национальной безопасности. В настоящее время, сознавая важность проблемы, разработчики космических средств руководствуются повышенными экологическими требованиями к надежности и безопасности разрабатываемых ракет космического назначения. Одновременно принимаются меры к снижению уровня воздействия на окружающую природную среду существующих ракетно-космических комплексов.

В основную концепцию разработки информационно-прогностической системы определения районов запуска и падений ракет-носителей сверхлегкого класса входят базовые положения по снижению техногенного воздействия ракетно-космической деятельности в районах падения космодрома Байконур, разработка методов выбора районов запуска и падения, автоматизации процессов оперативной оценки техногенного воздействия от момента пуска до ликвидации последствий пуска в районах падений.

Благодарности

Исследования проведены в рамках гранта Комитета науки Министерства образования и науки Республики Казахстан AP09258759 «Разработка модели информационно-прогностической системы определения районов запуска и падений ракет-носителей сверхлёгкого класса с учетом требований экологической безопасности».

Литература

1 Соглашение между Правительством Республики Казахстан и Правительством Российской Федерации по экологии и природопользованию на территории комплекса «Байконур» в условиях его аренды Российской Федерацией от 2 июня 2005 года.

2 Соглашение между Правительством Республики Казахстан и Правительством Российской Федерации о порядке взаимодействия в случае возникновения аварий при пусках ракет с космодрома «Байконур» от 18 ноября 1999 г. (Ратифицировано Законом РК от 22 мая 2006 года №141-111).

3 Кодекс Республики Казахстан от 2 января 2021 года № 400-VI «Экологический кодекс Республики Казахстан».

4 Я.Т. Шатров. Обеспечение экологической безопасности ракетно-космической деятельности. /Шатров. - г. Королев Моск.обл., 2009г. - С. 709.

5 Т.В. Наумова. Концептуальные основы оценки экологического ущерба // Научный вестник МГТУ ГА. Серия Эксплуатация воздушного транспорта и ремонт авиационной техники. Безопасность полетов, № 86(4), 2005. - С. 116-120.

6 И. К. Епифанов, А. Д. Кондратьев, В. Дорошин. Экологический ущерб при аварии ракет-носителей на активном участке полета //Угрозы и безопасность, № 24 (57), 2009. - С. 53-55.

РАЗВИТИЕ ЦИФРОВОЙ ГРАМОТНОСТИ УЧАЩИХСЯ С НАРУШЕНИЯМИ СЛУХА В СПЕЦИАЛЬНЫХ (КОРРЕКЦИОННЫХ) ШКОЛАХ

А.Е. Ибраимкулов[1] , А.С.Еримбетова[2]
[1,2]Институт информационных и вычислительных технологий, Алматы, Казахстан
[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[1]aibek_ibraimkulov@mail.ru, [2]aigerian@mail.ru
[1]ORCID ID: https://orcid.org/0000-0002-9337-9595
[2]ORCID ID: https://orcid.org/0000-0002-2013-1513

Аннотация. *Цифровая грамотность – это набор знаний и навыков, необходимых для безопасного и эффективного использования цифровых технологий и интернет-ресурсов. В современных условиях информационные технологии и цифровая трансформация являются основным фактором технологических изменений и условием обеспечения в образовании цифровых учебно-методических комплексов. Статья посвящена формированию цифровой грамотности при обучении детей с нарушениями слуха на основе двух компонентов: цифровой пользовательской компонент, цифровой коррекционно-интеллектуальной компонент, которые разработаны авторами. Описанный авторами созданный курс по информатике направлен на повышение цифровой грамотности учащихся с ограниченными возможностями.*

Ключевые слова: *образование, цифровая грамотность, информатика, учащиеся с нарушениями слуха, компоненты цифровой грамотности.*

В нашей стране цифровизация системы образования является одним из ведущих направлений в процессе ее реформирования. В соответствии с Государственной программой "Цифровой Казахстан", утвержденной Постановлением Правительства Республики Казахстан (12 декабря 2017 года), предусмотрен целевой показатель по повышению уровня цифровой грамотности населения к 2022 году до 83% (2019 – 78.5%; 2020 – 80%; 2021 – 81.5%). Согласно Государственной программе "Цифровой Казахстан" цифровая грамотность состоит из двух групп: базовых и профессиональных цифровых навыков.

Первые базовые цифровые навыки включают следующие пять компетенций:

- Базовые цифровые навыки, включая уверенное использование персонального компьютера и ноутбука, мобильных устройств, Интернета, безопасности и защиты данных;
- Навыки использования "электронного правительства" и государственных услуг, в том числе получения необходимых электронных государственных услуг "онлайн", не выходя из дома;
- Навыки использования Открытого правительства, которые включают в себя использование четырех компонентов Открытого правительства;
- Навыки "Электронной коммерции", которые включают навыки покупки, продажи и продвижения товаров и услуг "онлайн";

- Навыки информационной безопасности, включая защиту персональных данных, защиту ПК, планшетов, смартфонов и т.д., защиту в Интернете, защиту во время финансовых операций.

Вторые профессиональные цифровые навыки включают пять основных цифровых навыков компетенций:

- Медиа-навыки – навыки использования цифровых устройств (цифровых фотоаппаратов, видеокамер и т.д.);
- Профессиональные цифровые навыки – навыки использования программных и аппаратных решений в профессиональной деятельности.

Цифровая грамотность является важной областью обучения для всех учащихся, которые могут участвовать в обучении, отдыхе и работе в XXI веке [1]. Это может позволить учащимся с ограниченными возможностями использовать современные цифровые технологии в качестве творческого инструмента обучения. Термину "цифровая грамотность" уделяется много внимания в различных секторах сферы, в том числе в образовании, изучаются проблемы от цифровизации образования до формирования и развития цифровой грамотности преподавателей и студентов, но ограниченное внимание уделяется обучению студентов с ограниченными возможностями и различными образовательными потребностями. Цифровая грамотность открывает возможности для всех учащихся, особенно для людей с ограниченными возможностями. Например, использование ряда вспомогательных инструментов, таких как веб-приложение, в качестве онлайн-интернет-инструмента в классе предоставляет учащимся с ограниченными возможностями новые способы взаимодействия с учебным контентом, восприятия материала и выражения своего понимания этого контента.

Различные исследователи представили определения цифровой грамотности и провели ряд исследований по цифровой грамотности [2, 4-6] и исследования навыков цифровой грамотности для учащихся с помощью усовершенствованных педагогических методов [9,11]. Проанализировав цифровую грамотность, авторы отметили использование цифровых технологий, которые обладают большим педагогическим потенциалом, учащихся смогут уверенно использовать их в учебе и в жизни. Согласно с Martin, A. (2008) *цифровая грамотность* – это осознание, отношение и способность людей надлежащим образом использовать цифровые инструменты и средства для идентификации, доступа, управления, интеграции, оценки, анализа и синтеза цифровых ресурсов, создания новых знаний, создания средств массовой информации и общения с другими в контексте конкретных жизненных ситуаций, чтобы обеспечить конструктивное социальное действие и размышлять об этом процессе. В начале XXI века Eshet-Alkalai, Y. в своем исследовании [8], в котором говорится, что «Цифровая грамотность включает широкий спектр сложных когнитивных, моторных, социологических и эмоциональных навыков, необходимый пользователям для эффективного функционирования в цифровой среде», предложил новую концептуальную основу концепции цифровой грамотности, включающую пять типов грамотности: (а) фото-визуальная грамотность; (б) репродуктивная грамотность; (в) информационная грамотность; (г) разветвленная (branching) грамотность; (е) социально-эмоциональная грамотность. По мнению автора, эти виды цифровой грамотности охватывают большинство когнитивных навыков, используемых при использовании

цифровой среды. Соответственно, эта концептуальная основа может улучшить понимание того, как пользователи выполняют задачи, требующие использования различных типов цифровых навыков.

Учащиеся с нарушениями слуха, в отличие от учащихся без нарушений слуха, обладают рядом особенностей, создающих трудности в овладении содержанием образования, поэтому при организации учебного процесса содержание, педагогические методы, формы обучения и средства обучения должны быть адаптированы в зависимости от степени нарушения слуха.

Особенности психики ребенка с нарушением слуха развиваются по-разному по сравнению со слышащими детьми (наблюдается диспропорция в развитии наглядно-образного и словесно-логического мышления; письменная речь во всех формах-выразительной (чтение) и выразительной (письмо) приобретает большую роль по сравнению с устной; выразительная форма речи преобладает над выразительной. Эту особенность следует учитывать при организации обучения и воспитания детей с нарушениями слуха.

Для формирования и развития цифровой грамотности детей с нарушением слуха необходимо определить компоненты цифровой грамотности с учетом их психологических, педагогических возможностей. Рассмотрим особенности слабослышащих, влияющие на их учебную деятельность в учебном процессе:

- Сниженная способность получать информацию, а также ее хранение, т. е. проблемы с запоминанием, обработкой и использованием информации;
- Замедление процесса формирования концепций;
- Дети с нарушениями слуха медленнее распознают объекты по сравнению со слышащими детьми;
- Сложные фразы очень трудно воспринимаются, искажают грамматическую структуру предложения во время речи, недостаток словарного запаса;
- Требуется больше времени, чтобы выделить информативные особенности предмета.

В ходе исследования, с учетом авторских рекомендаций различных ученых по компонентам цифровой грамотности, мы сформулировали собственную двухкомпонентную модель цифровой грамотности учащихся с нарушениями слуха для повышения цифровой грамотности в дополнительном курсе информатики:

1) Компонент цифрового пользователя;
2) Коррекционно-интеллектуальный компонент.

Наш подход к формированию и повышению цифровой грамотности студентов с нарушением слуха основан на коррекционных когнитивных путях. На основе предложенных двух компонентов мы разработали адаптированную программу курса. Этот курс рассчитан на 34 часа в год. Во время курса студенты могут экспериментировать с цифровыми платформами, инструментами и узнавать об исследованиях и разработке программ в области цифровой грамотности. При разработке программы мы уделили время рассмотрению взаимодействия между двумя компонентами. Программа курса состоит из 4 модулей (таблица 1).

Таблица 1. Модуль курса

Компоненты	
Компонент цифрового пользователя	Коррекционно-интеллектуальный компонент
Модули	

Инженерно-техническая подготовка	Компьютерная графика и 3D моделирование
	Создание мобильного приложения
	Цифровой исследовательский проект

Стратегия формирования цифровой грамотности учащихся с ограниченными физическими возможностями должна включать работу по снижению неравенства в доступе к цифровым технологиям путем разработки дополнительных образовательных курсов. В школьном курсе задача формирования и развития цифровой грамотности учащихся рассматривалась как часть предмета «Информатика». Учебный процесс, организованный на занятиях по информатике, должен обеспечивать формирование у студентов готовности к творческому саморазвитию и получению новых знаний. Для развития цифровой грамотности по предмету информатика важно организовать дополнительные курсы. Поэтому авторами был составлен курс по информатике, охватывающие все вышеперечисленные компоненты цифровой грамотности. В рамках дополнительного курса информатики особое внимание уделяется развитию «слуховых и речевых навыков», а также их творческих, когнитивно-визуальных навыков, например, связанных с компьютерной графикой, созданием 3D-модели, разработкой мобильных приложения, создание проектов в среде MS Project, а также конфигурация и настройки компьютера, работа в различных программах, работа с информационными ресурсами сети, приложениями Интернет-сервисов. Итак, наш курс разработан на основе модульных технологий и разделен на четыре основных модуля (Таблица 2).

Таблица 2. Описание курса и методы обучения

Модуль	Описание	Методы обучения
1. Инженерно-техническая подготовка	Установка, запуск, удаление, обновление программ. Установка операционной системы. Увеличение скорости компьютера. Работа с драйверами и периферийными устройствами. Удаленное управление компьютером	Метод решения инженерных и проектных задач
2.Компьютерная графика и 3D моделирование	Разъяснение концепции компьютерной графики. Типы. Области применения. Значимость. Программы для работы с компьютерной графикой. Описание 3D моделирования. Примеры.	Создание и проектирование объектов
3. Создание мобильного приложения	История, интересные факты о мобильных технологиях и приложениях. Способы создания мобильных приложений.	Метод проектов

4. Цифровой исследовательский проект	Студенты используют компьютерные программы по разным темам и разрабатывают проекты, используя разные методы.	Индивидуальная, групповая работа

Все темы данного курса полностью ориентированы на формирование личностных характеристик выпускника, владеющего основами научных методов познания окружающего мира, мотивированного на творческий и новаторский подход, получение новых знаний, готовность к сотрудничеству в любых ситуациях, умеет проводить учебно-исследовательскую, конструкторскую и информационно-познавательную деятельность; осознавая себя человеком, социально активным гражданином страны.

Заключение. Результаты данного исследования можно понимать как формирование цифровой грамотности при обучении детей с ограниченными возможностями на основе двух компонентов: цифровой пользовательской составляющей, цифровой коррекционной и интеллектуальной составляющей. С помощью разработанного авторами статьи дополнительного курса информатики, направленного на повышение цифровой грамотности студентов с ограниченными физическими возможностями, обосновывается тематическое содержание учебных разделов курса. В компоненте «Цифровой пользователь» студенты смогут узнать об инженерном обучении. Например: установка программного обеспечения, удаление, обновление, очистка и т. д. В цифровой коррекционно-интеллектуальной составляющей студенты смогут улучшить свои навыки: когнитивные, логические, критические, творческие, системное мышление, память, воображение, внимание, речь, общение с помощью различных задач и программ. Для развития цифровой грамотности по предмету информатика важно организовать дополнительные курсы. Поэтому авторы составили свои курсы по информатике, охватывающие все вышеперечисленные компоненты цифровой грамотности.

Данное исследование финансируется Комитетом науки Министерства образования и науки Республики Казахстан (Грант № AP09057872)

Литература

1. Digital education for a strong recovery: A forward look, 2021 OECD https://oecd-events.org/digital-education

2. Gilster, P. (1997). Digital literacy. New York: Wiley

3. Martin, A. (2008). Digital literacy and the “digital society”. In C. Lankshear & M. Knoebel (Eds.), *Digital literacy: Concepts, policies and practices* (pp. 151–176). New York, NY: Peter. Google Scholar

4. Neumann, M. M., Finger, G., & Neumann, D. L. (2017). A conceptual framework for emergent digital literacy. Early Childhood Education Journal, 45(4), 471–479. doi:10.100710643-016-0792-z

5. Lankshear, C., & Knobel, M. (Eds.). (2008). Digital literacies: Concepts, policies and practices (Vol. 30). Peter Lang.

6. Erez Porat, Ina Blau, Azy Barak (2018) Measuring digital literacies: Junior high-school students' perceived competencies versus actual performance. Computers & Education, Volume 126, 2018, Pages 23-36. Https://doi.org/10.1016/j.compedu.2018.06.030.

7. Bawden, D. (2001). Information and digital literacies: A review of concepts. Journal of Documentation, 57(2), 218–259.

8. Eshet-Alkalai, Y. (2004). Digital literacy: A conceptual framework for survival skills in the digital era. *Journal of Educational Multimedia and Hypermedia, 13*, 93–106.Google Scholar

9. Allan Martin & Jan Grudziecki (2006) DigEuLit: Concepts and Tools for Digital Literacy Development, Innovation in Teaching and Learning in Information and Computer Sciences, 5:4, 249-267, DOI: 10.11120/ital.2006.05040249

10.Harish Kumar Sahu (2019). Digital Literacy Skills: A Study. Res. J. Humanities and Social Sciences.10(2):311-313. doi: 10.5958/2321-5828.2019.00055.X

11.Kuznekoff, Jeffrey & Munz, Stevie & Titsworth, Scott. (2019). Digital Inequality and Digital Literacy Skills. 10.4324/9780429355097-4.

ЧИСЛЕННЫЙ И ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ ОПРОСА СОГЛАСОВАННОГО ФИЛЬТРА ДАТЧИКОВ НА ОСНОВЕ ВРБ

Вуйцик[1,2] В., Кисала[1,2] П., Калижанова[1,3] А.У., Козбакова[1,4] А.Х.,
Кунелбаев[1] М., Едилхан[1,5] Д., Айткулов[1,6] Ж.С.
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Люблинский технический университет, Польша
[3]Алматинский университет энергетики и связи, Казахстан
[4]Алматинский технологический университет, Казахстан
[5]Астана IT университет, Казахстан
[6]Академия логистики и транспорта, Казахстан
e-mail: waldemar.wojcik@pollub.pl, kalizhanova_aliya@mail.ru

Аннотация. *В статье представлено влияние боковых лепестков волоконных решеток Брэгга на системы опроса, состоящие из датчика и согласованных фильтров. Проведенные исследования показывают, что высокоэффективные структуры боковых лепестков, применяемые в качестве датчиков или фильтров, обладают некоторыми интересными свойствами. В статье представлен как численный анализ, так и экспериментальная проверка системы опроса волоконных решеток Брэгга (ВРБ) с согласованными фильтрами для решеток с высокими боковыми лепестками. Было продемонстрировано, что высокий уровень боковых лепестков может быть использован для увеличения диапазона измерения систем опроса датчиков с волоконной решеткой Брэгга. Численно и экспериментально подтверждено, что с точки зрения проектирования систем опроса датчиков выгодно комбинировать определенные пары решеток: одна со спектром, характеризующимся низким уровнем боковых лепестков, и вторая, в которой спектр имеет очень высокие боковые лепестки.*

Ключевые слова: *волоконная решетка Брэгга, датчики ВРБ, опрос, аподизация.*

1. Введение

Преимущества датчиков с волоконными решетками Брэгга (ВРБ) обусловили их высокую популярность и расширили область их применения [1–7]. Эти преимущества можно разделить на две группы. В первую группу входят такие свойства всех оптоволоконных датчиков, как малый размер, вес и возможность удаленных измерений [8]. Вторая группа является результатом модуляции длины волны света, который отражается или проходит через решетку (рис. 1). Свойство спектральной трансдукции датчиков ВРБ означает, что изменения измеряемой величины, такие как удлинение и температура, преобразуются в сдвиг длины волны. В свою очередь, требуется применение соответствующего метода демодуляции для изменения сдвига длины волны в зависимости от интенсивности излучения. Было предложено множество схем опроса [9], включая портативные энергоэффективные интеррогаторы, основанные на спектральной свертке между датчиками и настраиваемыми фильтрами [10].

Метод, основанный на анализе электрических гармоник, который требует гармонического модулятора и соответствующего сбора сигналов, обсуждался в работе [11]. Это немного более сложное решение. Более того, эта конкретная математическая модель предназначена для опроса на решетках с большим периодом

(long period grating -длиннопериодная решетка, ДПВР-LPG). Дополнительными особенностями метода опроса могут быть нечувствительность к изменениям интенсивности источника света, а также нечувствительность к изменениям затухания на всем оптическом пути. Преимуществом также является возможность наличия нескольких датчиков ВРБ (различающихся по длине волны) на одном тракте передачи. Изменения физической величины, такой как удлинение, сила или температура, приводят к изменению параметров решетки - в основном ее периода и, следовательно, к спектральному сдвигу ее спектральных характеристик. В процессе измерения заданной физической величины следует определять сдвиг длины волны Брэгга. Это можно сделать несколькими способами. Основной метод - использование широкополосного источника света и анализатора оптического спектра (АОС-OSA). Этот метод чаще всего используется на этапе разработки конкретного датчика или в лабораторных испытаниях.

Анализаторы оптического спектра позволяют проводить измерения с очень высоким разрешением; однако они очень дороги и не являются портативными из-за их значительного веса и размера. Другие популярные методы демодуляции с использованием широкополосных источников света включают интерферометрические методы и методы с использованием оптических фильтров. Примеры включают интерферометр Фабри – Перо [12], а также краевые фильтры с различными спектральными характеристиками [13]. Для преобразования сдвига спектра ВРБ в мощность фотоприемника можно использовать оптический элемент, спектральные характеристики которого монотонно зависят от длины волны. Самым простым компонентом этого типа является источник излучения. Однако это решение не является гибким, поскольку спектральные характеристики источника света не могут быть произвольно сформированы. Многие другие варианты и возможности для формирования и выбора передаточных характеристик сенсорной системы могут быть достигнуты с помощью различных типов оптических фильтров.

Существует два типа фильтров: один со спектром, намного более широким, чем у датчика, и другой, с шириной спектра, подобной спектру датчика сенсора. Они называются широкополосными краевыми фильтрами и согласованными фильтрами [14,15] и имеют спектр, аналогичный спектру самого датчика. Дальнейшее улучшение свойств таких систем может быть достигнуто за счет использования техники параллельного согласования [16,17]. Во втором примере используются правильно подобранные периодические структуры ВРБ. Это решение относительно дешево и обеспечивает соответствующие параметры датчика, такие как чувствительность и линейность. Здесь можно использовать две основные конфигурации, в которых мощность, передаваемая (Рисунок 1a) или отраженная (Рисунок 1b) через решетку датчика, измеряется фотодетектором. В зависимости от формы спектров решеток, используемых в пропускающей и отражающей системах, можно получить несколько разные свойства (рис. 1).

Системы с опросом согласованного фильтра рассматривались в литературе в различных аспектах, например, с точки зрения линейности или скорости работы [16]. При рассмотрении форм передаточных характеристик датчика наиболее важной задачей системы оптических фильтров является достижение надлежащей линейности или увеличение динамического диапазона системы [18]. Похоже, что системы, содержащие согласованный фильтр, можно адаптировать к приложениям;

кроме того, они позволяют выбирать диапазон измерения в зависимости от ширины их спектра. К тому же они очень быстрые и отличаются хорошей точностью. В некоторых случаях для настройки длины волны фильтрующих решеток можно использовать пьезоэлектрический преобразователь (PZT- piezoelectric transducer) [19]. Однако следует отметить, что по сравнению со статической системой это вызывает как системные сложности, так и значительное увеличение затрат.

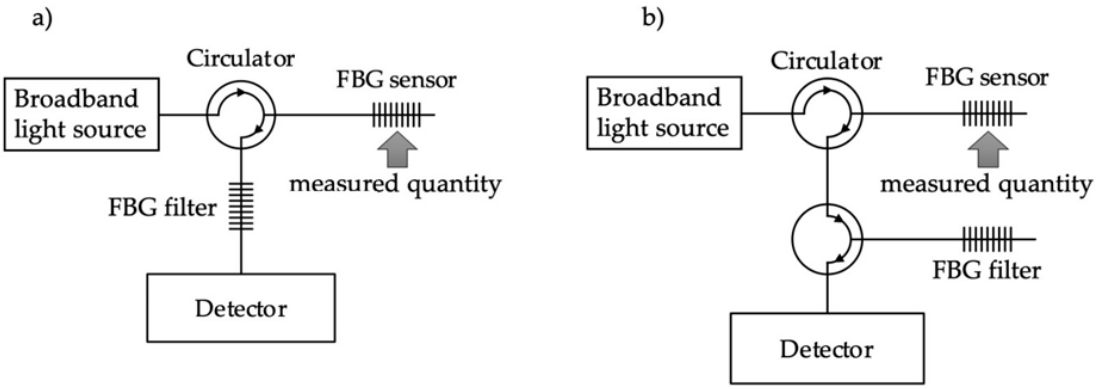


Рис. 1 Базовые конфигурации систем опроса: (а) пропускающая; (б) отражающая

Следует подчеркнуть, что в литературных источниках основное внимание уделяется датчикам и фильтрам гауссовой формы. Это связано с тем, что такой анализ относительно прост и позволяет даже получить аналитические формулы зависимости оптической мощности от сдвигов длины волны Брэгга [6].

Для других форм сравнения можно проводить только численными методами. Решетки с гауссовой формой спектра являются аподизированными структурами; таким образом, у них нет боковых лепестков в спектре. Создание ВРБ с идеальной гауссовой формой и в то же время с высоким значением коэффициента отражения - сложная задача. Идеальная гауссова форма может быть достигнута только для слабых структур с низким коэффициентом отражения. В целом, если получить более высокий коэффициент отражения, то большая мощность может достигать детектора, и, таким образом, достигается больший динамический диапазон.

Динамический диапазон и линейность системы зависят от полной ширины на полувысоте (FWHM- full width at half-maximum) структуры ВРБ. К сожалению, расширение параметра FWHM гауссовой ВРБ часто связано с уменьшением ее отражательной способности. Точный анализ и формулы для мощности, полученной на детекторе, в зависимости от сдвига длины волны Брэга можно найти в нескольких публикациях [18]. Второй тип решеток, предложенный в литературе, это система опроса согласованных фильтров с прямоугольной формой спектра. Это решение обеспечивает линейную зависимость между мощностью детектора и изменением измеряемой физической величины. Прямоугольную форму спектра можно получить с помощью волоконных чирпированных брэгговских решеток (ЧВРБ, chirped fiber Bragg gratings- CFBGs) [20].

В общем, передаточные характеристики систем опроса согласованных фильтров состоят из двух областей. Первая - это линейная область, характеризующаяся высокой чувствительностью. Вторая область находится в диапазоне длин волн, близком к длине волны Брэгга. Эта часть называется брэгговской областью, в сильных решетках она сплющена из-за насыщения спектральных характеристик. Как для широкополосных фильтров, так и для

согласованных фильтров, можно моделировать характеристики края спектра, используя параметры чирпа и аподизации [21]. Формирование преобразования между изменением длины волны и интенсивности путем согласования формы спектров позволяет получить правильное решение для конкретного приложения с требуемым диапазоном измерения. Для краевых фильтров можно выбрать форму только одного края фильтра, в то время как для системы согласованных фильтров формы обеих структур должны быть выбраны для датчика и фильтра.

Существует два основных типа систем опроса, использующих ВРБ. На рисунке 1 показаны диаграммы пропускающей и отражающей мод.

В данной работе рассмотрен вопрос о влиянии боковых лепестков брэгговских решеток на метод опроса согласованного фильтра в моде отражения. Анализируются свойства, которые можно получить, используя структуры с высоким боковым лепестком. Основной вопрос заключается в том, как боковые лепестки влияют на передаточные характеристики измерительной системы. Исследуется возможность формирования таких характеристик и увеличения диапазона измерений. Кроме того, изучен специально подобранный метод аподизации (обратная аподизация) для получения боковых лепестков со значительной отражательной способностью и определения их влияния на свойства системы опроса [22,23].

2. Моделирование спектров волоконных решеток Брэгга с боковыми лепестками с высоким коэффициентом отражения

Значительный уровень боковых лепестков в спектрах характеризует однородные ВРБ без предполагаемой аподизации. Следует добавить, что в большинстве приложений это нежелательное свойство. Появление боковых лепестков искажает спектральные характеристики ВРБ. В случае их использования, например, в телекоммуникациях, это вызывает искажения сигналов, которые подлежат такой фильтрации. Чтобы определить влияние различных уровней боковых лепестков на системы опроса, во-первых, следует определить метод создания структур с такими свойствами. Численное моделирование и математические модели для спектров ВРБ подробно обсуждались [24,25]. Численные расчеты проводились в программе OptiGrating, в результате чего были получены спектральные характеристики ВРБ. В модель введены структурные параметры световода, соответствующие SMF-28e +. Длина и глубина модуляции показателя преломления решеток подбирались таким образом, чтобы полученные спектры характеризовались одинаковым коэффициентом отражения и значением FWHM главного лепестка. Были рассчитаны различные профили аподизации, в результате чего форма спектров имела разные значения коэффициента отражения боковых лепестков. Таким образом, можно было сравнить системы опроса ВРБ с разной силой боковых лепестков. Параметр, который влияет на коэффициент отражения боковых лепестков, - это аксиальная аподизация брэгговской структуры [1,26]. На рис. 2 представлены профили аподизации, использованные в расчетах. Численные расчеты проводились для структур длиной 2 мм. Функция аподизации g (z) описывалась следующим уравнением:

$$g(z) = a\,\mathrm{tgh}(z) \cdot a\,\mathrm{tgh}(1 - z) \cdot (b\cos(2\pi z) + 1)$$

где a и b - константы, оба параметра волоконной решетки Брэгга, рассчитанные для анализа, со значениями, указанными в таблице 1.

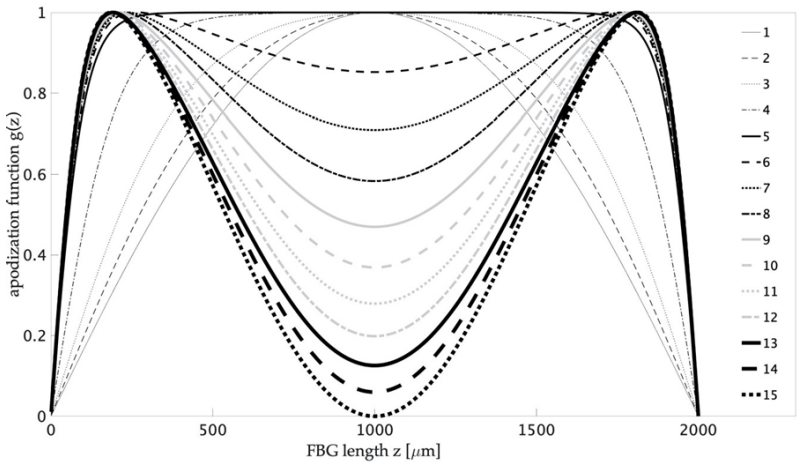


Рис. 2 Профили аподизации, использованные при численном моделировании спектральных характеристик волоконных решеток Брэгга (ВРБ)

Модуляция показателя преломления изменялась в диапазоне от 2 до 4×10^{-5} и чтобы показатель отражения R был одинаковым для всех структур. Сплошными линиями отмечены три опорные формы профиля: гауссовский, равномерный и полностью перевернутый. Промежуточные профили отмечены пунктирными линиями.

На рис. 3 показаны спектры отражения смоделированной ВРБ. Коэффициент отражения всех структур был равен 1, а параметр FWHM варьировался от 0,44 до 0,62 нм. Для анализа полученных результатов использовался параметр K, характеризующий спектры ВРБ, определяемый как отношение максимального коэффициента отражения бокового лепестка первого порядка к коэффициенту отражения главного лепестка. Для профиля аподизации, подобного распределению Гаусса, параметр K был равен 0. Форма аподизации, близкая к прямоугольнику (однородная), давала боковые лепестки с коэффициентом отражения 0,08 и K = 0,1. Получение более высокого коэффициента отражения боковых лепестков возможно за счет использования инвертированных профилей аподизации. Максимальное расчетное значение коэффициента отражения боковых лепестков составило 0,5318, а коэффициент K был равен 0,7014.

Таблица 1. Рассчитанные для анализа параметры волоконных решеток Брэгга.

Номер структуры	a Коэффициент	b Коэффициент
1	2	0
2	3	0
3	5	0
4	10	0
5	20	0
6	20	0,1
7	20	0,2
8	20	0,3
9	20	0,4
10	20	0,5
11	20	0,6
12	20	0,7

13	20	0,8
14	20	0,9
15	20	1

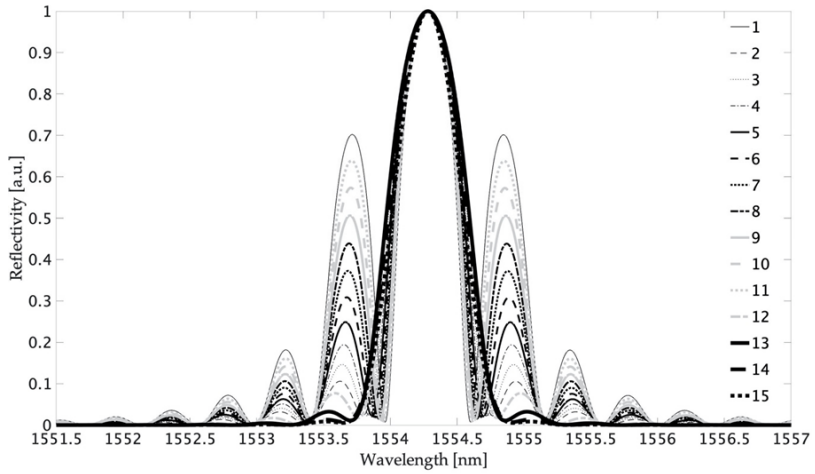


Рис. 3 Спектры волоконных решеток Брэгга для профилей аподизации с рис. 1

Проведено моделирование работы систем опроса с согласованным фильтром. Расчеты основаны на двух численных операциях со спектрами. Во-первых, это сдвиг спектральных характеристик одной волоконной решетки Брэгга (датчика) при фиксированном (несмещенном) спектре другой решетки. Далее определяется произведение спектров, соответствующее общей части характеристики. Зависимость произведенной структуры спектров как функция смещения (спектрального сдвига) эквивалентна операции оптической фильтрации для различных пар решеток, которая показана на рисунке 4. Одним из параметров, который можно использовать для анализа результатов, является диапазон спектрального сдвига, в котором амплитуда выходного сигнала снижается до 5% от его максимального значения. Расчеты проводились для двух случаев. В первом случае формы двух спектров (фильтра и датчика) были идентичны. На рис. 4а показаны численно определенные характеристики системы опроса. Полученные кривые имели неправильную форму и не были монотонными. Во втором предложенном подходе в качестве опорной (фильтрующей) структуры был выбран наименьший спектр боковых лепестков, что соответствует решетке с аподизацией гауссова профиля. В качестве структуры датчика были выбраны спектры с ненулевыми боковыми лепестками и разными коэффициентами отражения. В этом случае взаимный спектральный сдвиг, представляющий измеренный диапазон (5% от максимальной интенсивности), имел наименьший диапазон 0,753 нм. При более высоких уровнях боковых лепестков ширина передаточных характеристик увеличивалась и достигла значения 1,632 нм для пары смоделированных спектров решетки 1 и 15.

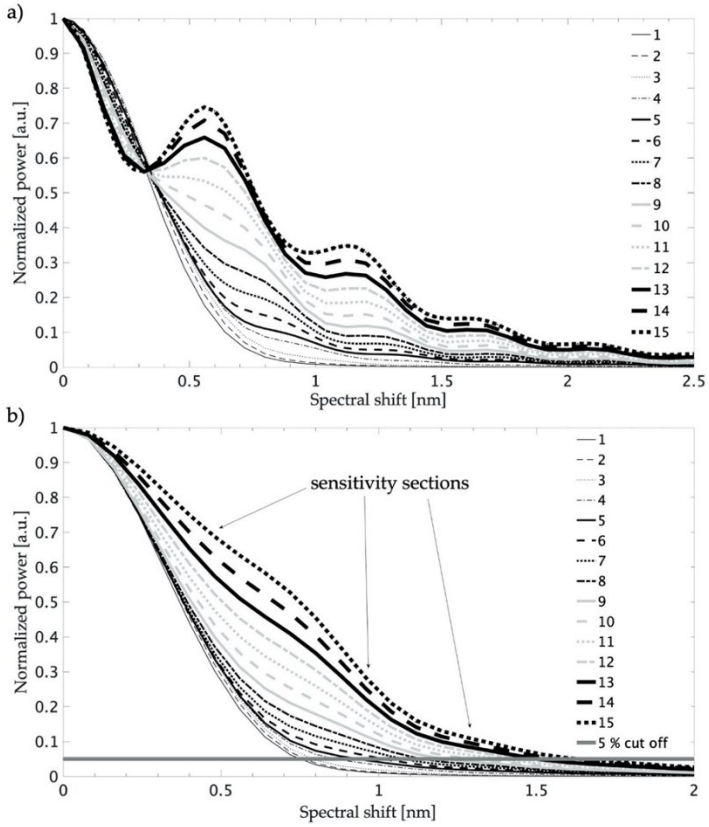


Рис. 4 Сравнение формы передаточных характеристик системы согласованных фильтров: (а) две аналогичные структуры; (б) однородная ВРБ1 с одним из фильтров ВРБ1 – ВРБ15

Передаточные характеристики датчиков с системой опроса представлены на рисунке 4б. Отдельные кривые имели различный наклон, а в некоторых диапазонах характеристики были линейными. Наклон этой кривой определяет чувствительность системы опроса. Наибольшая чувствительность была получена для системы с двумя ВРБ с наименьшими боковыми лепестками (зеленая линия). Эта чувствительность составила 1854 а.е. на нм. Для системы с двумя разными ВРБ (одна с боковыми лепестками и одна без боковых лепестков) можно выделить два или три диапазона передаточных характеристик, для которых форма характеристики близка к линейной. Это свойство важно для многих приложений датчиков с ВРБ в реальных измерительных системах. Наклоны отдельных частей характеристики были разными; таким образом, менялась и чувствительность сенсорной системы. Для структур ВРБ, для которых K-фактор находился в диапазоне от 0,077 до 0,572, начальные участки кривых характеризовались более крутым наклоном; в средней части наклон имел промежуточное значение и был наименьшим среди больших значений спектрального сдвига. Передаточные характеристики, полученные при K = 0,31 (синяя линия), достигли чувствительности 1,515 а.е. на нм в диапазоне от 0,16 до 0,48 нм, 0,416 а.е. на нм в диапазоне от 0,64 до 1,04 нм и 0,076 а.е. на нм в диапазоне от 1,2 до 1,6 нм. При K = 0,64 (черная линия) чувствительности двух линейных участков передаточной характеристики были равны. В диапазоне от 0,16 до 0,56 нм чувствительность составила 0,905 а.е. на нм, а для диапазона от 0,8 до 1,04 нм чувствительность составила 0,909 а.е. на нм. В остальной части диапазона от 1,2 до 1,6 нм чувствительность равнялась 0,17 а.е. на нм. Переходная характеристика для структуры ВРБ15 и K = 0,70 (красная линия) достигла

максимальной чувствительности 0,99 а.е. на нм в центральной части характеристики в диапазоне от 0,72 до 1,04 нм. В диапазоне от 0,16 до 0,64 нм наклон составляет 0,755 а.е. на нм, и составила 0,194 а.е. на нм в диапазоне от 1,2 до 1,6 нм.

Поэтому, проанализировав моделирование, можно предположить, что более выгодно комбинировать пары решеток, в которых спектр первой характеризуется низким уровнем отражения боковых лепестков (предпочтительно нулевым), а второй, спектр которого имеет более высокое отражение боковых мод. Эти пары FGB могут увеличивать и формировать наклон переходной характеристики. Пары структур с одинаково высокими коэффициентами отражения боковых лепестков имеют несколько разные свойства. Их передаточные характеристики немного шире, что приводит к большему диапазону измерения, но форма характеристики нерегулярна и трудна для моделирования.

3. Экспериментальная проверка

Для экспериментальной проверки была изготовлена группа волоконных решеток Брэгга с различными спектральными характеристиками. В таблице 2 приведены параметры анализируемых волоконных решеток Брэгга.

Таблица 2. Параметры изготовленных для анализа волоконных решеток Брэгга.

	***K* [0..1]**	**Отражение Reflection [0..1]**	**FWHM [nm]**
ВРБ1	0.0217	0.775	0.380
ВРБ2	0.1882	0.9165	0.664
ВРБ3	0.5615	0.5615	0.360
ВРБ4	0.7178	0.7178	0.372
ВРБ5	0.8260	0.8260	0.520

Структуры ВРБ были изготовлены с использованием метода фазовой маски, в котором реализована система заслонок пучка, позволяющая управлять профилем аподизации записываемых структур. Коэффициент К варьировал от 0,0217 до 0,826. На рисунке 5 показаны спектральные характеристики записанных структур.

Полученные структуры имели разную полуширину и отражательную способность. Для сравнения свойств был нормирован коэффициент отражения. После этого численные расчеты были выполнены аналогично расчетам, выполненным для смоделированных спектров. На рисунке 6 показаны рассчитанные характеристики опроса.

Форма характеристик соответствовала результатам численных расчетов. Наблюдались заметные диапазоны передаточных характеристик с разным наклоном, соответствующие основному пику Брэгга и амплитуде первого бокового лепестка. Для пар ВРБ1 с ВРБ4 и ВРБ5 максимальная чувствительность была получена в среднем диапазоне передаточных характеристик. Для пар ВРБ1 с решетками ВРБ3 и ВРБ2 наибольший наклон характеристики был получен в начальном диапазоне. Затем чувствительность уменьшилась в середине переходной характеристики и еще больше уменьшилась в финальной части. С учетом уровня отсечки характеристики 5% диапазон измерения увеличился вдвое, с 0,62 до 1,22 нм.

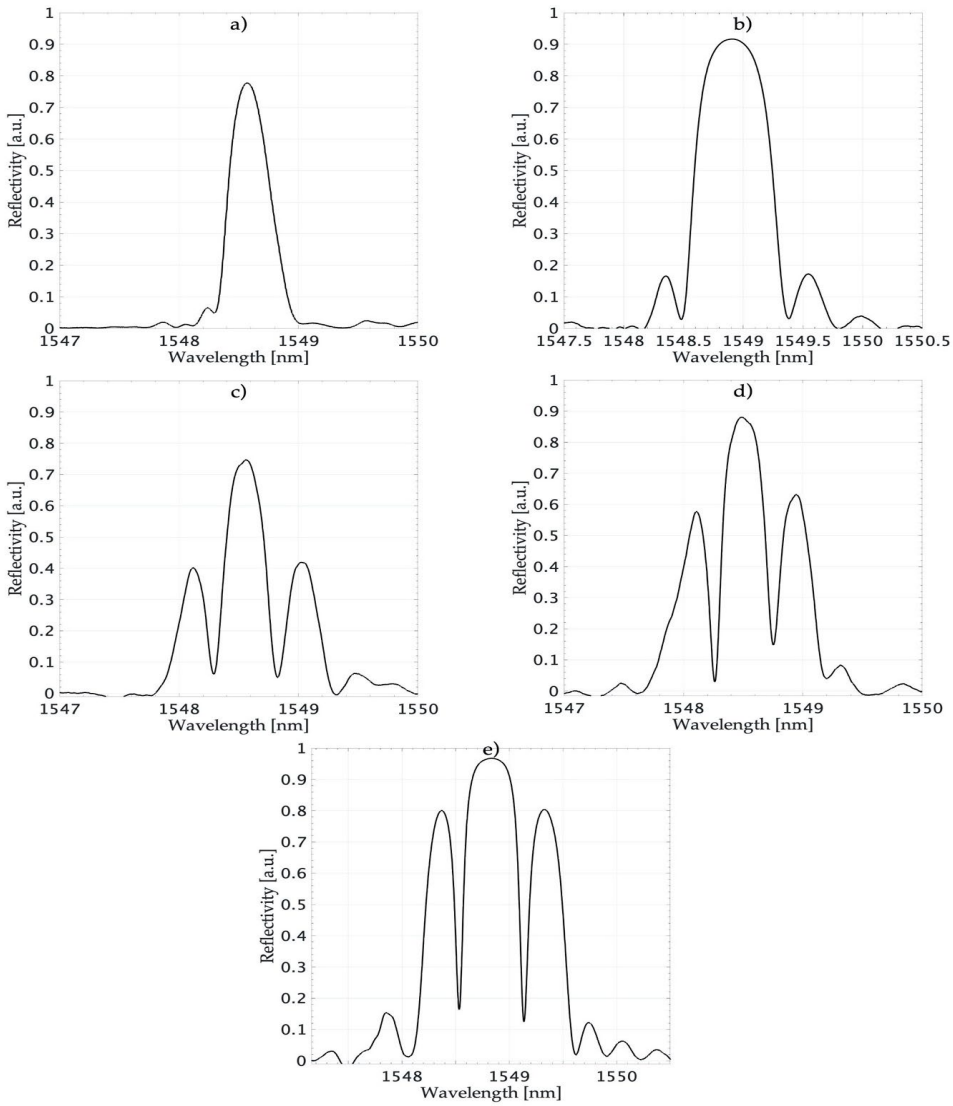


Рис. 5 Спектральные характеристики изготовленных ВРБ: (а) ВРБ1; (б) ВРБ2; (с) ВРБ3; (d) ВРБ4; (е) ВРБ5

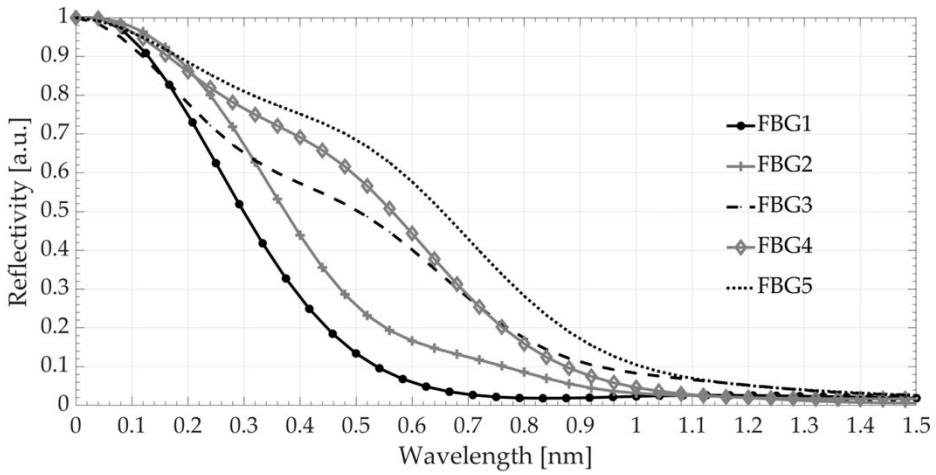


Рис. 6 Расчетные передаточные характеристики на основе спектров реальных структур

Экспериментальная проверка проводилась на специально подобранных изготовленных структурах, упомянутых ранее. Схема системы опроса представлена на рисунке 7. В качестве датчика ВРБ использовалась структура ВРБ1 с наименьшим К-фактором. В качестве фильтра ВРБ использовались две ВРБ с разными боковыми лепестками. Структура датчика была помещена в климатическую камеру, температура которой изменялась от 0 до 180 градусов Цельсия. На рисунке 8 показаны схема и изображение измерительной системы.

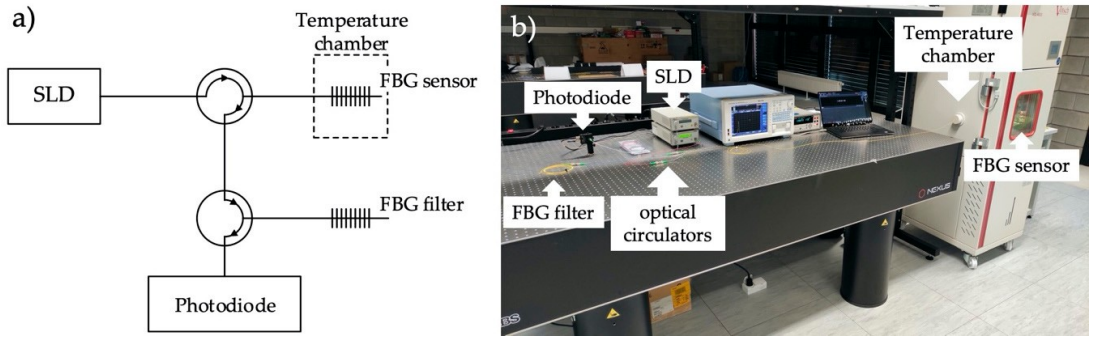


Рис. 7 Схема (а) и изображение (б) экспериментального стенда для тестирования передаточных характеристик системы волоконных брэгговских решеток

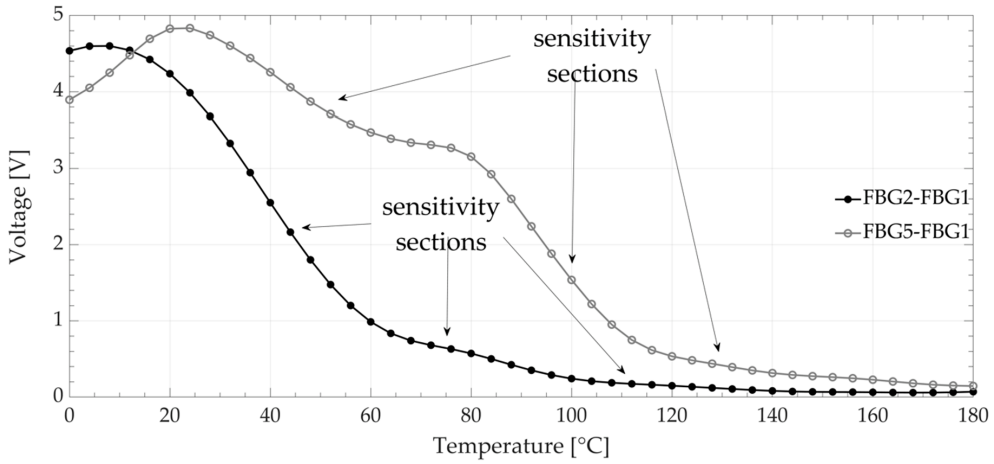


Рис. 8 Экспериментальные передаточные характеристики

Экспериментально работа системы опроса ВРБ была подтверждена измерениями температуры внутри температурной камеры, в которую помещалась сенсорная решетка. В результате эксперимента были получены переходные характеристики, показанные на рисунке 8.

Экспериментальная проверка, проведенная для пар ВРБ2-ВРБ1 и ВРБ5-ВРБ1, подтвердила результаты численных расчетов. Кривая обработки системы допроса имела разный наклон на разных участках. Для первой пары волоконных брэгговских решеток (ВРБ2-ВРБ1) были получены значения чувствительности 0,0843, 0,0162 и 0,0036 (В / °С), а для чувствительности - 0,0379, 0,0822 и 0,0072 (В / °С). пара решеток ВРБ1-ВРБ5. Диапазон измерения температуры (уровень отсечки 5%) в представленной системе также изменился с 92° С для пары с меньшими боковыми

лепестками до 132 °C для пары с большими уровнями боковых лепестков (ВРБ5-ВРБ1).

4. Анализ полученных результатов

Обратная аподизация волоконных решеток Брэгга приводит к высокой отражательной способности их боковых лепестков. Вследствие этого увеличивается ширина передаточной характеристики опросных систем с такой ВРБ. Таким образом, непосредственно увеличивается и диапазон измерения. Для изготовленных структур, содержащих боковые лепестки, диапазон измерений увеличился с 0,583 до 1,2 нм. Процесс записи ВРБ с большой спектральной шириной без введения чирпа затруднен. FWHM более 1,5 нм достижима для коротких структур длиной менее 0,5 мм. Запись таких коротких ВРБ с высоким коэффициентом отражения затруднена, поскольку уменьшение длины структуры также снижает ее коэффициент отражения. Альтернативой являются чирпированные волоконные брэгговские решетки (ЧВРБ), но во многих производственных системах до недавнего времени было трудно получить такие структуры с высоким коэффициентом отражения и низкими значениями FWHM. В настоящее время появляются новые методы и возможности для получения ЧВРБ с высоким коэффициентом отражения и низкими значениями FWHM. Следовательно, их использование в системах опроса проблематично. ЧВРБ часто имеют неправильные значения отражения в своем спектральном диапазоне. Еще один эффект боковых лепестков - изменение чувствительности опросных систем на отдельных фрагментах передаточных характеристик. Высота боковых лепестков определяет максимальную чувствительность, которая может быть достигнута. Изменение значения отражательной способности боковых лепестков и FWHM решетки датчика будет регулировать чувствительность системы опроса, и это также позволяет управлять диапазоном измерения.

Спектральный диапазон измерений с использованием систем согласованных фильтров ограничен величиной FWHM структур датчика и фильтра, а также спектральным сдвигом между ними. Диапазон измерения длины волны коммерчески доступных интеррогаторов довольно широк и достигает 100 нм На практике измерение физических величин, таких как температура или деформация, ограничивается свойствами материала оптических волокон, используемых для создания датчика. Максимальная деформация оптического волокна с вписанными периодическими структурами ВРБ, используемого в качестве датчика деформации, обычно составляет 6000 με. В случае измерения температуры ограничением диапазона измерения является термостойкость волоконной брэгговской решетки и покрытия волокна. Для акрилового покрытия максимальная рабочая температура составляет около 85°C, а для полиамидного покрытия уже 300°C. Системы опроса с согласованным фильтром и структуры с высокой FWHM позволяют расширить диапазон измерения спектрального сдвига примерно до 3 нм. Это ограничивает измерение температуры значением около 270° C, а измерение деформации - значением около 2500 με.

Системы согласованных фильтров ВРБ позволяют получить частотную характеристику около 500 кГц и разрешение по длине волны 0,3 пм [16]. Коммерческие интеграторы достигают максимальной частоты 5 кГц и обычно 1 кГц. В исследуемом случае в результате повторных измерений достигли относительного разрешения $0{,}5 \cdot 10^{-3}$, что в случае диапазона измерения 1,2 нм означает разрешение 0,6 пм и разрешение измерения температуры 0,1° C в диапазон от 10°C до 120°C. Типичное разрешение измерений для коммерческого интеррогатора составляет 0,5

пм. Согласованные системы фильтрации также по крайней мере в пять раз дешевле, чем коммерчески доступные системы опроса.

Метод согласованных фильтров предназначен скорее для опроса одного датчика. Однако благодаря соответствующей системе демультиплексирования можно обнаруживать величины, измеряемые на основе сигналов от многих датчиков, расположенных на одном и том же оптоволокне. В случае систем AWG (Arrayed Waveguide Grating -упорядоченная волноводная решетка), концептуально подобных системам согласованных фильтров, можно мультиплексировать даже до 128 решеток. Следует подчеркнуть, что в таких системах форма спектральных характеристик датчика ВРБ не исключает использования решетки с высокими боковыми лепестками. Таким образом, можно построить распределенные датчики с использованием ВРБ с высокими боковыми лепестками. В свою очередь, возможность расширения диапазона измерения и возможность формирования и регулировки наклона передаточных характеристик датчика являются большими преимуществами использования таких решеток. В работе представлено, что самый широкий диапазон измерения и возможность формирования чувствительности имеют место для пар: датчик верхних боковых лепестков и фильтр нижних боковых лепестков или датчик нижних боковых лепестков и фильтр верхних боковых лепестков. Эти свойства и соображения, касающиеся ВРБ с высокими боковыми лепестками, представленные в документе, также применимы, например, к системам AWG, поскольку, в принципе, AWG представляют собой системы согласованных фильтров, состоящих из фильтров гауссовой формы с низкими боковыми лепестками. Следует отметить, что расширение диапазона измерения вызывает соответствующее расширение спектра, занимаемого одним датчиком, и уменьшает количество датчиков, которые могут быть размещены на одном оптическом волокне.

Заключение

В этой работе предлагается использовать боковые лепестки для расширения диапазона измерений датчика ВРБ, опрашиваемого с помощью однородной ВРБ. Расширение диапазона измерений было получено при небольшом изменении формы передаточных характеристик системы. Это решение сохраняет простоту измерительной системы и упрощает процесс изготовления ВРБ из-за отсутствия чирпа при записи структур в оптическое волокно. Использование предлагаемой измерительной системы меняет приложение, в котором нет необходимости в увеличении диапазона измерения, позволяет использовать пары структур ВРБ, которые легче изготавливать из-за более легкой адаптации к требуемому диапазону измерения.

Доказано, что правильный выбор параметров ВРБ позволяет разработать систему опроса со свойствами, оптимизированными для измерения конкретной физической величины с точки зрения согласования диапазона измерения и изменения чувствительности его отдельных частей.

Экспериментальные исследования проводились в лабораториях Оптоэлектроники факультета электротехники и компьютерных наук Люблинского технического университета в рамках проекта ГФ №AP09259547 «Разработка системы из распределенных волоконно-оптических датчиков на основе волоконных

решеток Брэгга для контроля состояния строительных конструкций» ИИВТ КН МОН РК.

Литература

1. Khalid, K.S.; Zafrullah, M.; Bilal, S.M.; Mirza, M.A. Simulation and analysis of Gaussian apodized fiber Bragg grating strain sensor. J. Opt. Technol. 2012, 79, 667–673. [CrossRef]
2. Liu, Z.; Zheng, D.; Madrigal, J.; Villatoro, J.; Antonio-Lopez, E.; Schulzgen, A.; Amezcua-Correa, R.; Zou, X.; Pan, W. Strongly coupled multicore fiber with FBGs for multipoint and multiparameter sensing. Opt. Fiber Technol. 2020, 58, 102315. [CrossRef]
3. Melo, L.; Rodrigues, J.; Farinha, A.F.; Marques, C.; Bilro, L.; Alberto, N.; Tomé, J.P.; Nogueira, R.N. Concentration sensor based on a tilted fiber Bragg grating for anions monitoring. Opt. Fiber Technol. 2014, 20, 422–427. [CrossRef]
4. Sahota, J.K.; Gupta, N.; Dhawan, D. Fiber Bragg grating sensors for monitoring of physical parameters: A comprehensive review. Opt. Eng. 2020, 59, 060901. [CrossRef]
5. Udd, E. Review of multi-parameter fiber grating sensors. In Proceedings of the Fiber Optic Sensors and Applications V, Boston, MA, USA, 10–12 September 2007.
6. Wild, G.; Richardson, S. Analytical modeling of power detection-based interrogation methods for fiber Bragg grating sensors for system optimization. Opt. Eng. 2015, 54, 097109. [CrossRef]
7. Yuksel, K.; Kinet, D.; Chah, K.; Caucheteur, C. Implementation of a Mobile Platform Based on Fiber Bragg Grating Sensors for Automotive Traffic Monitoring. Sensors 2020, 20, 1567. [CrossRef] [PubMed]
8. Campanella, C.E.; Cuccovillo, A.; Campanella, C.; Yurt, A.; Passaro, V. Fibre Bragg grating based strain sensors: Review of technology and applications. Sensors 2018, 18, 3115. [CrossRef]
9. Díaz, C.A.R.; Marques, C.A.F.; Domingues, M.F.F.; Ribeiro, M.R.N.; Frizera-Neto, A.; Pontes, P.S.; Antunes, P.F.C. A cost-effective edge-filter based FBG interrogator using catastrophic fuse effect micro-cavity interferometers. Measurement 2018, 124, 486–493. [CrossRef]
10. Díaz, C.A.R.; Leal-Junior, A.G.; Avellar, L.M.; Antunes, P.F.C.; Pontes, M.J.; Marques, C.A.; Frizera, A.; Ribeiro, M.R.N. Perrogator: A Portable Energy-Efficient Interrogator for Dynamic Monitoring of Wavelength-Based Sensors in Wearable Applications. Sensors 2019, 19, 2962. [CrossRef] [PubMed]
11. Neto, P.X.; Carneiro, A.C.; López-Barbero, A.P.; Silva, V.N.H.; Ribeiro, R.M.; dos Santos, A.B. A Mathematical Model for the Interrogation of LPG Fiber Optical Sensors Based on Electrical Harmonic Analysis. IEEE Sens. J. 2020, 20, 4237–4244. [CrossRef]
12. Chen, H.; Liang, Y. Analysis of the tunable asymmetric fiber FP cavity for fiber strain sensor edge-filter demodulation. Photonic Sens. 2014, 4, 338–343. [CrossRef]
13. Bandyopadhyay, S.; Biswas, P.; Pal, A.; Bhadra, S.K.; Dasgupta, K. Empirical relations for design of linear edge filters using apodized linearly chirped fiber Bragg grating. J. Lightwave Technol. 2008, 26, 3853–3859. [CrossRef]
14. Chuang, K.C.; Ma, C.C.; Wang, C.H. Performance analysis of a fiber Bragg grating filter-based strain/temperature sensing system based on a modified Gaussian function approximation method. Appl. Opt. 2011, 50, 5243–5255. [CrossRef] [PubMed]
15. Wade, S.A.; Attard, D.P.; Stoddart, P.R. Analysis of transmission mode of a matched fiber Bragg grating interrogation scheme. Appl. Opt. 2010, 49, 4498–4505. [CrossRef] [PubMed]
16. Cui, J.; Hu, Y.; Feng, K.; Li, J.; Tan, J. FBG Interrogation Method with High Resolution and Response Speed Based on a Reflective-Matched FBG Scheme. Sensors 2015, 15, 16516–16535. [CrossRef]
17. Wang, Z.F.; Sui, Q.M.; Wang, J.; Chang, J.; Peng, G.D.; Song, H.Y. Experimental and technical research on fiber Bragg grating vibration measuring based on two matching gratings

demodulation. In Proceedings of the Third Asia Pacific Optical Sensors Conference, Sydney, Australia, 31 January–3 February 2012.

18. Zhan, Y.; Yu, M.; Pei, J.; Yang, X.; Xiang, S. A linearity interrogation technique with enlarged dynamic range for fiber Bragg grating sensing. Opt. Commun. 2010, 283, 3428–3433. [CrossRef]

19. Jiang, B.; Zhao, J.; Qin, C.; Huang, Z.; Fan, F. An optimized strain demodulation method based on dynamic double matched fiber Bragg grating filtering. Opt. Lasers Eng. 2011, 49, 415–418. [CrossRef]

20. Zhang, H.; Jiang, J.; Liu, S.; Chen, H.; Zheng, X.; Qiu, Y. Overlap Spectrum Fiber Bragg Grating Sensor Based on Light Power Demodulation. Sensors 2018, 18, 1597. [CrossRef]

21. Wu, Q.; Farrell, G.; Semenova, Y. Simple design technique for a triangular FBG filter based on a linearly chirped grating. Opt. Commun. 2010, 283, 985–992. [CrossRef]

22. Lin, B.; Tjin, S.C.; Ngo, N.Q.; Song, Y.; Liang, S.; Xia, L.; Jiang, M. Analysis of inverse-Gaussian apodized fiber Bragg grating. Appl. Opt. 2010, 49, 4715–4722. [CrossRef]

23. Lin, B.; Zhang, H.; Tjin, S.C.; Tang, D.; Hao, J.; Tay, C.M.; Liang, S. Inverse-Gaussian apodized fiber Bragg grating for dual-wavelength lasing. Appl. Opt. 2010, 49, 1373–1377. [CrossRef] [PubMed]

24. Erdogan, T. Fiber grating spectra. J. Lightwave Technol. 1997, 15, 1277–1294. [CrossRef]

25. Liu, Q.; Li, Q.; Sun, Y.; Chai, Q.; Zhang, B.; Liu, C.; Sun, T.; Liu, W.; Sun, J.; Ren, Z.; et al. Transfer matrix method for simulation of the fiber Bragg grating in polarization maintaining fiber. Opt. Commun. 2019, 452, 185–188. [CrossRef]

26. Ali, T.A.; Shehata, M.I.; Mohamed, N.A. Design and performance investigation of a highly accurate apodized fiber Bragg grating-based strain sensor in single and quasi-distributed systems. Appl. Opt. 2015, 54, 5243–5251. [CrossRef]

АНАЛИЗ МЕТОДОВ ОБРАБОТКИ СИГНАЛОВ ОТ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ

Вуйцик[1,2] В., Кисала[1,2] П., Калижанова[1,3] А.У., Козбакова[1,4] А.Х., Кунелбаев[1] М., Едилхан[1,5] Д., Айткулов[1,6] Ж.С, Искакова[1] М.Т.
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан
[2]Люблинский технический университет, Польша
[3]Алматинский университет энергетики и связи, Казахстан
[4]Алматинский технологический университет, Казахстан
[5]Астана IT университет, Казахстан
[6]Академия логистики и транспорта, Казахстан
e-mail: waldemar.wojcik@pollub.pl, kalizhanova_aliya@mail.ru

Аннотация. *В данной работе представлены результаты моделирования однородных волоконно-оптических решеток Брэгга с использованием метода матрицы перехода и был определен уровень погрешности. На основании полученных результатов была проверена правильность моделирования структуры по указанному методу, что дало удовлетворительные результаты.*

В работе не только проверялось, соответствуют ли и в какой степени характеристики пропускания волоконно-оптических решеток Брэгга, полученные при моделировании, аналогичным характеристикам, полученным в лаборатории, но также была определена зависимость этого соответствия от физических параметров структур. Измерения и моделирование проводились для «эталонной решетки» с заданными параметрами, а затем изменялись фиксированными значениями свойств, таких как длина, период и модуляции коэффициента глубины. Сравниваются основные свойства, которые влияют на параметры оптических датчиков (которые могут измерять различные физические величины), построенных на основе решеток Брэгга, поскольку упомянутые свойства характеристик передачи оказывают непосредственное влияние на параметры датчика, такие как чувствительность, разрешение и диапазон измерений, а также требования к используемым компонентам.

Ключевые слова: *волоконная решетка Брэгга, численное моделирование, спектральная характеристика, датчик.*

Введение

Современные волоконно-оптические датчики позволяют измерять многие физические параметры: давление, температуру, расстояние, положение в пространстве, скорость вращения, скорость линейного перемещения, ускорение, колебания, массу, звуковые волны, уровень жидкости, деформацию, коэффициент преломления, напряженность электрического и магнитного поля, силу электрического тока, концентрацию газа, дозу радиационного излучения и т. д. С точки зрения безопасности строительных конструкций и сооружений наиболее востребованы такие параметры как изгибы и напряжения.

Благодаря использованию оптических волокон в качестве чувствительных элементов отсутствует влияние на результат измерения электромагнитных полей,

побочного электромагнитного излучения, перекрестных помех каналов, отсутствуют проблемы, связанные с контурами заземления и с напряжениями смещения в местах соединения разнородных проводников, существенно повышается электрическая безопасность, отсутствуют проблемы дугообразования и искрения. Такие датчики имеют высокую стойкость к вредным воздействиям среды; малые габариты и вес; высокую механическую прочность; стойкость к повышенным температурам, вибрациям и др.; высокую скорость передачи данных. Кроме того, волоконно-оптические датчики могут использоваться во взрывоопасной среде ввиду их абсолютной взрывобезопасности. Они химически инертны, имеют простую конструкцию и высокую надежность.

Среди волоконно-оптических датчиков особое место занимают датчики на основе волоконных решеток Брэгга (ВРБ). Такие решетки записаны в оптическом волокне при помощи ультрафиолетового лазера и представляют собой участок световода с периодическим изменением показателя преломления вдоль оси. Одним из перспективных направлений развития технологии оптических датчиков являются волоконные брэгговские решетки.

Используемый метод также зависит от метода, применяемого для исследования. Компьютерное моделирование используется в основном там, где процесс не может быть воспроизведен аналитическими методами или он невыгоден во времени из-за его сложности. Такая ситуация имеет место в процессе прохождения света через оптическое волокно, изучаемое в данной работе, с периодически модулированным показателем преломления в его сердцевине.

Для того, чтобы моделирование использовалось для анализа происходящих явлений, необходимо знать их уровень точности. Результат, полученный в результате моделирования, никогда не будет таким точным, как результат, полученный в лаборатории, который зависит от используемой модели, которая всегда является упрощенным объектом, принимая некоторые допущения, некоторые из которых могут быть неправильно определены из-за неполного знания о предмете процесса. Не менее важной причиной такого положения вещей являются обобщения, введенные используемыми методами моделирования. В зависимости от типа выполняемых вычислений и диапазона используемых в них переменных источником неточности также может быть арифметика, используемая в компьютерной программе, и в случае моделирования непрерывных сигналов - их выборка и количественная оценка. В данной работе уровень точности волоконно-оптического моделирования решеток Брэгга оценивался без анализа причин неточности.

Методология работы

Метод матрицы перехода рассматривает решетку Брэгга как сеть с четырьмя терминалами. Это означает, что на обоих концах структуры предполагается наличие входных и выходных волн, которые записаны в векторной форме, как показано на рис. 1. Модель вводится в односторонний вектор и нулевой вектор справа, которые в методе матрицы перехода являются граничными условиями, позволяющими записать систему уравнений, необходимую для математической постановки решаемой задачи.

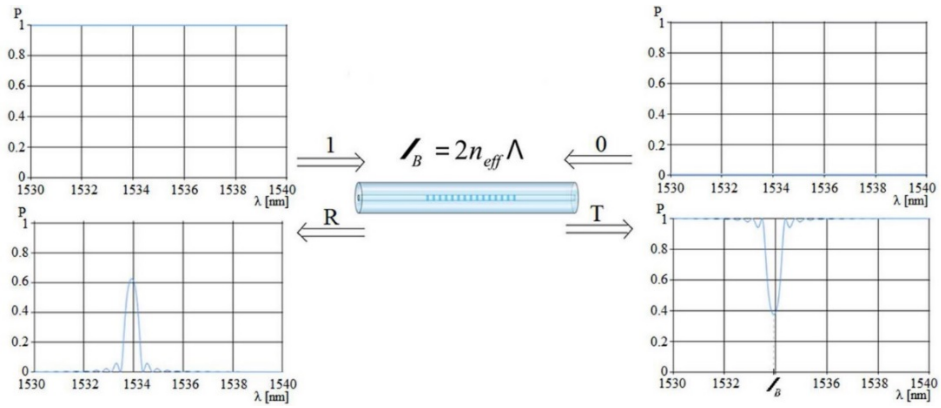


Рис. 1 Диаграмма, показывающая однородную решетку Брэгга в виде четырехполюсной сети

Метод матрицы переходов вводит логическое разделение решетки на равные участки, для которых вычисления выполняются отдельно, а выходные векторы одного из участков одновременно являются входными векторами последующих участков [1]. В результате вычисления выполняются на полных матрицах, однако для целей данной работы математические детали этих действий опущены. Однако следует подчеркнуть, что уровень неточности этого метода зависит от количества разделов, на которые была разделена структура модели.

Эта зависимость намного больше при моделировании аподизированных или чирпированных решеток (это структуры, в которых их длина изменяется соответственно: коэффициент модуляции показателя преломления в сердечнике или его период). Это связано с тем, что в сечении период решетки и глубина модуляции эффективного показателя преломления в структуре должны быть постоянными, поэтому увеличение количества сечений приводит к лучшему представлению профилей аподизации и чирпирования.

Моделирование проводилось в разработанном для этой цели приложении, написанном на языке программирования C#, с графическим интерфейсом на основе технологии Windows Forms. В программе используются десятичные типы данных, благодаря которым в расчетах, выполненных приложением, была получена точность 28 десятичных знаков [2]. Было проверено, что значения в переменных, хранящихся во время работы алгоритма, имели до 12 или даже 16 цифр, значимых для результатов вычислений, из-за особенностей выбранного метода моделирования. Эти значения лежат в пределе диапазона точности двоичных переменных в C #, который составляет от 15 до 16 десятичных знаков [2]. Было подтверждено, что изменение арифметики с десятичного на двоичное вызывает небольшие различия в спектре пропускания решетки Брэгга, полученной в результате моделирования. В связи с вышеуказанными фактами был сделан вывод о том, что ошибки, возникающие в результате округлений, связанных с цифровым представлением, используемым при расчете переменных, пренебрежимо малы и не влияют на результаты сравнения спектров, полученных в результате моделирования, со спектрами, полученными в лаборатории.

Спектры пропускания решеток, полученные в результате моделирования, сравнивались с лабораторными спектрами пропускания решеток, полученных с использованием метода фазовой маски. На рисунке 2 показаны спектральные характеристики, измеренные в моде передачи для различных значений длины структур, их периода и глубины модуляции показателя преломления. Набор измеренных характеристик пропускания решеток Брэгга 530 нм и различной длины

соответственно: синий - структура длиной 2 мм; красный - структура длиной 4 мм; зеленый - структура длиной 6 мм; фиолетовый - структура длиной 8 мм.

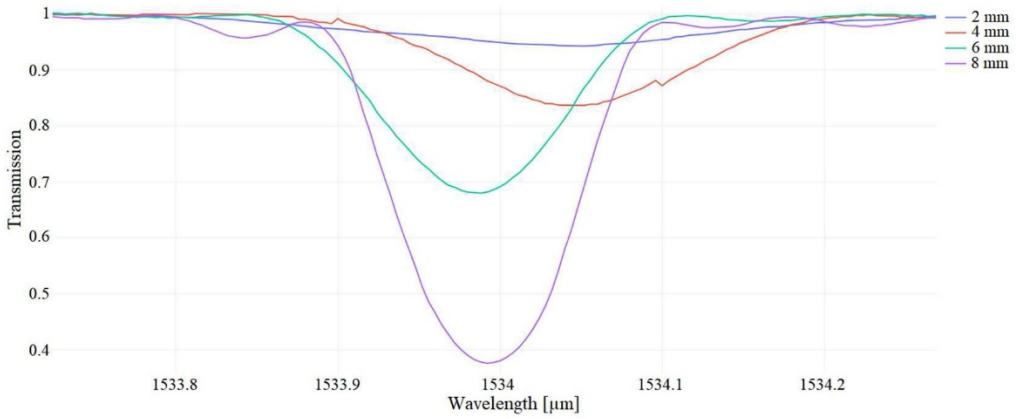


Рис. 2 Набор измеренных характеристик пропускания решеток Брэгга 530 нм и различной длины соответственно

Структуры, испытанные в лаборатории, были изготовлены с использованием когерентного эксимерного лазера «Bragg Star M» (длина волны 248 нм). Характеристики пропускания определяли путем пропускания широкого спектра света, генерируемого диодами SLED, через решетки и регистрации энергии на выходе структуры с помощью анализатора спектра.

Критерии для сравнения характеристик, полученных при моделировании, и результатов, достигнутых в лаборатории, основаны на сходимости их свойств, которые имеют решающее значение при применении решеток в волоконно-оптических датчиках. Этими свойствами являются: длина волны Брэгга, то есть длина волны, которая передается в наименьшей степени решеткой Брэгга, определяющая положение характерного пика в характеристике передачи; динамика пика, определяющая уровень отражения длины волны, аналогичной длине Брэгга, выраженной отношением энергии волны на выходе оптического волокна к энергии на его входе на длине волны, при которой это подавление является наибольшим (Брэгговская волна); полная ширина на половине максимума (FWHM-Full Width at Half Maximum) пика, описывающая диапазон длин волн, который представляет собой разность длин волн, для которой отношение их энергии, передаваемой к их входной энергии, составляет половину максимального значения, уменьшенного на количество шума (в смысле прерывания монотонности части характеристики, содержащей огибающую пика (соответствующей отражению волн тестируемой структурой), измеренной отдельно для длины волны, более короткой, и отдельно для длины волны, большей длины волны Брэгга (рис. 3). Диаграмма, показывающая последовательность шагов, приводящих к вычислению FWHM пика: определение минимального значения передачи (1) и определение длины волны Брэгга (отмечено на абсциссе красным цветом); определение величины передачи, для которой первое изменение монотонности происходит вблизи длины волны Брэгга (2). Вычисление разности между полученными коэффициентами передачи (3) и определение среднего значения (4); Определение длины волны, для которой функция принимает расчетное значение (5). Шаги 2–5 следует выполнять отдельно для двух частей

характеристики; Удаление определенных длин волн друг от друга приведет к FWHM пика (6).

Динамика боковой полосы определяет отношение энергии, передаваемой на вход (чем больше динамика, тем меньше это отношение) для волны с длиной, отличной от брэгговской, но близкой к ней, для которой наблюдается локальное максимальное отражение волны, видимое в характеристике передачи в виде бокового пика (намного ниже, чем основной пик, называемый боковой полосой), где этот коэффициент относится к боковому пику с более высокой динамикой. Схема определения этого коэффициента приведена на рис. 4 [3].

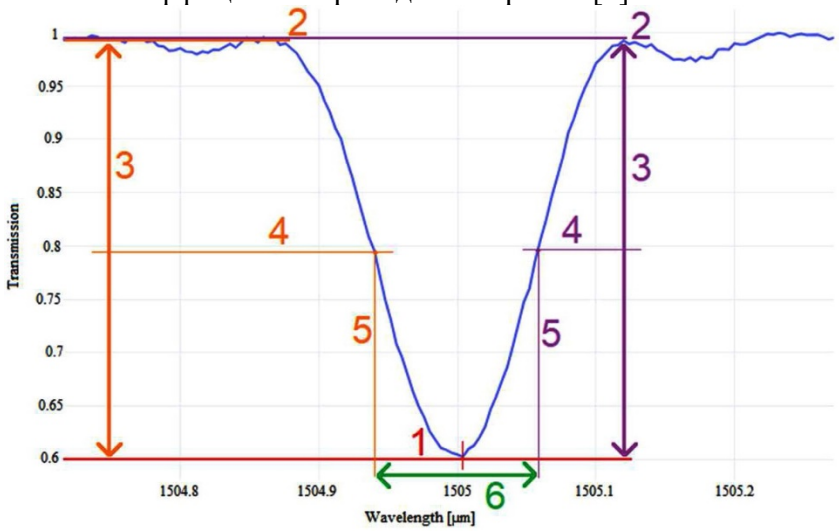


Рис. 3 Диаграмма, показывающая последовательность шагов, приводящих к вычислению FWHM пика

Сравнение характеристик было сделано путем сравнения каждого из свойств, перечисленных выше. Это действие не дает полной картины различий между сравниваемыми объектами, но имеет несколько неоспоримых преимуществ. Во-первых, позволяет сравнивать параметры, значения которых создают переходные характеристики (определяющие зависимость свойств характеристик пропускания от физических свойств структур) решеток Брэгга и таким образом, позволяет определять уровень точности таких характеристик, созданных на основе численных расчетов.

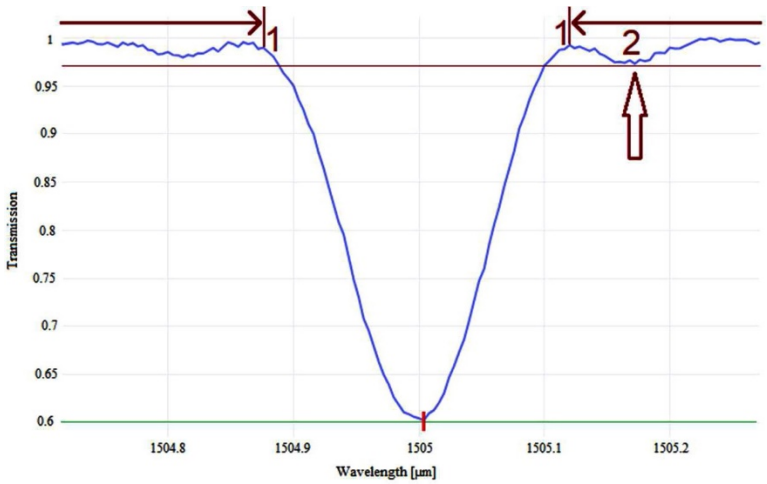


Рис. 4. Диаграмма, показывающая способ определения коэффициента передачи

боковой моды первого порядка («боковая полоса»)

После определения длины волны Брэгга (отмечено красным) необходимо найти точки, в которых изменяется монотонность спектральных характеристических диапазонов (1). Далее следует определить интервал в окне пропускания, не содержащий заданных монотонных интервалов, составляющих пик основной моды - этот интервал отмечен в верхней части диаграммы. Минимальное значение коэффициента передачи в этом диапазоне (2) является искомым значением.

Во-вторых, как уже указывалось, сравниваются основные свойства, которые влияют на параметры оптических датчиков (которые могут измерять различные физические величины), построенных на основе решеток Брэгга, поскольку упомянутые свойства характеристик передачи оказывают непосредственное влияние на параметры датчика, такие как чувствительность, разрешение и диапазон измерений, а также требования к используемым компонентам [4]. Другим преимуществом принятой методологии сравнения характеристик является возможность независимо исследовать взаимосвязь между описанными свойствами, что было бы невозможно при использовании методов, основанных на сравнении корреляции характеристик передачи в виде наборов точек. В используемой методологии сравниваемые векторы данных рассматривались как объекты с определенными характеристиками, что позволило выделить детали на ожидаемом уровне.

Полученные неточности численных расчетов и их зависимости

Длина волны Брэгга строго зависит от параметров структуры и, в соответствии с формулой Брэгга, прямо пропорциональна периоду решетки и показателю преломления в сердцевине волокна [5]. Казалось бы, что длина волны Брэгга является поэтому самым простым значением для вычисления. Однако из компиляции (таблица 1) следует, что рассчитанные значения отличаются от измеренных, а абсолютная погрешность (которая является разницей между измеренными и рассчитанными значениями) отличается для отдельных решеток. Стоит отметить, что полученные значения длины волны Брэгга с помощью численных расчетов были одинаковыми для двух наборов симуляций, отличающихся предполагаемым коэффициентом модуляции показателя преломления в сердечнике.

Таблица 1. Сводка длин волн Брэгга, полученных на основе лабораторных измерений и численных расчетов, вместе с ошибками расчета при измерении набора решеток с заданными параметрами.

	Решетка 1	Решетка 2	Решетка 3	Решетка 4	Решетка 5=2	Решетка 6	Решетка 7	Решетка 8	Решетка 9=3	Решетка 10	Решетка 11
Период решетки [нм]	530	530	530	530	530	530	530	520	530	540	550
Длина решетки [см]	2	2	6	8	4	4	4	6	6	6	6
Основной показатель преломления	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471

Время облучения [мин]	2	2	2	2	2	4	6	2	2	2	2
Измеренная длина волны Брэгга [нм]	1534.048	1534.052	1533.988	1533.992	1534.052	1534.160	1534.240	1505.004	1533.988	1562.100	1590.644
Расчетная длина волны Брэгга [нм]	1533.924	1533.924	1533.926	1533.926	1533.924	1533.924	1533.924	1504.982	1533.926	1562.869	1591.811
Абсолютная ошибка [нм]	0.124	0.128	0.062	0.066	0.128	0.236	0.316	0.022	0.062	0.769	1.167

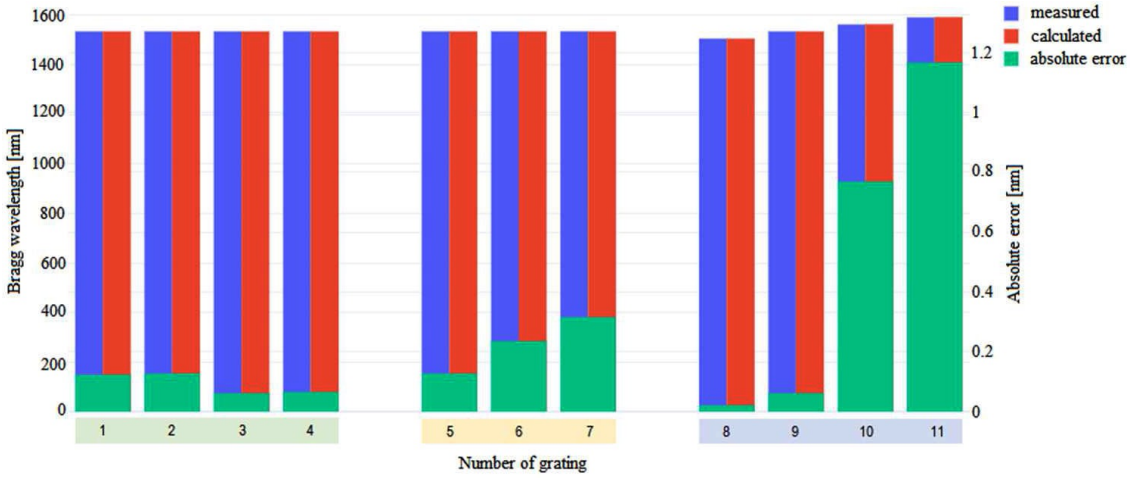


Рис. 5 Данные из таблицы 1 в графической форме

Для каждой решетки были определены измеренные и рассчитанные значения длины волны Брэгга и получена абсолютная ошибка (была использована вторая ось возвышения, масштаб которой виден с правой стороны графика).

На основании приведенного выше списка (таблица 1) можно сделать несколько интересных наблюдений. Прежде всего, следует отметить, что в подавляющем большинстве случаев измеренное значение больше расчетного. Во-вторых, если не удается определить зависимость уровня ошибки от длины решетки (решетки 1–4), то зависимость значения ошибки от времени включения решетки (структура 5–7) видна. Можно также отметить зависимость величины погрешности от периода решетки, который значительно возрастает для структур с 540 нм и 550 нм (решетки 10 и 11), что видно на рис. 5. В-третьих, это видно из того, что для двух исследованных решеток с наибольшим периодом расчетное значение длины волны Брэгга больше измеренного, что является исключением из правила, наблюдаемого в других случаях. Прежде чем объяснять эти наблюдения, необходимо рассмотреть, являются ли полученные ошибки большими или малыми (в контексте распространенных применений решеток и возможности использования моделирования по принятому методу). Следует также проверить, могут ли они быть только результатом неопределенности измерений.

Значения ошибок измерений

Раздел, посвященный методологии исследования, описывает проблему отсутствия возможности измерения глубины модуляции показателя преломления в сердцевине оптического волокна. Также было упомянуто, что в связи с вышеизложенным неточности, полученные на основе измерений и расчетов,

являются приблизительными, поскольку модель, используемая при моделировании, содержит определенные допущения. Было принято решение приблизить значения этих ошибок, и для этого необходимо было оценить реальное значение коэффициента глубины модуляции. Вышеуказанное было достигнуто путем расчета - путем моделирования - значения этого коэффициента для каждой из использованных структур, для которого рассчитанная динамика отражения будет равна динамике отражения сформированной решетки. Использовался тот факт, что глубина модуляции показателя преломления оказывает из всех изученных свойств характеристик пропускания наибольшее влияние на коэффициент пропускания для длины волны Брэгга [7], с помощью которого описывается динамика отражения. Результаты этих расчетов включены в таблицу ниже (Таблица 2).

Таблица 2. Сводка оценочных значений коэффициента глубины модуляции, содержащая граничные значения, ожидаемые значения, рассчитанные значения и различия между ожидаемыми и рассчитанными значениями для каждой из рассмотренных решеток.

	Решетка 1	Решетка 2	Решетка 3	Решетка 4	Решетка 5=2	Решетка 6	Решетка 7	Решетка 8	Решетка 9=3	Решетка 10	Решетка 11
Период решетки [нм]	530	530	530	530	530	530	530	520	530	540	550
Длина решетки [см]	2	2	6	8	4	4	4	6	6	6	6
Основной показатель преломления	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471	1.4471
Время облучения [мин]	2	2	2	2	2	4	6	2	2	2	2
Краевой коэффициент глубины модуляции показателя преломления. сильно зависит от времени облучения	0.000047	0.000047	0.000047	0.000047	0.000047	0.000094	0.000141	0.000047	0.000047	0.000047	0.000047
Ожидаемый коэффициент глубины модуляции показателя преломления. рассчитано для эталонных решеток	0.000075	0.000075	0.000075	0.000075	0.000075	0.000094	0.000113	0.000075	0.000075	0.000075	0.000075
Краевой коэффициент глубины модуляции	0.000103	0.000103	0.000103	0.000103	0.000103	0.000094	0.000085	0.000103	0.000103	0.000103	0.000103

показателя преломления. слабо зависит от времени облучения											
Расчетный (для каждой решетки отдельно) коэффициент глубины модуляции показателя преломления	0.000084	0.000075	0.000076	0.000099	0.000075	0.000094	0.000113	0.000087	0.000076	0.000067	0.000088
Отличие расчетного значения от ожидаемого для эталонных решеток	0.000009	0.000000	0.000001	0.000024	0.000000	0.000000	0.000000	0.000012	0.000001	0.000008	0.000013

На основании приведенных выше испытаний можно сделать вывод, что коэффициент глубины модуляции не прямо пропорционален времени производства решетки. Это может быть связано с явлением насыщения, возникающим при производстве брэгговских решеток [8], и с методом, используемым для производства, методом фазовой маски, соответствующий технический процесс которого может привести к небольшому изменению показателя преломления в сердечнике в течение вся структура, ослабляющая модуляцию [9]. Независимо от причины такого положения дел, из вышеупомянутых исследований можно сделать два вывода.

Значение абсолютной погрешности расчетов динамики отражения составило в среднем 0,042, а ее максимальное значение составило 0,163. Среднее значение относительной погрешности расчета составило 14,3%, а максимальное значение составило 35,3%. Среднее значение абсолютной ошибки при расчете диапазона полосы отражения составляло 0,036 нм (относительная ошибка 16,2%), а его максимальное значение составляло 0,135 нм (относительная ошибка 36,5%). Среднее значение и абсолютная ошибка расчетов динамики боковой полосы составили 0,0062 (максимальное значение было 0,0138). Однако среднее значение относительной погрешности этих расчетов составило 34,3% (максимальное значение было 75,6%).

Приведенные выше данные подтверждают сходимость характеристик передачи брэгговских решеток, полученных в результате моделирования этих структур, с характеристиками передачи сгенерированных решеток (относительная погрешность между основными характеристиками этих характеристик в среднем значительно ниже 50%). Тем не менее, необходимо учитывать, что численные расчеты, выполненные с использованием упрощенной модели, обременены ошибкой, приблизительные значения которой были приведены выше. Разумеется, эти значения определяются для принятого набора решеток. Для другого набора структур средние значения ошибок могут отличаться от указанных выше.

Заключение

Наиболее важный вывод, сделанный из проведенного исследования, заключается в том, что характеристики пропускания однородных решеток Брэгга, полученные путем моделирования, аналогичны характеристикам пропускания решеток с такими же параметрами, полученными в результате измерений, и в большинство случаев, по крайней мере, частично - совпадают с ними. Это означает, что использованный в численных расчетах метод матрицы перехода позволяет хорошо представить характеристики решеток Брэгга. Тем не менее, этот метод содержит некоторые ошибки, которые подтверждают возможность использования этого сопоставления для конкретных приложений. Исследования, описанные в данной работе, позволили определить приблизительные значения ошибок расчета, а также их зависимость от физических параметров решетки. В качестве сравнительного критерия были приняты четыре значения, описывающие характеристики передачи: длина волны Брэгга, динамика отражения, полная ширина на половине максимума (FWHM) и динамика боковой полосы.

Таким образом, результаты исследования показали, что метод матрицы перехода подходит для моделирования волоконно-оптических решеток Брэгга. Было показано, что характеристики пропускания, полученные с помощью численных расчетов с использованием этого метода, близки к характеристикам реальных решеток с параметрами, соответствующими моделируемым структурам. Выявлены зависимости между размером параметров решетки Брэгга и эффективностью расчетов. Исходя из этого, можно сделать вывод, что моделирование этих структур может использоваться не только для прогнозирования их характеристик пропускания до их создания, но и в качестве инструмента, позволяющего определять неизвестные параметры решеток Брэгга на основе их характеристик.

Экспериментальные исследования проводились в лабораториях Оптоэлектроники факультета электротехники и компьютерных наук Люблинского технического университета в рамках проекта ГФ №AP09259547 «Разработка системы из распределенных волоконно-оптических датчиков на основе волоконных решеток Брэгга для контроля состояния строительных конструкций» ИИВТ КН МОН РК.

Литература

1. Yamada M., Sakuda K.(1987).Analysis of almost periodic distributed feedback slab waveguide via a fundamental matrix approach. Applied Optics, 26(16), 3474–3478.

2. Saeed, J.M. (2019). A memory-efficient canonical data structure for decimal floating point arithmetic systems modeling and verification. Turkish Journal of Electrical Engineering & Computer Sciences, 27(1), 471–483.

3. Zhang, W., Huang, W., Li, F. (2018). High-resolution fiber Bragg grating sensor and its applications of geophysical exploration, seismic observation and marine engineering. Guangdian Gongcheng/Opto- Electronic Engineering, 45(9).

4. Jacques, A., Antonello, C., Andrea, C. (2011). Fiber Bragg Grating Sensors: Recent Advancements, Industrial Applications and Market Exploitation. Bentham Science Publishers, 10–14.

5. Othonos,A.,Kalli,K.(1999).FibreBragggratings:fundamentalsandapplicationsinteleco mmunications and sensing.

6. Chia-Ju,Y., Tzu-Hsiang, Y.,You-Cheng, L.,Bing-Hao,S., Yung Jr,H.(2018).

Apodizationtechniques for side-lobes suppression in silicon photonics waveguide gratings. Lasers and Electro-Optics (CLEO).

7. Stepniak, P., Kisała, P. (2017). Analysis of impact long period Bragg gratings parameters on their spectral transmission characteristics. Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments 2017, Proc. of SPIE, 10445.

8. Kaim, S., Mokhov, S., Divliansky, I., Zeldovich, B.Y., Glebov, L.B., Smirnov, V., Lumeau, J. (2015). Saturation of multiplexed volume Bragg grating recording. Journal of the Optical Society of America A: Optics and Image Science, and Vision, 32(1) 22–27.

9. Mahakud,R.,Prakash,O.,Kumar,J.,Nakhe,S.V.,Dixit,S.K.(2012).Analysisontheeffectof UVbeam intensity profile on the refractive index modulation in phase mask based fibre Bragg grating writing. Optics Communications, 285(24), 5351–5358.

ИССЛЕДОВАНИЕ И АНАЛИЗ ОБРАБОТКИ СИГНАЛОВ ОТ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ НА ОСНОВЕ НАКЛОННЫХ ПЕРИОДИЧЕСКИХ СТРУКТУР

Вуйцик[1,2] В., Кисала[1,2] П., Калижанова[1,3] А.У., Козбакова[1,4] А.Х., Кунелбаев[1] М., Айткулов[1,5] Ж.С., Оразбеков[1,6] Ж.
[1]*Институт информационных и вычислительных технологий КН МОН РК, Казахстан*
[2]*Люблинский технический университет, Польша*
[3]*Алматинский университет энергетики и связи, Казахстан*
[4]*Алматинский технологический университет, Казахстан*
[5]*Академия логистики и транспорта, Казахстан*
[6]*Казахский национальный педагогический университет имени Абая Алматы, Казахстан*
e-mail: waldemar.wojcik@pollub.pl, kalizhanova_aliya@mail.ru

Аннотация. *В данной работе рассматриваются волоконно-оптические датчики, предназначенные для измерения угла поворота и вращения, на основе наклонных периодических структур. Изложены основные принципы и методы измерения кручения и вращения оптическими методами. Представлены измерительная система и результаты лабораторных испытаний. В результате исследования была продемонстрирована возможность измерения степени вращения и скручивания оптического волокна с данной структурой. Получено, какие параметры сигналов от датчиков можно использовать для определения угла поворота. Показано, насколько поворот датчика вызывает изменение его коэффициента передачи для выбранной длины волны, при этом показано, какая часть характеристик обработки позволяет получить максимальную чувствительность.*

Ключевые слова: *система опроса, датчик, измерительная система, наклонная периодическая структура.*

Введение

Принцип измерения кручения и вращения оптическими методами. Оптическое измерение физических величин в механических системах и конструкциях приобретает коммерческое значение в различных отраслях промышленности. Кручение и вращение - очень часто измеряемые механические величины. Существует большой спрос на датчики для измерения этого типа величин, например, в буровых шахтах или различных типах лифтовых, вентиляционных, шахтных и строительных шахт, а также различных строительных конструкциях. В последние годы датчики поворота и вращения стали интенсивно развивающейся темой исследования новых решений волоконно-оптических датчиков [1,2]. Первые работы в области волоконно-оптических датчиков вращения появились в конце 1980-х годов. Эта работа основывалась на знаниях из появлявшейся тогда технологии оптоволоконных датчиков и объединила их с результатами исследований в других областях, таких как механика. Предметом первых работ на эту тему были как оптические датчики с внешней обработкой (рис. 1а), так и

внутренние (рис. 1б). Это разделение в основном относится к месту обработки измеряемой величины.

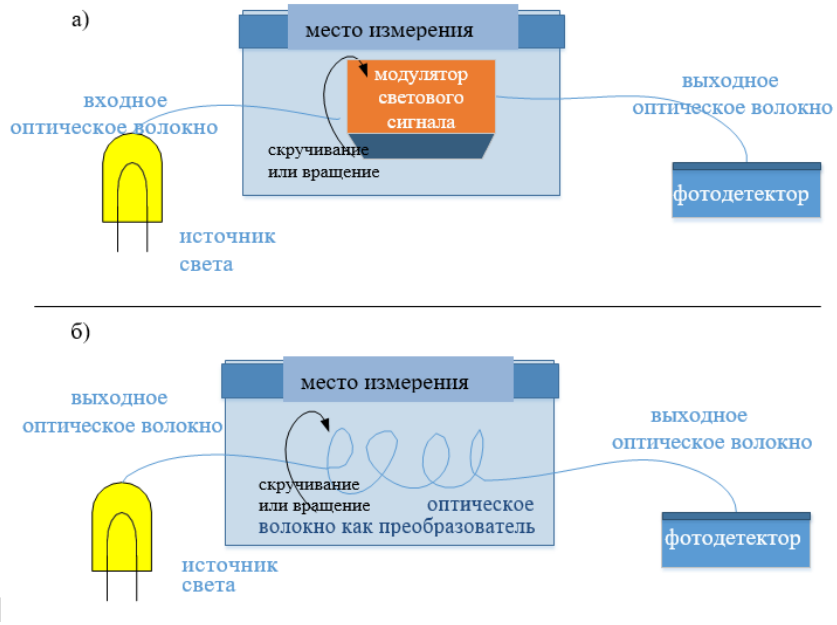


Рис. 1 Пример волоконно-оптических датчиков: а) с внешней обработкой, б) с внутренней обработкой [3]

Примером работ, использующих внешний подход, являются, например, системы, использующие двулучепреломляющие пластины задержки, помещенные между двумя коллимированными оптическими волокнами [4]. Пластины с оптической задержкой используются для кодирования информации о вращательном смещении. Когда пластина задержки вращается, оптический луч задерживается. Волна, на которой задержка составляет половину ее длины, дает минимум характеристики передачи. Длина волны, при которой наблюдается минимальная интенсивность излучения, зависит от угла поворота пластины задержки. В свою очередь, примером работ с использованием методов с внутренней обработкой является, например, использование эффекта вращения поляризации [5] или использование многомодовых оптических волокон [6]. Система преобразования угла поворота в изменение интенсивности излучения работает по принципу возбуждения выбранных мод в многомодовом волокне. Если такой многомодовый сегмент волокна скручен, моды связаны, что приводит к перераспределению мощности на разные моды (рис. 2). Таким образом, интенсивность излучения отдельных мод изменяется вместе с закруткой.

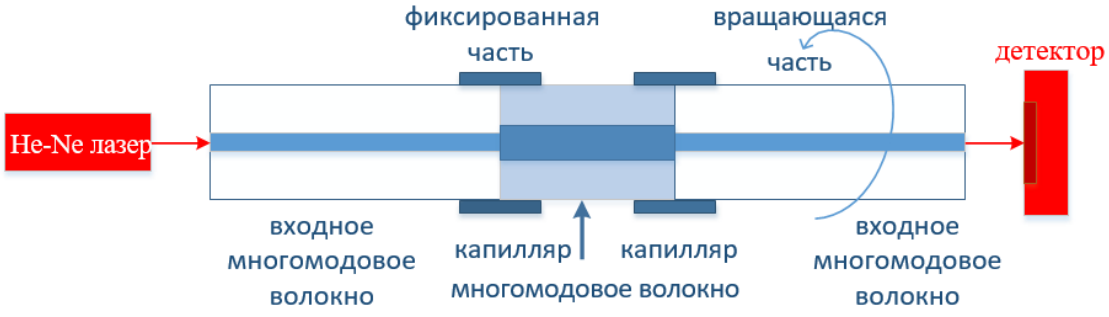


Рис. 2 Оптоволоконный датчик рулевого управления с использованием многомодовых волокон [6]

В данной работе рассматриваются выбранные оптоволоконные методы измерения угла поворота и вращения. Основная часть работы описывает идею измерения этих величин с помощью наклонных волоконных решеток Брэгга (НВРБ). Представлено понятие измерительной системы и результаты лабораторных испытаний. В этой части исследования была продемонстрирована возможность измерения степени вращения и скручивания оптического волокна со структурой НВРБ с известным углом наклона. Было указано, какие параметры сигналов от НВРБ можно использовать для определения угла поворота. Было показано, насколько поворот датчика вызывает изменение его коэффициента передачи для выбранной длины волны, при этом показано, какая часть характеристик обработки позволяет получить максимальную чувствительность. Было показано, что ту же структуру можно использовать для измерения угла поворота.

Измерения вращения и скручивания важны для мониторинга различных типов кабельных систем и механических конструкций [7, 8], и даже в текстильных изделиях [9]. В статье [3] представлен метод, использующий простые и однородные решетки Брэгга для отслеживания сил, действующих на металлические провода, которые являются элементами механических конструкций. На рис. 3 показан стальной армированный углеродным волокном стержень, состояние которого контролируется датчиками с волоконной решеткой Брэгга (ВРБ - волоконная решетка Брэгга).

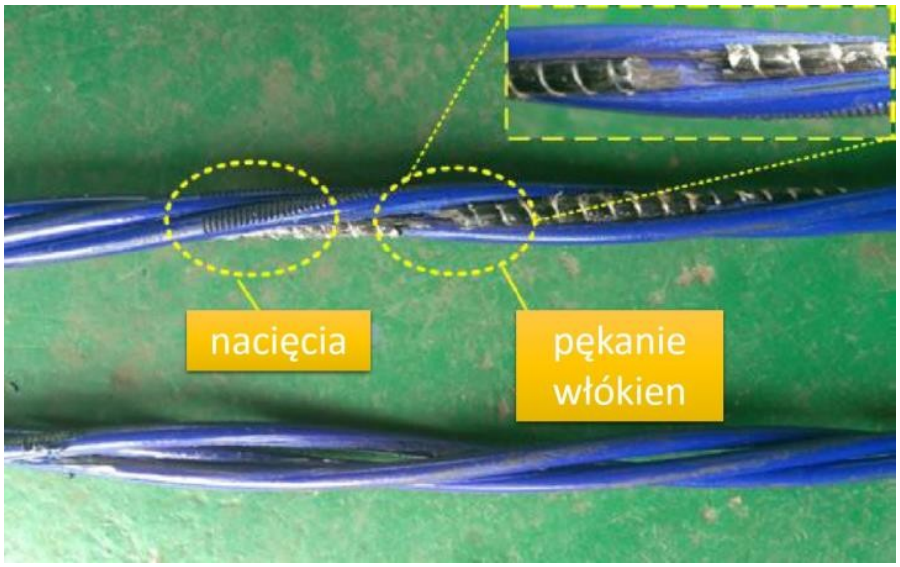


Рис. 3 Пример интеллектуального стального кабеля, контролируемого с помощью датчиков ВРБ[3]

Чувствительность систем этого типа чаще всего оценивается с помощью статических и усталостных испытаний. На рис. 3 показаны так называемые интеллектуальные стальные кабели со встроенными стержнями из углеродного

волокна и с установленными датчиками ВРБ. Система, предложенная в данной работе, была подвергнута испытаниям на растяжение с целью определения чувствительности измерительной системы. Полученные результаты показывают стабильность измерений и точность выше, чем измерения с использованием тензодатчиков.

Волоконно-оптические методы измерения крутки и витка имеют несколько важных преимуществ, таких как устойчивость к влиянию внешних условий (переменная температура или электромагнитное поле), относительно простая возможность размещения датчиков на конструкции и возможность одновременного измерения во многих местах [10]. Существует множество методов оптического измерения вращения и кручения [11]. Датчики, использующие оптические волокна, включают следующие: системы на основе петли Саньяка и оптических соединителей [12], интерферометр Саньяка и оптические волокна с эллиптической поляризацией PM (PM- polarization maintaining) [13], одномодовый волоконный ответвитель [14], длиннопериодные волоконно-оптические решетки ДПВР (LPFG: long period fiber gratings, длиннопериодные волоконно-оптические решетки) [15], решетки ВРБ с сохранением поляризации [16] и простые простые ВБР [17]. В последнее время наклонные структуры НВРБ стали очень популярными в приложениях для измерения вращения, крутки и других размеров [18, 19]. Эти решетки используют свойство влияния приложенного света СОП (SOP- state of polarization, состояния поляризации) на спектральные характеристики мод оболочки [20]. Это связано с тем, что решетка НВРБ лишает оптическое волокно цилиндрической симметрии [21] и, таким образом, позволяет обнаруживать изменения ориентации поляризации входящего света. НВРБ обладают всеми преимуществами классических технологий ВРБ, важнейшими из которых являются нечувствительность к изменениям электромагнитного поля и малые размеры. Дополнительным преимуществом структур НВРБ является большое количество мод оболочек, видимых в относительно узком спектральном диапазоне. Системы опроса, использующие классические решетки ВБР [22] или прямые лазерные сигналы [23], также могут быть использованы для обнаружения спектрального сдвига, возникающего в наклонных структурах ВРБ. Область спектральных характеристик решетки НВРБ, соответствующая модам оболочки, изменяется под влиянием многих факторов, например, показателя преломления [24], силы, вызывающей изгиб структуры [25], изменения уровня жидкости, на котором расположена решетка [26, 27, 28], а также температура и удлинение структуры [29].

Измерения кручения и вращения с использованием НВРБ, записанных на одномодовом волокне

В работе представлено использование одного оптического волокна с полученной наклонной периодической структурой для измерения угла поворота и скручивания оптического волокна. Для выполнения и анализа измерений вращения и скручивания необходимо записать периодическую структуру, в которой плоскости модуляции показателя преломления записаны под углом по отношению к нормали к оси волокна. На рисунке 4 показаны реальные размеры структуры, изготовленной таким образом.

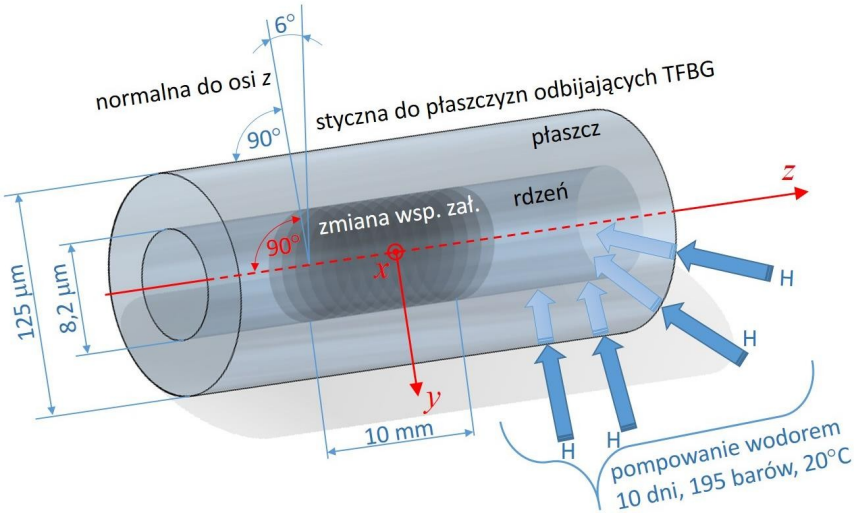


Рис. 4 Размеры и характерные параметры изготовленной структуры НВРБ, используемой в качестве датчика поворота и скручивания

Структура, показанная на рис. 4, была создана с помощью эксимерного лазера с использованием метода фазовой маски, обеспечивающего распространение света таким образом, что плоскости решетки располагались под углом θ = 6° к нормали оси волокна. Одномодовое оптическое волокно SMF-28 было предварительно подвергнуто процессу фотосенсибилизации в атмосфере водорода при давлении 195 бар и температуре 20° С в течение 10 дней. После записи решетка имела общую длину 10 мм. Полученная таким образом структура была затем подвергнута спектральным испытаниям. На рисунке 5 показан спектр пропускания полученной структуры. Как можно видеть, он имеет ряд резонансов для длин волн короче длины волны Брэгга. Как видно, наибольшая высота минимумов, исходящих от мод оболочек, наблюдается для длин волн в области 1540 нм. Этот диапазон длин волн, выделенный на рисунке 5, был выбран для измерения углов поворота и закручивания. В этой области также была получена наивысшая динамика изменения индивидуальных минимумов, обусловленных модами оболочек, с изменением поворота и закрутки структуры НВРБ.

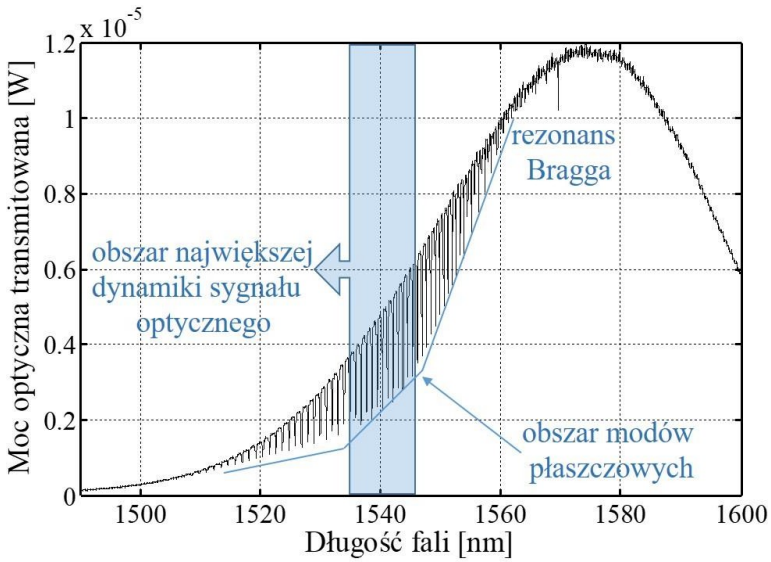


Рис. 5 Спектр пропускания полученной наклонной структуры

Характеристики показывают основной резонанс сердечника и серию резонансов для мод оболочек. Заштрихованный вертикальный прямоугольник указывает диапазон длин волн, выбранный для анализа.

Поскольку известно, что оптическое волокно НВРБ реагирует на изменения угла поляризации света, вводимого в такое волокно [11], в этой работе показаны различия в реакции спектральных характеристик такой системы на изменение угла его вращения и скручивания.

Во время измерений оптическое волокно подвергалось как вращению (рис. 6a), так и скручиванию (рис. 6b). В случае вращения оба конца волокна с записанным элементом НВРБ поворачивались на один и тот же угол, что приводило к вращению всего волокна. Длина элемента НВРБ составляла $L_{НВРБ}$ = 10 мм, а длина оптического волокна между правым вращающимся концом волокна и элементом НВРБ составляла 15 мм.

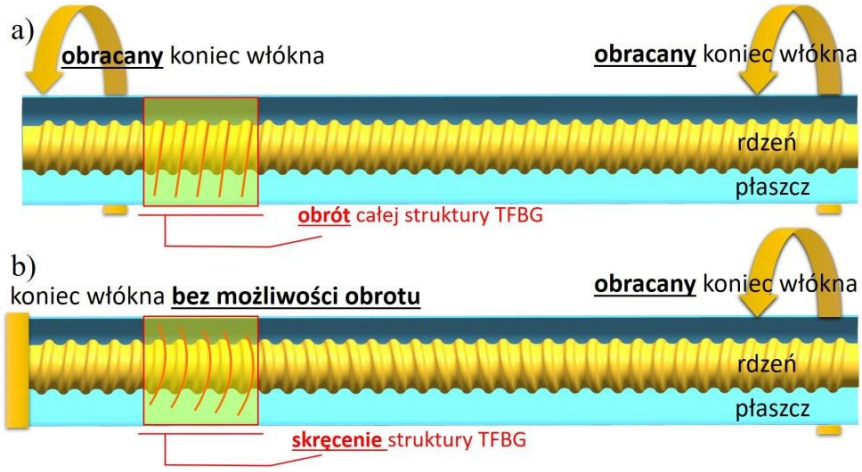


Рис. 6 Метод настройки и измерения: а) вращение, б) скрутка поворота оптического волокна, в котором записана структура НВРБ

В случае скрутки световода элемент НВРБ длиной 10 мм размещался непосредственно на жестко закрепленном конце световода. Расстояние НВРБ от вращающегося конца световода составляло 30 мм. Использовалось одномодовое

волокно SMF-28 с диаметром модового поля сердцевины 10,4 мкм (@1550нм), диаметром сердцевины 8,2 мкм, диаметром оболочки 125 мкм и диаметром внешней оболочки 242 мкм. Длина SMF-28 составляла 1 м. В обоих случаях в световод вводился линейно поляризованный свет с известной плоскостью поляризации. В исследовании использовался источник света SLD (SLD-superluminescent diode) с максимальной мощностью 2,5 мВт, центральной длиной волны 1550 нм и полосой пропускания 90 нм. Измерение проводилось при токе источника 200 мА и его температуре 20° С. Поляризация света определялась и контролировалась с помощью дополнительных оптических элементов. В первом случае (рис. 6a) оба конца волокна были повернуты с помощью прецизионного вращателя оптических волокон Thorlabs HFR007 на один и тот же угол с точностью до двух градусов. Вращение волокна вызывало изменения в распределении энергии между отдельными модами оболочек в структуре НВРБ. Изменения этой энергии наблюдали с помощью анализатора оптического спектра Yokogawa AQ6370D. Анализатор имел спектральное разрешение 0,02 нм. Оптический спектр измеряли в диапазоне от 1490 нм до 1600 нм. Во втором случае (рис. 6b) измерения были аналогичными, с той разницей, что вращался только один конец оптического волокна, что приводило к скручиванию оптического волокна и зарегистрированному в нем НВРБ.

Идея измерительной системы представлена на рисунке 7 Свет суперлюминесцентного диода через линзу (O1) направлялся на поляризатор (P) и полуволновую пластину (λ/ 2), чтобы пропускать весь падающий свет, контролируя только состояние его поляризации. Затем через линзу (O2) свет направлялся на одномодовое оптическое волокно с записанным на нем НВРБ. Связь света между волокнами и линзами осуществлялась с помощью манипуляторов x, y, z от Thorlabs Inc. Обе контрольные точки (ref. 1 и ref. 2) использовались для запуска и управления вращением и скручиванием волокна с помощью датчика НВРБ. Сигнал измеряли после прохождения через всю систему с помощью анализатора оптического спектра (OSA- Optical Spectrum Analyzer). Во всех измерениях использовалась решетка НВРБ с углом θ = 6°, измерения проводились при стабилизированной температуре окружающей среды 20° С, постоянной температуре и токе SLD 200,8 мА.

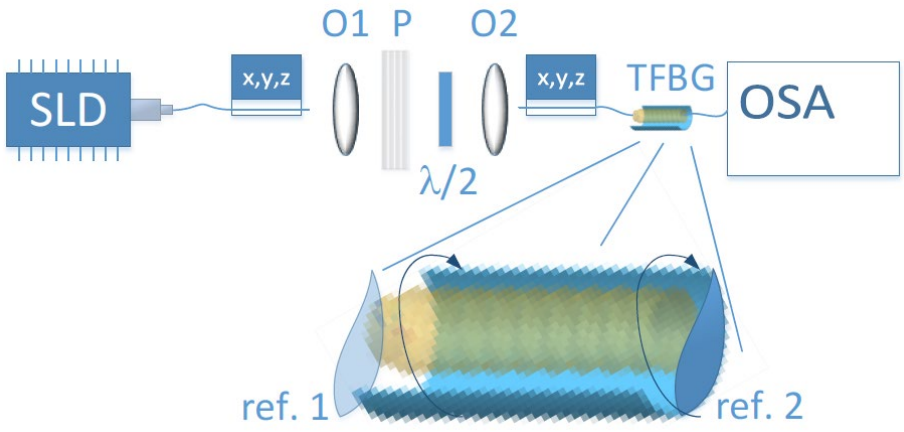


Рис. 7 Система измерения угла поворота и вращения

Для ясности остальная часть работы разделена на две части: первая посвящена измерениям вращения, а вторая - повороту.

Анализ возможности измерения вращения с использованием наклонных периодических структур.

Структура НВРБ, полученная в соответствии с процедурой, представленной на рис. 9, была подвергнута спектральным испытаниям в системе, показанной на рис.7. В результате изменения угла поворота волокна НВРБ были получены спектральные характеристики передачи - рис. 9 для различных ориентаций волокна.

В работе также представлены результаты измерений спектральных характеристик пропускания конструкций, изготовленных в лаборатории. Поэтому в данной части работы представлены результаты проверки корректности математической модели НВРБ. Для этого были изготовлены наклонные структуры со строго заданными физическими параметрами. Решетки записывались методом фазовой маски с использованием эксимерного УФ-лазера, работающего на длине волны 248 нм. На предварительно гидрированное оптическое волокно (рис. 8a) воздействовали светом УФ-лазера, который направлялся через фазовую маску (рис. 8b). Система вызывала вращение оптического волокна относительно фазовой маски, чтобы получить возможность записи периодических структур с наклонной модуляцией показателя преломления (рис. 8в).

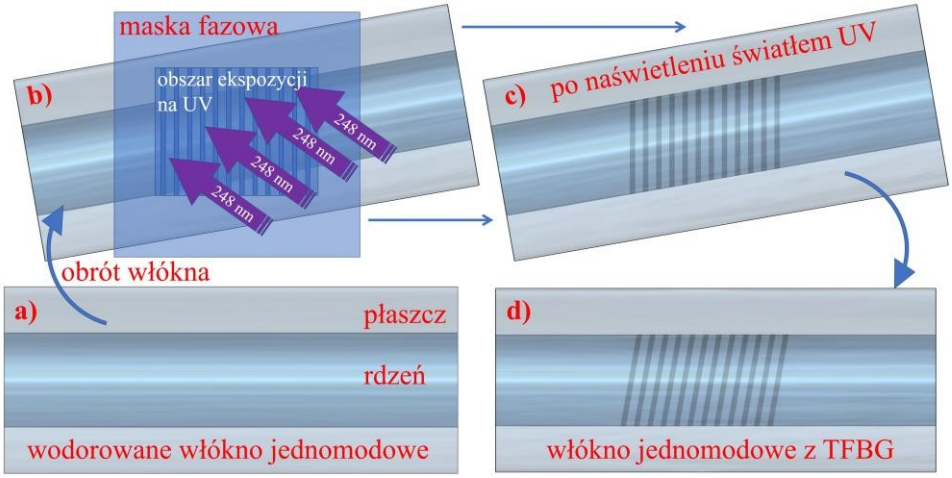


Рис. 8 Способ получения структур НВРБ на гидрогенизированных одномодовых волокнах: а), б), в), г) отдельные этапы процедуры

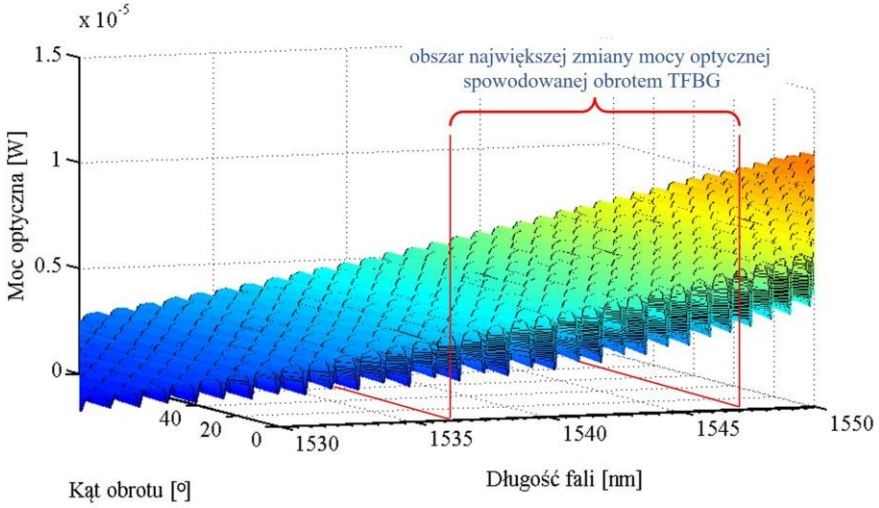


Рис. 9 Изменение оптической мощности, передаваемой после прохождения через НВРБ (6 °) для разных углов поворота

Для решетки с углом θ = 6 ° область наибольших изменений пропускания, вызванных поворотом структуры, находится между 1536 нм и 1548 нм (рис. 9). В результате предварительных измерений спектра пропускания был выбран именно этот диапазон длин волн, соответствующий модам оболочек.

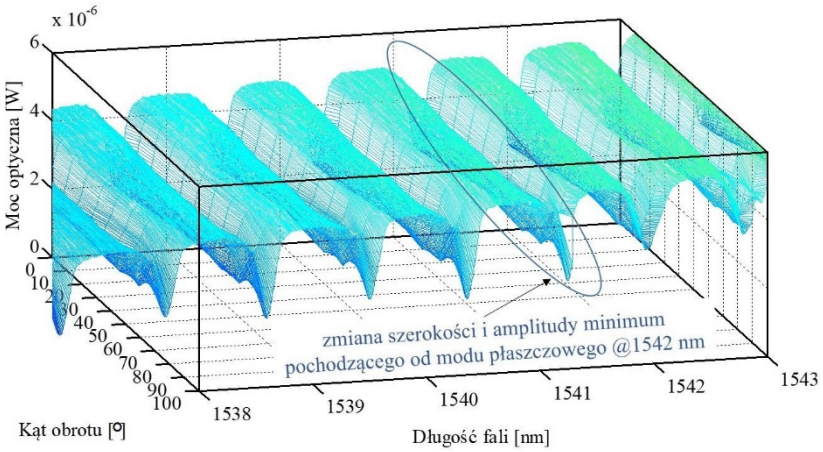


Рис. 10 Изменение характеристик передачи НВРБ для углов поворота от 0° до 100°

На рис. 10 показаны изменения оптической мощности после прохождения структуры НВРБ с выделенной областью мод оболочек, выбранной для дальнейших измерений. Предварительный анализ спектральных характеристик показал реакцию полученного НВРБ на вращение, проявляющуюся в изменении амплитуды минимумов, полученных от мод оболочек @1542 нм, а также в изменении длины

волны, соответствующей минимумам для мод оболочек в этом диапазоне длин волн. Дальнейшие исследования проводились в области 1542 нм, измеряя сдвиги минимумов спектральных характеристик и изменения амплитуды мод оболочек (рис. 11).

Явление изменения коэффициента передачи НВРБ для данной длины волны показано на рисунке 11a. На рисунке также показаны точки измерения коэффициента передачи для НВРБ (6°). На рис. 11b показано смещение спектра оболочечных мод из-за вращения структуры НВРБ. По практическим соображениям, самый простой способ измерить это смещение - это определить смещение крайних значений на характеристике передачи. На рисунке 11b также показана минимальная область измерения спектральных характеристик пропускания.

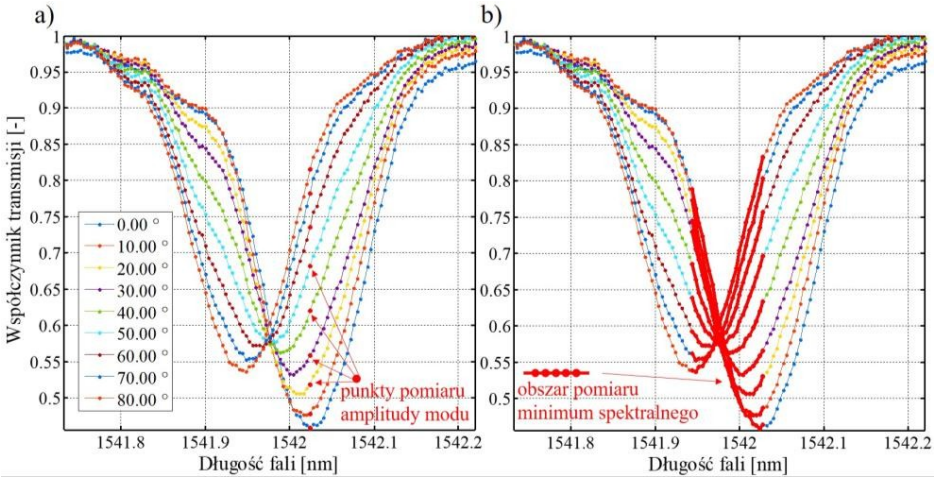


Рис. 11 Два наблюдаемых явления, возникающих в результате вращения НВРБ: а) изменение амплитуды моды для выбранной длины волны, б) смещение минимума, соответствующего конкретной моде оболочки

На рисунке 12 показаны результаты спектральных измерений волокна НВРБ, подвергнутого повороту от 0 до 80 градусов. Направление вращения соответствовало обозначению на чертеже и было названо в работе так называемым поворотом направо (P- вращение по часовой стрелке).

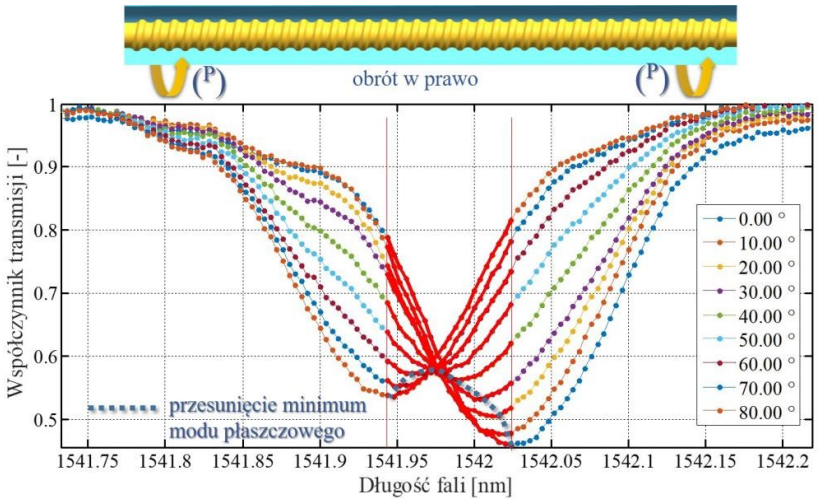


Рис. 12 Характеристики передачи изготовленной структуры НВРБ, измеренные для различных углов поворота (P)

Часть спектральных характеристик, соответствующая минимуму для более коротких длин волн (минимум, появляющийся слева), в литературе называется модой S-типа. Правый минимум чаще всего упоминается в литературе как мода P - типа. Как видно, вращение световода с НВРБ изменяет степень возбуждения левой (S) и правой (P) мод, распространяющихся в структуре. Это связано с изменением коэффициента связи мощности между отдельными модами. Этот эффект можно использовать для определения угла поворота, например, путем измерения значения мощности для данной длины волны. Для этого в исследовании была выбрана длина волны 1542,2 нм (рис. 11а), для которой наблюдается значительное изменение мощности из-за вращения волокна. Эта длина волны может использоваться для косвенных угловых измерений. Согласно рис. 11а, для исходного положения коэффициент передачи имеет значение менее 0,5. Поворот структуры на 80° увеличивает коэффициент пропускания для выбранной длины волны даже до значения 0,85. В то же время в этих диапазонах вращения волокна заметен минимальный сдвиг передаточной характеристики (рис. 11б и 12). Длина волны, соответствующая минимальному пропусканию для эталонного волокна (угол поворота 0°), составляет 1542,025 нм и смещается по мере увеличения угла поворота в сторону более коротких длин волн, достигая 1541,94 нм для угла поворота 80°. Таким образом, чувствительность НВРБ с углом 6° на оборот составляет 1пм/°. На полученных спектральных характеристиках также есть определенная область, в которой значение мощности не изменяется (или изменяется незначительно) из-за вращения. Отдельные моды обмениваются энергией, но значение мощности для длины волны, например, 1541,975 нм (рис. 12), претерпевает очень мало изменений. Любое изменение значения мощности для этих длин волн происходит из-за изменения температуры. Если температура изменится во время измерения, то весь спектр сместится, что приведет к изменению мощности для этих конкретных длин волн. В данном исследовании это явление называется температурным эффектом. Это необходимо учитывать при спектральных измерениях НВРБ в условиях варьирования угла поляризации света. Аналогичные испытания можно провести для структуры НВРБ, повернув ее в обратном направлении. На рис. 13 показаны результаты спектральных измерений НВРБ для переменных углов его поворота в противоположном направлении, чем в случае 12. Это движение названо в работе вращением против часовой стрелки и отмечено символом (L).

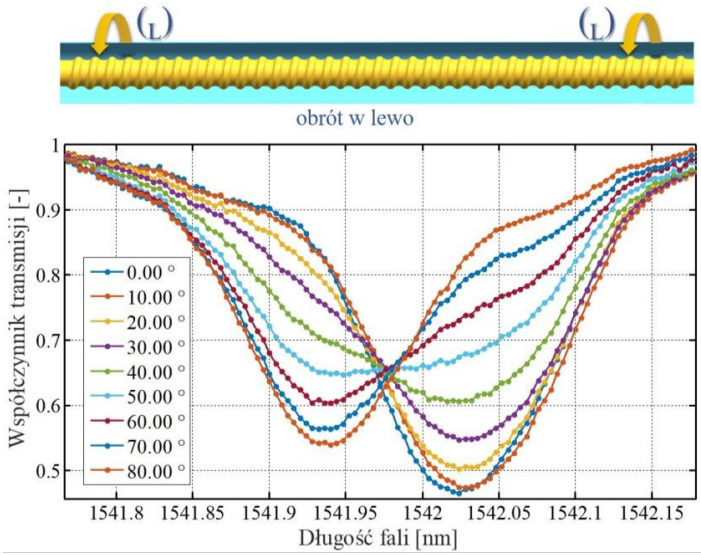


Рис. 13 Характеристики передачи изготовленной структуры НВРБ, измеренные для разных углов поворота (L)

Анализируя рисунки 13 и 14, можно увидеть, что вращение волокна в отрицательном направлении (L) в диапазоне от 0° до 80° вызывает аналогичный эффект по отношению к вращению в положительном направлении (P). Коэффициент пропускания структуры достигает максимального значения 0,82 с углом поворота 80°. При угле поворота, равном 0°, значение коэффициента пропускания для выбранной длины волны 1542,25 нм было даже ниже 0,48.

Характер изменений идентичен, и поворот (L), и (P) вызывают аналогичные изменения спектральных характеристик структуры. Измеряя значение оптической мощности для выбранной длины волны - в описанном случае это 1542,25 нм - можно определить угол поворота оптического волокна с записанной в нем структурой НВРБ.

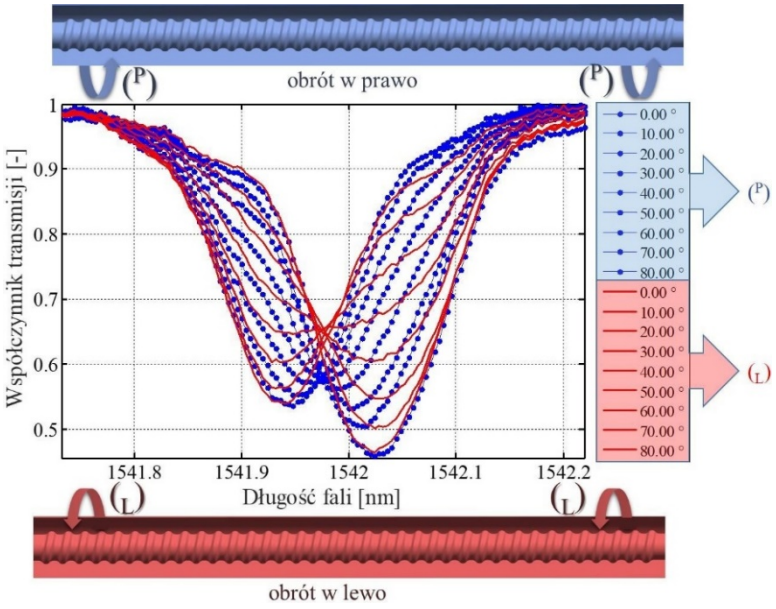


Рис 14. Список характеристик передачи НВРБ, измеренных для различных углов поворота (P) и (L)

Представленные результаты показывают возможность использования НВРБ для измерения угла поворота. Для сравнения характеристики преобразования угла поворота в изменение коэффициента передачи НВРБ представлены далее в этой статье вместе с характеристиками преобразования угла поворота структуры. Результаты спектральных исследований закрученного НВРБ представлены далее. В этом разделе работы было проанализировано влияние скрутки волокна на спектральные характеристики при различных параметрах поляризации входящего света.

Анализ возможности измерения поворота крутки с использованием наклонных периодических структур.

В работе представлены результаты спектральных измерений изготовленной структуры НВРБ, подвергнутой кручению в соответствии с рис. 6б. Спектры были исследованы при наклоне структуры в направлении (P) и (L). Заданный угол закрутки - это угол, на который структура НВРБ была закручена по своей длине. Измерения проводились также при начальном возбуждении различных мод структуры (рис. 15), соответствующих S поляризации (рис. 15a) и P (рис. 15c). Здесь также анализируется изменение спектральных характеристик при возбуждении обеих мод одновременно. Это состояние было названо непрямой поляризацией и обозначено символом: S | P (рис.15b).

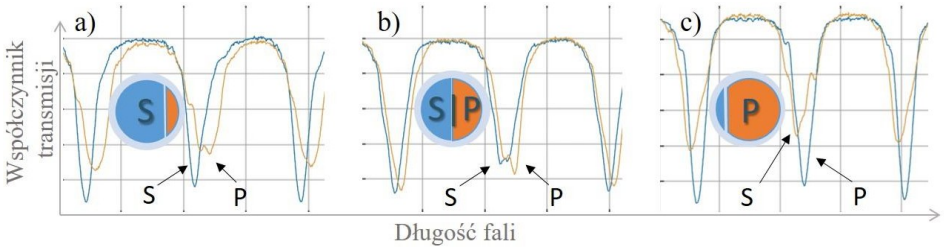


Рис.15 Три состояния возбуждения мод испытуемого НВРБ:
а) состояние типа S, б) промежуточное состояние - S | P, в) состояние типа P

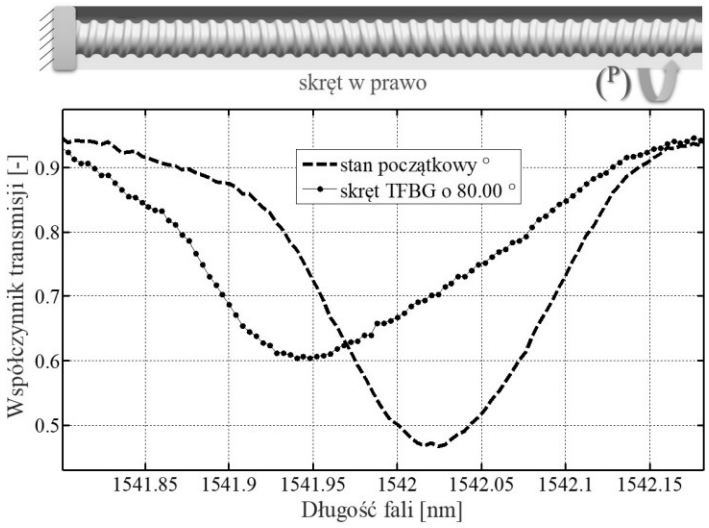


Рис. 16 Характеристики передачи тестируемого НВРБ измерены для нескрученной решетки и скрученной решетки (P) с углом 80 °. Возбуждение мод P-типа

Анализ влияния поворота НВРБ на его спектральные характеристики проводился с использованием решетки с углом θ = 6°. Структура была закручена на угол, равный 80°, и изменения ее пропускания были исследованы для известного состояния возбуждения моды. На рис. 16 показано изменение спектра пропускания для возбуждения P-типа и поворот структуры вправо на угол, равный 80 °. Анализируя результаты измерений кручения НВРБ, можно увидеть, что характеристики передачи структуры также смещаются, как это было в случае ее вращения. Обмен мощностью между модами S-типа и P-типа также является характерным. На рис. 16 показано переключение мощности из моды P-типа в моду S-типа из-за скручивания (P) структуры на угол 80 °.

На рисунках 17–19 показаны спектры пропускания для шести случаев. Во-первых, мода на более коротковолновой стороне (возбуждение S-типа) стимулировалась соответствующей настройкой поляризации входящего света, и вся структура подвергалась (P) закручиванию (рис. 17a). Затем также возбуждалась мода S-типа и одновременно вызывалось скручивание (L) структуры (рис. 17b).

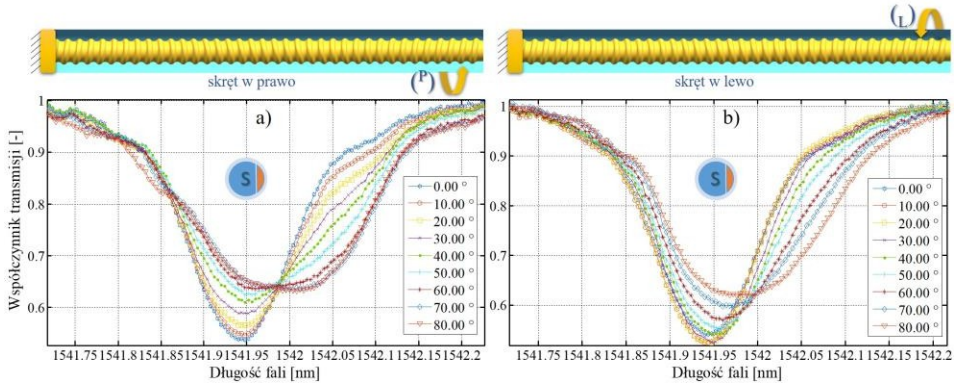


Рис.17 Характеристики передачи полученной структуры НВРБ, измеренные для различных значений угла закрутки: а) возбужденная мода поляризации S-типа, вращение в направлении (P), б) возбужденная мода поляризации S-типа, вращение в направлении (L)

В дальнейшей части экспериментов стимулировались обе моды S | P НВРБ и при этом структура закручивалась в направлении (P) (рис. 18a). Затем при возбуждении обеих мод в системе S | P был выполнен (L) поворот НВРБ (рис. 18b).

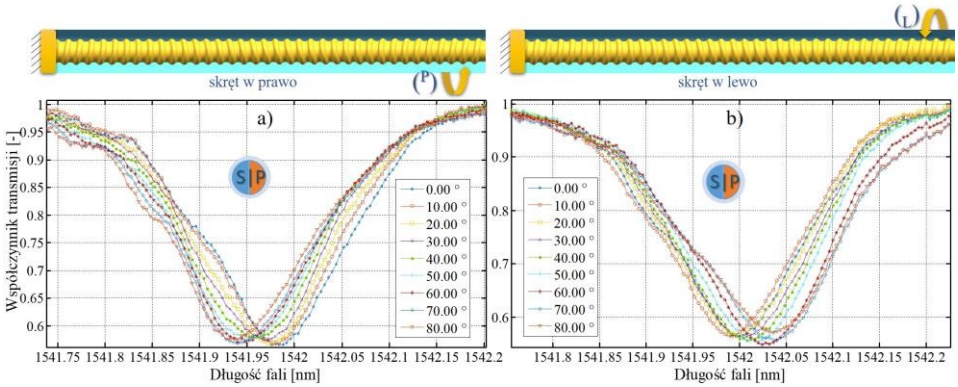


Рис.18 Характеристики пропускания полученной структуры НВРБ, измеренные для различных значений угла закрутки: а) возбуждали обе поляризационные моды S | P, вращение в направлении (P), б) возбуждали обе поляризационные моды S | P, вращение в (L) направление

Наконец, была возбуждена правая мода НВРБ, и одновременно были вызваны скручивание (P) структуры (рис. 19a) и закручивание (L) НВРБ (рис. 19b). Как и в случае вращения - в этой части измерений также выбиралась длина волны, для которой определялось значение коэффициента передачи. Из-за положения пиков, полученных от мод оболочки в случае кручения, длина волны, для которой было определено значение пропускания, составляла 1541,95 нм.

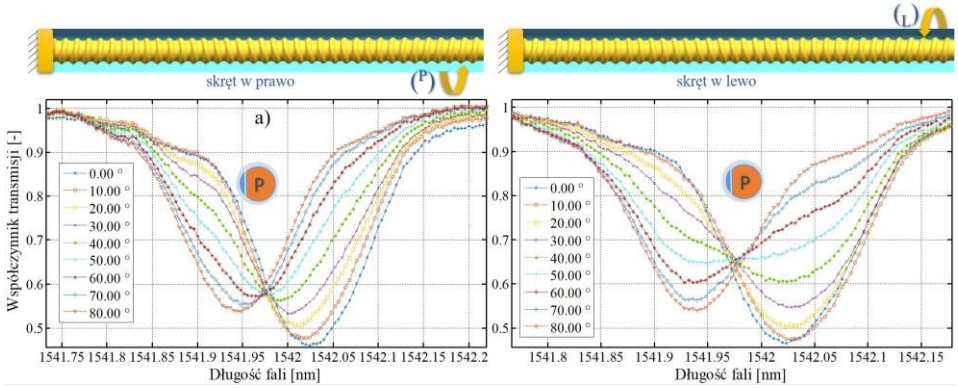


Рис.19 Характеристики передачи полученной структуры НВРБ, измеренные для различных значений угла закрутки: а) возбужденная мода правой поляризации, вращение в направлении (P), б) возбужденная мода правой поляризации, вращение в направлении (L)

Результаты испытаний на вращение и кручение с использованием датчиков с наклонными решетками Брэгга.

В этой части исследования представлены характеристики обработки периодической структуры, созданной и описанной ранее. На рисунке 20 показаны результаты измерений коэффициента пропускания структуры НВРБ под углом 6° для выбранной длины волны (1542,025 нм). На одном графике представлены результаты измерения вращения (P) и (L). Передача достигает минимального значения для невращающейся структуры (поворот равен 0 °).

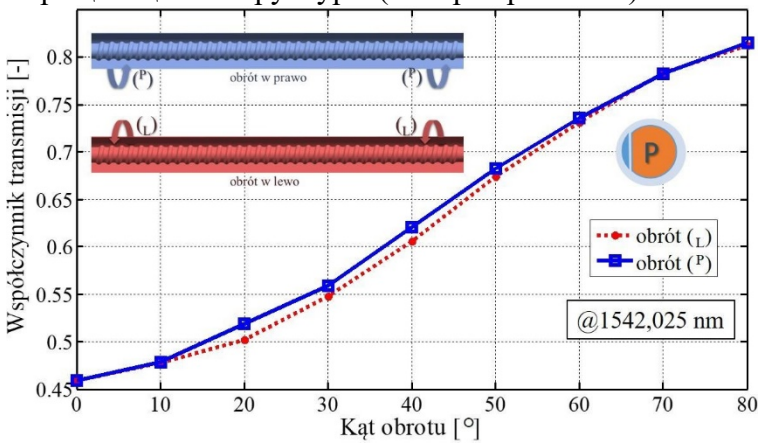


Рис.20 Изменение коэффициента пропускания НВРБ из-за вращения для длины волны 1542,025 нм. Возбуждается мода правой поляризации, вращение в направлении (P) и (L)

Как видно, вращение датчика увеличивает передачу НВРБ. Наибольшая чувствительность была получена в середине характеристик обработки для углов от 20° до 70°. Характер изменения коэффициента передачи для вращения (P) такой же,

как и для вращения (L) (рис. 20). Приведенные выше результаты показывают, что запись решетки НВРБ под углом 6° позволяет обнаруживать вращение оптического волокна путем измерения передачи системы на выбранной длине волны. Изменения коэффициента передачи системы аналогичны для вращения (P) и (L).

Для сравнения аналогичные кривые обработки построены на рис. 21, на котором показано значение длины волны, соответствующее минимуму в характеристике пропускания для выбранной моды оболочки. В этом случае характер длины волны минимального сдвига моды также аналогичен для вращений (P) и (L). Однако характерно различие в смещении минимального значения коэффициента пропускания, соответствующего мантийной моде (1542.025 нм).

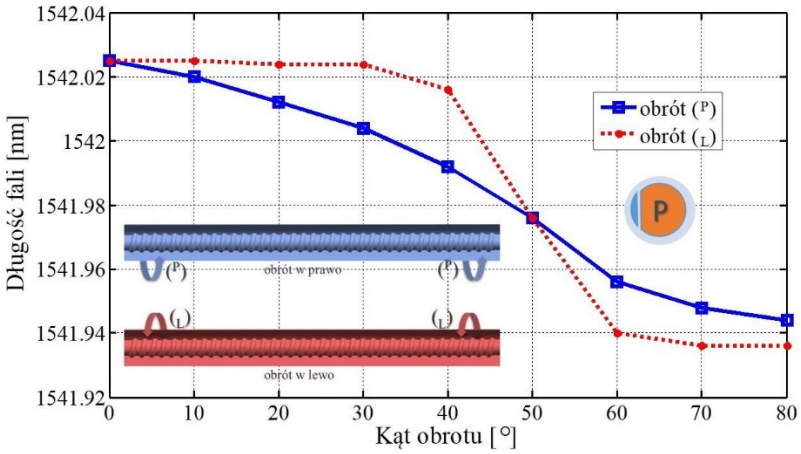


Рис.21 Длина волны изменяется в соответствии с минимальным значением передачи моды оболочки для вращения НВРБ. Возбуждается мода правой поляризации, вращение в направлении (P) и (L)

На рисунке 21 показаны изменения положения минимального пропускания моды оболочки, которая первоначально (для 0°) была локализована для длины волны 1542,025 нм по обе стороны от вращения (P) и (L) оптического волокна. Такой же характер изменений имеет место для всех других мод оболочки, минимумы которых появляются на характеристиках пропускания для других длин волн. Это связано с несимметричным возбуждением составляющих этой моды. Поэтому в дальнейшей части этой главы представлены характеристики обработки для других состояний возбуждения моды в структуре НВРБ, включая симметричное возбуждение (S | P).

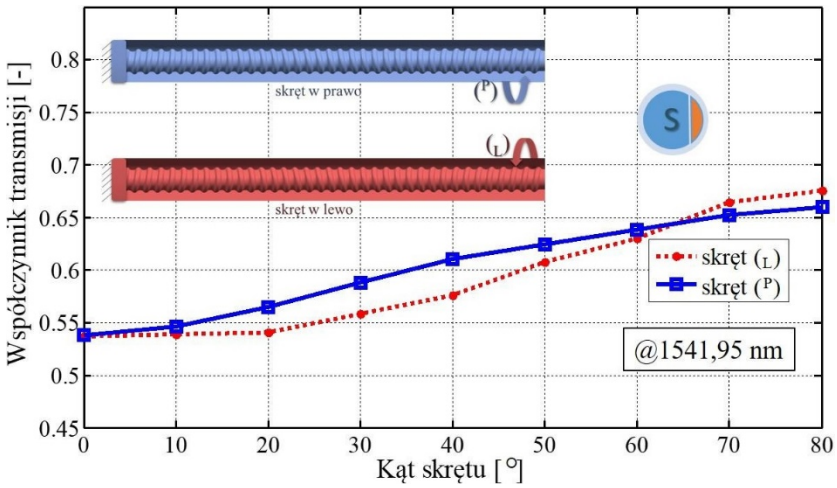


Рис.22 Изменение коэффициента пропускания НВРБ под влиянием кручения для длины волны 1541,95 нм. Включена мода левой поляризации, поворот в сторону (P) и (L)

Анализируя рисунок 22, можно увидеть, что скручивание структуры НВРБ - как и в случае вращения - влияет на значение коэффициента передачи для выбранной длины волны. На рисунке 22 показаны результаты, полученные в системе, в которой была возбуждена мода поляризации S. Предельные значения витка находились в диапазоне от + 80 °до -80°. Структура реагирует на кручение в диапазоне от + 80 ° до –80 °, изменяя коэффициент пропускания для выбранной длины волны (рис. 22).

Дальнейшая часть работы содержит описание, результаты измерений и их анализ для структуры НВРБ, закрученной с возбуждением мод S, S | P и P. На рисунке 23 приведены характеристики обработки сенсора в случае возбуждения левой поляризационной моды (S). В этом случае характерно увеличение длины волны, для которой наблюдается минимум моды оболочки.

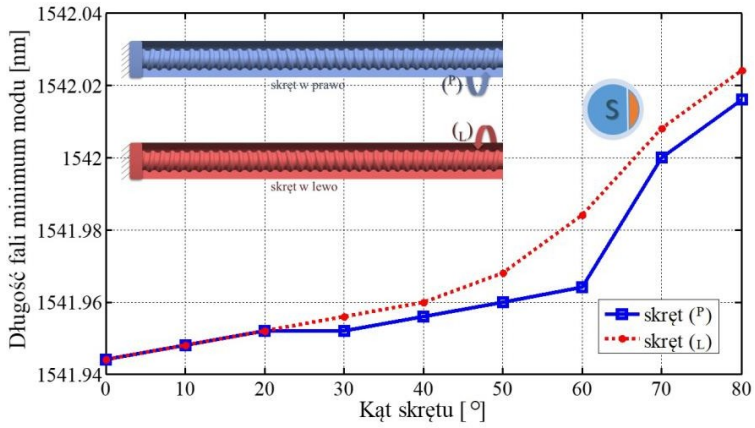


Рис.23 Длина волны изменяется в соответствии с минимальным значением передачи моды оболочки для поворота НВРБ. Включена мода левой поляризации, поворот в сторону (P) и (L)

На рисунке 23 показаны характеристики обработки в области, где такой минимум имеет место для выбранной моды. Если тестируемый элемент НВРБ

должен был использоваться в качестве датчика кручения, а контролируемой величиной был сдвиг минимальной длины волны моды, то знание состояния поляризации стимулированных мод могло бы сыграть важную роль. Смещение минимальной длины волны передачи НВРБ в сторону более длинных волн (рис. 23), а не более коротких (рис. 21) можно объяснить различием в возбуждении моды НВРБ. При возбуждении поляризационной моды S-типа большая часть энергии приходится на левую часть спектральной характеристики моды (так называемый левый пик, левый минимум). С другой стороны, скручивание структуры НВРБ вызывает связь возрастающего значения оптической мощности с минимумом, лежащим в правой части характеристики. Это «переполнение» мощности между модами и соответствующими минимумами, левым и правым, из-за кручения и того факта, что в исходном состоянии (структура НВРБ раскручена) возбуждение S-типа (левый пик) приводит к тому, что длина волны минимум, соответствующий данной моде оболочки, смещен в сторону более длинных волн. Важный вывод, вытекающий непосредственно из анализа этих измерений, заключается в том, что использование элемента НВРБ с известными параметрами для мониторинга, измерения или управления скручиванием требует дополнительных знаний о поляризации света, вводимого в оптическое волокно от НВРБ.

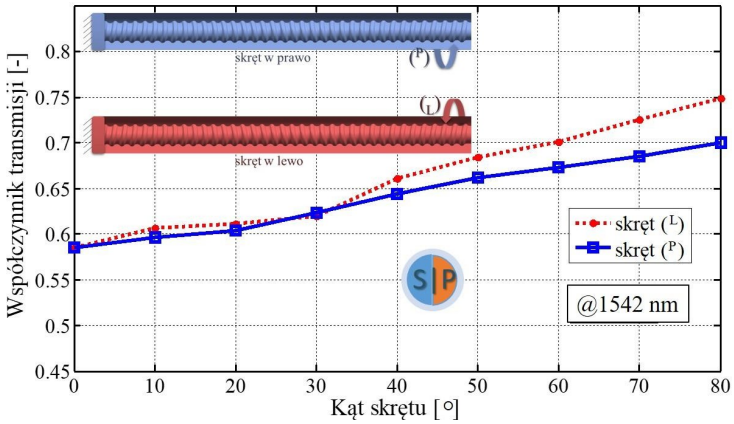


Рис. 24 Характеристики обработки поворота на передачи НВРБ для длины волны, равной 1541,95 Нм. Возбужденные две поляризационные моды: состояние S|P, поворот в направлении (P) и (L)

На рисунке 24 показаны результаты измерений коэффициента пропускания для углов поворота от 0 ° до 80 ° при равном возбуждении двух минимумов, соответствующих одной моде поляризации, которая согласно номенклатуре, предложенной в предыдущей части этой монографии, соответствует состоянию поляризации S|P. Чтобы можно было сравнить полученные результаты с данными, полученными в этой работе, и данными, описанными выше, измерения также были выполнены при повороте НВРБ в направлении (P) и (L). В этом случае, что касается состояния поляризации S, форма изменения коэффициента передачи системы для данной длины волны аналогична. Различия в значениях пропускания проявляются при больших углах кручения структуры НВРБ. Только после того, как угол кручения превысит 30°, между круткой (P) и (L) возникает разница в значении коэффициента передачи. Последующие исследования показали, что эти различия являются результатом несовершенства возбуждения S | P. Чем меньше разница в амплитуде левого и правого минимумов данной моды оболочки, тем меньше разница в значениях коэффициента прохождения для вращения (P) и (L). Поэтому геометрия

оптической системы играет ключевую роль в датчиках этого типа. Интересное явление наблюдается при измерениях минимальной моды оболочки при возбуждении S | P (рис.25).

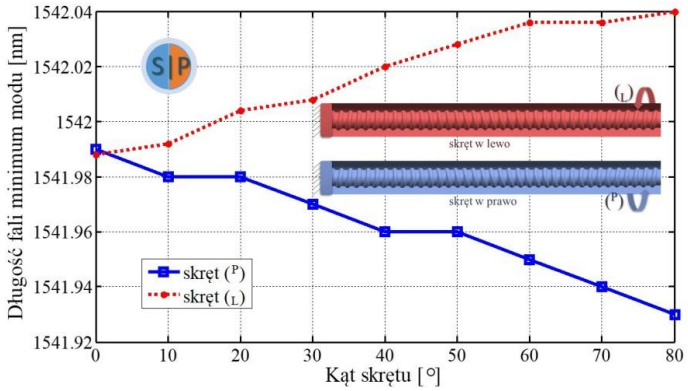


Рис.25 Характеристики обработки закрутки НВРБ на длине волны, соответствующей минимуму оболочки-моды. Стимулируются два режима поляризации: состояние S | P, поворот в сторону (P) и (L)

Характер изменения сдвига длины волны этого минимума совершенно иной для витков (P) и (L). Наклоны кривых обработки раскладки для этих поворотов имеют противоположные знаки. Скручивание (P) сдвигает длину волны минимальной моды оболочки в сторону более коротких волн, а скручивание (L), наоборот, в сторону более длинных волн (рис. 25). Абсолютные значения наклона характеристик обработки для (P) и (L) действительно похожи, но в случае скручивания (P) наклон отрицательный, в то время как скручивание (L) конструкции вызывает положительное крутизна характеристики обработки. Это связано с симметрией обоих минимумов оболочечной моды. В идеальных условиях начальное состояние, в котором ТПБР раскручивается, представляет собой точно такое же возбуждение обоих минимумов (S | P). Таким образом, если поворот (P) конструкции вызовет "перетекание" мощности из правого минимума передачи в левый минимум, то поворот (L) вызовет все большую и большую связь мощности с правым пиком передачи за счет левого. Это, в свою очередь, является причиной того, что изгиб (P) заставляет весь спектр мантийной моды сдвигаться в сторону более коротких длин волн, а изгиб (L) - в сторону более длинных волн. Объяснение этого явления, а также демонстрация его повторяемости позволяет утверждать, что с точки зрения приложений НВРБ для измерения физических величин, состояние поляризации введенного света S | P является наиболее благоприятным. Он позволяет определить вектор кручения, поскольку в этом случае можно определить знак (направление) кручения конструкции НВРБ. В заключительной части этой главы представлены характеристики обработки в случае возбуждения правой части поляризационной моды (рис. 26).

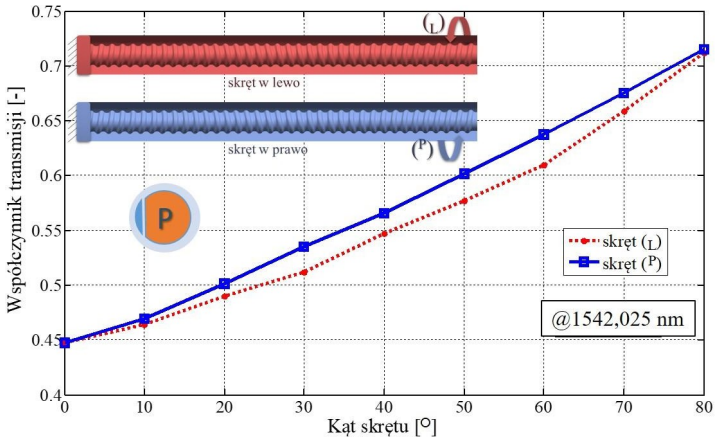


Рис. 26 Характеристики преобразования изменения крутки в передачу системы для длины волны 1542,025 нм. Режим правой поляризации (P) стимулирован, повернуть в сторону (P) и (L)

Характеристики обработки кручения НВРБ аналогичны характеристикам на рис. 23 и 25, но для возбужденных мод P-типа показан рисунок 27.

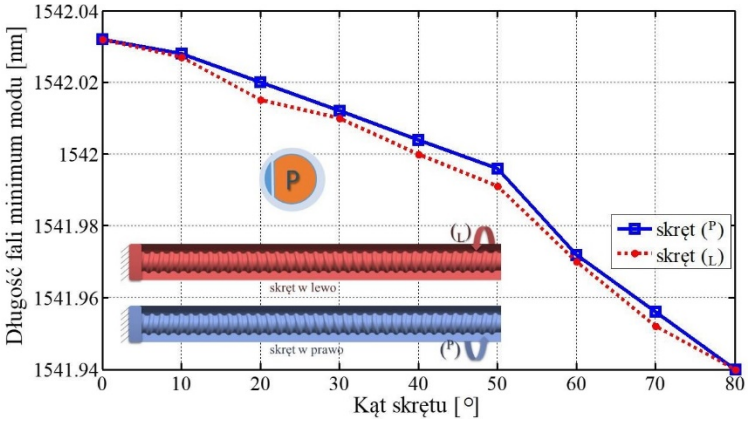


Рис. 27 Характеристики обработки НВРБ изменения поворота на длину волны, соответствующую минимальной передаче моды оболочки. Возбужденная правая поляризационная мода (P), поворот в направлении (P) и (L)

Структура реагирует на кручение в диапазоне от 80 ° (P) до 80 ° (L) с возбуждением моды правой поляризации, также изменяя длину волны, соответствующую минимальному коэффициенту передачи для данной моды оболочки (рис. 27). Сравнивая результаты, полученные для различных стимуляций и представленные на рисунках 23, 25, 27, можно увидеть, что только возбуждение типа S|P вызывает изменение угла наклона характеристики преобразования при оборотах (P) и (L). Также характерна симметрия характеристик преобразования для вращений (P) и (L), а также для типов S и P.

Заключение

Таким образом, в настоящей работе была продемонстрирована возможность измерения степени вращения и поворота оптического волокна с записанной в нем структурой НВРБ с углом наклона 6°. Было показано, что вращение датчика на 160° приводит к изменению коэффициента передачи от 0,45 до 0,83 для длины волны,

равной 1542,025 нм. Также было доказано, что наибольшая чувствительность может быть достигнута в средней части характеристик обработки для углов от 35° до 65°. Было показано, что одна и та же структура также может использоваться для измерения угла поворота. Это позволяет контролировать как угол поворота, так и скручивание оптического волокна. НВРБ реагирует на кручение 160 ° на длине 10 мм (от -80 ° до + 80 °), изменяя коэффициент передачи в диапазоне от 0,45 до 0,72 для длины волны 1542,025 нм, при этом наибольшая чувствительность к кручению наблюдается для входной поляризации P (рис. 26). Для входной поляризации типов S и S | P изменение значения коэффициента пропускания для выбранной длины волны даже в 2 раза меньше (рис. 22 и рис. 24). Таким образом, используя участок оптического волокна с записанным НВРБ и принимая коэффициент передачи для выбранной длины волны в качестве меры скручивания такой структуры, наиболее выгодным случаем будет предварительное возбуждение в структуре НВРБ моды P-типа за счет высочайшей чувствительности системы. Если, с другой стороны, возьмем минимальный модовый сдвиг на спектральных характеристиках пропускания в качестве меры поворота, наиболее благоприятным случаем будет начальное возбуждение мод типа S | P из-за возможности измерения вектора кручения.

Экспериментальные исследования проводились в лабораториях Оптоэлектроники факультета электротехники и компьютерных наук Люблинского технического университета в рамках проекта ГФ №AP09259547 «Разработка системы из распределенных волоконно-оптических датчиков на основе волоконных решеток Брэгга для контроля состояния строительных конструкций» ИИВТ КН МОН РК.

Литература

1. Jiang S., Wang J., Sui Q., Distinguishable circumferential inclined direction tilt sensor based on fiber Bragg grating with wide measuring range and high accuracy. Optics Communications 355, 58-63 (2015). doi: 10.1016/j.optcom.2015.05.055

2. Zhao Y., Wang Ch., Yin G., Jiang B., Zhou K., Mou Ch., Liu Y., Zhang L., Wang T., Fiber Specklegram Sensor Based on the Twist-induced Effect in Tilted Two-mode Fiber Bragg Gratings. 2017 Conference on Lasers and Electro-Optics Pacific Rim (CLEO-PR), 1-3 (2017). doi: 10.1109/CLEOPR.2017.8119080

3. Li F., Du Y., Sun X., Zhao W., Sensing performance assessment of twisted CFRP with embeddedfiber Bragg grating sensors subjected to monotonic and fatigue loading, Sensors and Actuators A 271, 153-161 (2018). doi: doi.org/10.1016/j.sna.2018.01.027

4. Song B., Zhang H., Miao Y., Lin W., Wu J., Liu H., Yan D., Liu B., Highly sensitive twist sensor employing Sagnac interferometer based on PM-elliptical core fibers, Optics express 23(12), 15372-15379 (2015). doi: 10.1364/OE.23.015372

5. Itoh, K., Saitoh, T., Ohtsuka, Y., Optical-rotation sensing by the geometric effect of fiber-loop twisting, Journal of Lightwave Technology 5, 916-919 (1987). doi: 10.1109/JLT.1987.1075584

6. Wang Q., Liu Y., Review of optical fiber bending/curvature sensor. Measurement 130, 161-176 (2018). doi: 10.1016/j.measurement.2018.07.068

7. Kim S.-W., Jeon B.-G., Kim N.-S., Park J.-Ch., Vision-based monitoring system for evaluating cable tensile forces on a cable-stayed bridge, Structural Health Monitoring 12(5-6), 440-456 (2013). doi: 10.1177/1475921713500513

8. Zhou Y., Zhou W., Chan Ch. Chi., Wong W. Ch., Shao L.-Y., Cheng J., Dong X., Simultaneous measurement of curvature and temperature based on PCF-based interferometer and fiber Bragg grating. Optics Communications 284, 5669-5672 (2011). doi: 10.1016/j.optcom.2011.08.048

9. Czaplicki Z., A New Method of Measuring Twist of Yarn, Fibres & Textiles in Eastern Europe 14(1), 27-29 (2006).

10.Ni Xi., Zhao Y., Yang J., Research of a novel fiber Bragg grating underwater acoustic sensor. Sensors and Actuators A 138, 76-80 (2007). doi: 10.1016/j.sna.2007.04.055

11.Budinski V., Donlagic D., Fiber-Optic Sensors for Measurements of Torsion, Twist and Rotation: A Review, Sensors 17(3), 443 (2017). doi: doi:10.3390/s17030443

12.Chen Y., Semenova Y., Farrell G., Xu F., Lu Y. Q., A compact sagnac loop based on a microfiber coupler for twist sensing, IEEE Photonics Technology Letters 27(24), 2579-2582 (2015). doi: 10.1109/LPT.2015.2478479

13.Smith D. W., Coherent fiberoptic communications, Laser Focus, 92-106 (1985).

14.Gao R., Jiang Y., Jiang L., Multi-phase-shifted helical long period fiber grating based temperature-insensitive optical twist sensor, Optics Express 22(13), 15697-15709 (2014). doi: 10.1364/OE.22.015697

15.Liu H., Zhu Z.-w., Zheng Y., Liu B., Xiao F., Experimental study on an FBG strain sensor, Optical Fiber Technology 40, 144-151 (2018). doi: 10.1016/j.yofte.2017.09.003

16.Ying Y., Zhang R., Si G.-Y., Wang X., Qi Y.-W., D-shaped tilted fiber Bragg grating using magnetic fluid for magnetic field sensor. Optics Communications 405, 228-232 (2017). doi: 10.1016/j.optcom.2017.08.009

17.Alberto N., Vigário C., Duartea D., Almeida N. A.F., Gonçalves Gil, Pintoc João L., Marques P. A.A.P., Nogueira R., Neto V., Characterization of graphene oxide coatings onto optical fibers for sensing applications, Materials Today: Proceedings 2, 171-177 (2015). doi: 10.1016/j.matpr.2015.04.019

18.Dong X., Zhang H., Liu B., Miao Y., Tilted Fiber Bragg Gratings: Principle and Sensing Applications, Photonic Sensors 1(1), 6-30 (2011). doi: 10.1007/s13320-010-0016-x

19.Guo T., Liu F., Guan B.-O., Albert J., Tilted fiber grating mechanical and biochemical sensors, Optics & Laser Technology 78, 19-33 (2016). doi: dx.doi.org/10.1016/j.optlastec.2015.10.007

20.Li M., Shao L.-Y., Albert J., Yao J., Continuously Tunable Photonic Fractional Temporal Differentiator Based on a Tilted Fiber Bragg Grating. IEEE Photonics Technology Letters 23(4), 251-253 (2011). doi: 10.1109/LPT.2010.2098475

21.Caucheteur Ch., Guo T., Albert J., Polarization-assisted fiber Bragg grating sensors: Tutorial and review, Journal of Lightwave Technology 35(16), 3311-3322 (2017). doi: 10.1109/JLT.2016.2585738

22.Cięszczyk S., Harasim D., Kisała P., Novel twist measurement method based on TFBG and fully optical ratiometric interrogation, Sensors and Actuators A 272, 18-22 (2018). doi: doi.org/10.1016/j.sna.2018.01.048

23.Yan Z., Mou C., Sun Z., Zhou K., Wang H., Wang Y., Zhang L., Hybrid tilted fiber grating based refractive index and liquid level sensing system, Optics Communications 351, 144-148 (2015). doi: 10.1016/j.optcom.2015.04.038

24.Cięszczyk S., Harasim D., Kisała P., A novel simple TFBG spectrum demodulation method for RI quantification, IEEE Photonics Technology Letters 29(24), 2264-2267 (2017). doi: 10.1109/LPT.2017.2768601

25.Kisała P., Harasim D., Mroczka J., Temperature-insensitive simultaneous rotation and displacement (bending) sensor based on tilted fiber Bragg grating, Optics express 24(26), 29922-29929 (2016). doi: 10.1364/OE.24.029922

26.Jiang Q., Hu D., Yang M., Simultaneous measurement of liquid level and surrounding refractive index using tilted fiber Bragg grating, Sensors and Actuators A: Physical 170(1-2), 62-65 (2011). doi: 10.1016/j.sna.2011.06.001

27.Morand A., Phan-Huy K., Desieres Y., Benech P., Analytical Study of the Microdisk's Resonant Modes Coupling With a Waveguide Based on the Perturbation Theory. Journal of Lightwave Technology 22(3), 827- 832 (2004). doi: 10.1109/JLT.2004.824528

28.Osuch T., Jurek T., Jędrzejewski K., Spectral transmission characteristics of weakly tilted and tilted chirped fiber gratings: comparative studies, Proceedings of SPIE 8903, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, 89030W-1- 89030W-6 (2013). doi: 10.1117/12.2035446

29.Miao Y.-p., Liu B., Zhao Q.-d., Refractive index sensor based on measuring the transmission power of tilted fiber Bragg grating. Optical Fiber Technology 15, 233-236 (2009). doi: 10.1016/j.yofte.2008.11.002

ОБ ОДНОМ ПОДХОДЕ ПОСТРОЕНИЯ ГРУППОВЫХ РЕШЕНИЙ В ЗАДАЧАХ КЛАССИФИКАЦИИ

Едилханулы Мейир
e-mail: meiredilkhanulu@list.ru
Казахский национальный университет имени аль – Фараби, Алматы, Казахстан

Аннотация. *В работе рассматривается возможность решения задачи группового синтеза классификаций для исходных алгоритмов. Рассмотрены различная конфигурация параметров алгоитмов классификации. В результате вычислительного эксперимента для определенных параметров алгоритмов, участвующих в групповом решении установлен наилучший вариант классификации.*

Ключевые слова. *групповое решение, алгоритм классификации, кластер, метрика близости, параметры алгоритмов, объект.*

Задача распознавания образов состоит в классификации объектов по нескольким классам (образам). Каждый объект характеризуется конечным набором признаков. Классификация происходит на основании анализа объектов, для которых мы знаем классы, которым они принадлежат. В основной постановке задачи классы известны для всех объектов выборки, после чего подаются новые объекты, которые требуется наиболее точно отнести к какому-то классу (классификация с учителем, Supervised learning).

Существуют множество алгоритмов и подходов к решению задачи полуконтролируемого обучения. Цель данной работы заключается в разработке нового подхода для решения задачи полуконтролируемого обучения, его теоретическом и экспериментальном обосновании. Новизна работы состоит в сочетании алгоритмов коллективного кластерного анализа и ядерных методов классификации.

Задачей кластерного анализа является разбиение выборки на непересекающиеся подмножества, называемые кластерами, так, чтобы каждый кластер представлял группу похожих объектов, а объекты в разных кластерах существенно различались. Решение задачи кластеризации не является однозначным по нескольким причинам:

- Не существует наилучшего критерия качества кластеризации. Известно большое число разумных эвристических критериев и алгоритмов, не имеющих явно заданного критерия, но осуществляющих достаточно качественную кластеризацию;
- Число кластеров очень часто неизвестно заранее и устанавливается либо вручную, либо в ходе работы алгоритма;
- Результаты кластеризации очень сильно зависят от метрики, которая выбирается экспертом и специфики прикладной области.

Кроме того, алгоритмы кластерного анализа не универсальны: каждый алгоритм имеет свою специфическую область применения. Например, некоторые алгоритмы направлены на «шарообразные» структуры данных, другие на «ленточные» кластеры и т.д.

На основании этих особенностей был предложен коллективный подход к кластерному анализу. В настоящее время коллективный подход показывает

наилучшие результаты по сравнению с отдельными алгоритмами и позволяет использовать преимущества и особенности сразу нескольких алгоритмов.

В системах интеллектуального анализа данных особое место занимает проблема классификации, поскольку необходимость в проведение классификация объектов встречается при решении широкого круга прикладных задач: при анализе кредитного риска, в медицинской диагностике, при распознавании рукописных символов (почерка), при категоризации текстов, при извлечении информации и т.п. Не менее актульно проведение качественной классификации данных в технических системах, например, при обработке изображений, полученных при дистанционном зондирований, при идентификации различных объектов (пешеходов, лиц и т.п.). На практике довольно часто приходится проводить декомпозицию объектов в случае, когда об их внутренних связах ничего неизвестно и заранее неизвестна группировка объектов, на основе которой можно определить принципы для их разделения. В таком случае в качестве первой задачи анализа, требующий решения, можно рассматривать задачу кластеризации, предполагающую выполнение обучения без учителья в машинном обучение с целью выявления внутренней структуры в данных. Следует отметить, что не существует универсальных алгоритмов и методов классификации и кластерного анализа. Более того, применение различных алгоритмов классификации к одному и тому же набору объектов может привести к различным результатом. Это связано с тем, что в основу этих агоритмов заложены различные принципы классификации и используемые в них метрики, функции близости, критерии оптимальности, способы выбора начальных параметров и т.п. В связи с этим возникает необходимость в получении результирующего классификационного решения, объединяющего результаты разбиений, полученные при реализации нескольких декомпозиционных алгоритмов, и совершающего меньшее число ошибок, чем каждый из этих алгоритмов.

Существует несколько вариантов получения группового решения задачи кластерного анализа, в предлагаемой в данной работе используется усредненная матрица коассоциации и метод основанных на выделении центральных объектов.

Сегодня алгоритмом групповых решений занимается ученые: Журавлев Ю.И., Рязанов В.В., Лбов Г.С., Бирюков А.С. (г. Москва), Мазуров В.Д. (г. Свердловск), Ивахненко А.Г. (г. Киев), Айдарханов М.Б., Мухамедғалиев И.А., Дүйсембаев А.Е, Амиргалиев Е.Н. (г. Алматы) и другие. Задачей полуконтролируемой обучения: Загоруйко Н.Г., Пестунов И.А., Бериков В.Б. (г. Новосибирск).

Пусть $A_1,...,A_m \in \{A\}$ – исходный заданный набор алгоритмов классификации и $M = \{S_1,...,S_n\}$ – конечное множество допустимых объектов, $M \subset D$. Результатом применения A_i к M является некоторая классификация из всевозможных вариантов классификации, т.е. из пространства классификации $K_i(M) \in \Re(M)$, где $\Re(M)$ - пространство классификации, элементами которого являются конкретные классификации. Основная задача группового синтеза состоит в следующем.

Пусть определена метрика $d(K',K'')$ в $\Re(M)$ и $F(\mathrm{K})=\sum_{i=1}^{m} d(K,K_i)$, $K \in \Re(M)$. Найти $K^*(M) \in \Re(M)$ такое, что $F(K^*) = \min_{K \in \Re(M)} F(K)$.

Пространство классификаций $\Re(M)$ конечно множества объектов $M = \{S_1,...,S_n\}$ помимо рассмотренных метрических свойств, обладает некоторыми "структурными" свойствами, которые также можно использовать для решения задач синтеза групповых классификаций [1].

Очевидно, что структура $\Re(M)$ не является булевой алгеброй, так как в ней, нетрудно проверить, не выполнены дистрибутивные законы, однако по аналогии с дискретной булевой алгеброй можно показать, что $\Re^{n-1}(M)$ - базис в $\Re(M)$.

Действительно, $\Re^{n-1}(M)$ является единственным из множеств $\Re^{l}(M)$, $l = 2,...,n-1,$ которое является дизъюнктным множеством. Также, очевидно, что ни для одного элемента $K \in \Re^{n-1}(M)$ не может существовать элемента K', удовлетворяющего неравенству $O < K' < K$, т.е. элементы $\Re^{n-1}(M)$ неделимы и являются атомами $\Re(M)$. Таким образом, пространство классификаций $\Re(M)$ характеризуется наличием минорантного дизъюнктного множества атомов $\Re^{n-1}(M)$.

Таким образом, в качестве метрики близости в пространстве классификации использована метрика, введенная в работе [2]. В качестве базовых алгоритмов использованы алгоритмы максиминного расстояния и К- внутригрупповых средних, рассмотренных в подробно в работе [3]. В качестве исходных объектов использованы данные, 61 объектов, характеризующиеся с 14 признаками, таким образом исходная информация представлена матрицей с размерностью 61x14 (реальные гидрогеологические данные, представленные Институтом гидрогеологии НАН РК). С помощью реализованной программы, исходные допустимые объекты классифицировались при различных параметрах алгоритмов, сначала максиминным методом, где получены центральные объекты будущих классов, затем корректировались методом К-внутригрупповых средних. В результате совместной работы двух алгоритмов получены следующие классификации для различных подобранных параметров:

Классификация 1

Алгоритм: максиминный метод + метод К-внутригрупповых средних

Входные параметры максиминного алгоритма: первый объект: S1, параметр: 0,4

Количество кластеров 12

Кластер 1 (7): S0, S1, S2, S3, S4, S7, S8; Кластер 2 (2): S11, S21;

Кластер 3 (8): S26, S34, S35, S36, S37, S39, S40, S41; Кластер 4 (1): S51;

Кластер 5 (6): S24, S27, S29, S30, S49, S50; Кластер 6 (2): S10, S15;

Кластер 7 (7): S9, S12, S17, S18, S19, S23, S31

Кластер 8 (9): S52, S53, S54, S55, S56, S57, S58, S59, S60

Кластер 9 (2): S16, S20

Кластер 10 (13): S22, S25, S28, S32, S33, S38, S42, S43, S44, S45, S46, S47, S48; Кластер 11 (3): S5, S6, S14; Кластер 12 (1): S13.

Классификация 2

Алгоритм: максиминный метод + метод К-внутригрупповых средних

Входные параметры максиминного алгоритма: первый объект: S1, параметр: 0,5

Количество кластеров 8

Кластер 1 (9): S0, S1, S2, S3, S4, S5, S7, S8, S13; Кластер 2 (2): S11, S21;

Кластер 3 (11): S26, S33, S34, S35, S36, S37, S38, S39, S40, S41, S42

Кластер 4 (1): S51; Кластер 5 (16): S16, S20, S24, S25, S27, S28, S29, S30, S43, S44, S45, S46, S47, S48, S49, S50; Кластер 6 (4): S6, S10, S14, S15;

Кластер 7 (9): S9, S12, S17, S18, S19, S22, S23, S31, S32;

Кластер 8 (9): S52, S53, S54, S55, S56, S57, S58, S59, S60.

Классификация 3

Алгоритм: максиминный метод + метод К-внутригрупповых средних

Входные параметры максиминного алгоритма: первый объект: S1, параметр: 0,6

Количество кластеров 6

Кластер 1 (13): S0, S1, S2, S3, S4, S5, S7, S8, S12, S13, S17, S18, S19

Кластер 2 (2): S11, S21; Кластер 3 (17): S22, S23, S26, S31, S33, S34, S35, S36, S37, S38, S39, S40, S41, S42, S53, S56, S60; Кластер 4 (7): S51, S52, S54, S55, S57, S58, S59; Кластер 5 (17): S16, S20, S24, S25, S27, S28, S29, S30, S32, S43, S44, S45, S46, S47, S48, S49, S50; Кластер 6 (5): S6, S9, S10, S14, S15

Классификация 4

Алгоритм: максиминный метод + метод К-внутригрупповых средних

Входные параметры максиминного алгоритма: первый объект: S52, параметр: 0,4

Количество кластеров 11

Кластер 1 (1): S51; Кластер 2 (2): S11, S21; Кластер 3 (2): S6, S14; Кластер 4 (8): S24, S27, S28, S29, S30, S32, S49, S50; Кластер 5 (3): S23, S26, S35; Кластер 6 (5): S12, S13, S17, S18, S19; Кластер 7 (2): S16, S20

Кластер 8 (3): S9, S10, S15; Кластер 9 (18): S22, S25, S31, S33, S34, S36, S37, S38, S39, S40, S41, S42, S43, S44, S45, S46, S47, S48;

Кластер 10 (9): S52, S53, S54, S55, S56, S57, S58, S59, S60

Кластер 11 (8): S0, S1, S2, S3, S4, S5, S7, S8

Классификация 5

Алгоритм: максиминный метод + метод к-внутригрупповыхсредних

Входные параметры максиминного алгоритма: первый объект: S52, параметр: 0,5

Количество кластеров 9

Кластер 1 (3): S51, S52, S59; Кластер 2 (2): S11, S21; Кластер 3 (4): S3, S5, S6, S14; Кластер 4 (8): S24, S27, S28, S29, S30, S32, S49, S50; Кластер 5 (10): S23, S26, S35, S53, S54, S55, S56, S57, S58, S60; Кластер 6 (11): S0, S1, S2, S4, S7, S8, S12, S13, S17, S18, S19; Кластер 7 (2): S16, S20

Кластер 8 (3): S9, S10, S15; Кластер 9 (18): S22, S25, S31, S33, S34, S36, S37, S38, S39, S40, S41, S42, S43, S44, S45, S46, S47, S48.

Классификация 6

Алгоритм: максиминный метод + метод к-внутригрупповыхсредних

Входные параметры максиминного алгоритма: первый объект: S52, параметр: 0,6. Получены кластера, с центрами соответственно S55 и S6.

Определяя расстояний между классификациями, получаем следующую таблицу расстояний:

Таблица 1. Расстояний между классификациями

	A_1	A_2	A_3	A_4	A_5	A_6	Сумма растояний
A_1	0	23	38	21	30	48	160
A_2	23	0	21	32	43	49	168
A_3	38	21	0	33	35	44	171
A_4	21	32	33	0	15	43	144
A_5	30	43	35	15	0	43	166
A_6	48	49	44	43	43	0	227

Из таблицы видно, что наиболее приближенной ко всем классификациям является классификация, полученная в результате выполнения алгоритма A_4 (максиминный метод + метод К- внутригрупповых средних с входными параметрами: первый объект: S52, параметр: 0,4).

Таким образом, групповой синтез на базе двух алгоритмов при различных параметрах дает классификацию на базе алгоритма A_4 , что и является искомым решением.

Литература

1. M.B. Aidarkhanov. Metric and Structural Approaches to the Construction of Group Classifications // Pattern Recognition and Image Analysis. USA 1994. Vol.4, №4, P. 372-389

2. Айдарханов М.Б. Методы синтеза классификации для конечных и континуальных множеств объектов. Алматы, Галым, 1994, 200с.

3. Амиргалиев Е.Н. Теория распознавания образов и кластерного анализа. Алматы, Издательский Центр КазНТУ, 2003, 340с.

ОЦЕНКА ЭПИДЕМИОЛОГИЧЕСКОЙ СИТУАЦИИ САХАРНОГО ДИАБЕТА В РЕСПУБЛИКЕ КАЗАХСТАН: НОВОЕ ВИДЕНИЕ

Ескермес Т.Е., Бимурат Ж., Мукашева А.К.
e-mail: t.yeskermes@aues.kz, zh.bimurat@aues.kz, a.mukasheva@aues.kz

Алматинский университет энергетики и связи имени Г.Даукеева, Институт информационных технологии, Кафедра Информационных систем и кибербезопасности, Казахстан

Аннотация. *Ситуация с распространенностью диабета в Казахстане вызывает беспокойство, так как согласно данным, предоставленным Общественным фондом «Казахстанское общество по изучению диабета», количество диагностированных людей с диабетом в 2018 году превышает 300 тысяч человек. В РК СД отводится в ранг социально значимых заболеваний, это требует разработки и принятия мер по улучшению лечения заболеваний и увеличению продолжительности жизни граждан. В статье был сделан обзор эпидемиологической ситуации в Республике Казахстан с помощью статистических методов с применением информационных технологии в области обработки и визуализации данных. Вся исследовательская работа проводилась с использованием библиотеки Pandas языка Python и встроенных функций Excel для статистической обработки медицинских данных.*

Сахарный диабет (СД) признан самым быстрорастущим хроническим неинфекционным заболеванием (НИЗ) в мире. Общее количество людей с диабетом 2 типа растет в каждой стране [5]. Уровень заболеваемости СД в мире за последние два десятилетия вырос почти вдвое, то есть ожирение и другие проблемы со здоровьем, которые он порождает, с каждым днем увеличиваются [3]. Диабет был определен как одно из четырех приоритетных неинфекционных заболеваний (НИЗ), на которые Организация Объединенных Наций (ООН) акцентирует внимание из-за растущего бремени [8].

По официальным данным ВОЗ, в РК около 11,5% людей от общего количества населения страны страдают от СД; из которых представители женского пола составляют - 11,7%, а мужского пола – 11,3% [2]. Согласно материалам Национального регистра, в Казахстане зарегистрированных пациентов в 2018 году составило 317 597 человек. Общее количество взрослого населения страдающих от диабета – 314 407 человек, до 14 лет 2 379 человек, а также от 15 до 17 лет 811 человек. В РК действующий регистр по сахарному диабету содержит данные только о больных, которым уже было диагностировано данное заболевание. Следует учитывать, что значительное количество пациентов наблюдается в частных медицинских организациях и эти данные не охвачены регистрацией [6].

Для разработки эффективной программы профилактики и борьбы с сахарным диабетом в РК необходимо в первую очередь оценить текущую ситуацию в отношении заболеваемости, смертности, госпитализации в стране с использованием

комплексных статистических методов. К сожалению, данная практика пока не внедрена в полной мере в практику здравоохранения Казахстана, хотя в последние годы были предприняты определенные шаги как со стороны Комитета по статистике [1], так и научного сообщества [4]. Анализ вышеперечисленных показателей и их тенденция на региональном, национальном, глобальном уровнях позволяют выявлять проблемные стороны, оценивать и отслеживать предпринятые интервенции и принимать правильные решения.

Для проведения данного эпидемиологического исследования были использованы данные, которые были получены из официальных источников Министерства здравоохранения РК, Комитета статистики МНЭ РК, базы данных смертности ВОЗ, а также данных из публикаций журналов базы данных Scopus. Во время статистических экспериментов и исследований были включены в обработку подсчеты абсолютных чисел, процентные соотношения, медиана для неправильных данных. Для анализа базы данных были использованы MS Office Excel 2010, SAS University Edition, Python 3.8.4.

Согласно базе Диспансерного учета пациентов, состоящих с диагнозом сахарный диабет за 2019 г., в РК наблюдается значительный рост абсолютного числа зарегистрированных пациентов с диагнозом СД от 143266 до 373183 пациента. Направление в области прогнозирования СД в РК было изложено в исследовании [7], где авторы отмечают, что с помощью библиотеки Scikit-learn машинного обучения и методов регрессионного анализа вполне возможно осуществить прогноз роста пациентов СД в РК. Результаты, полученные с помощью Python, сравнивались с результатами, полученными с помощью Excel, где при сравнении было обнаружено, что эти методы дают одинаковые предположительные значения.

Процесс сбора, хранения и обработки медицинских данных является основной проблемой для решения актуальных задач в области здравоохранения. Необходимо использовать современные инструменты информационных технологии, чтобы эффективно применять цифровые медицинские данные для обеспечения поддержки принятия решений в этой области. Для исследования были использованы медицинские данные, предоставленные ОФ «Казахстанское общество по изучению диабета» в рамках целевой программы «Бремя диабета 2019-2020 для РК». Набор данных включает в себя всю информацию об диспансерных больных всех граждан РК, состоящих на учете с диагнозом «Сахарный диабет» с 31.12.2009 г. по 31.12.2019 г. Для решения поставленных задач использовалось программное решение Anaconda, который включает в себя все необходимые инструменты для решения задач по анализу и обработке данных. Дистрибутив Anaconda состоит из интерпретатора Python и содержит множество различных пакетов для обработки данных, включающих в себя популярные библиотеки такие как NumPy, Pandas, SciPy, Matplotlib. Для обработки данных использовался инструмент Jupyter Notebook, который входит в пакет Anaconda. Pandas – один из самых популярных инструментов Python для работы с данными, она поддерживает различные текстовые, бинарные и SQL форматы файлов, в том числе .xlsx, .xls и .csv. Для работы с файлами Excel Pandas использует модули xlrd и xlwt.

Для загрузки файлов в необходимо импортировать необходимые библиотеки для исследовательского анализа данных. Далее необходимо проверить, какое количество данных было загружено. На рисунке 4 приведены результаты количества строк и столбцов всех файлов, где общее количество строк превышает 2700000 записей.

```
In [47]: df.shape
Out[47]: (2705693, 8)
```

Рис. 1 Результаты подсчета всех строк и столбцов

В данном исследований для визуализации данных использовалась библиотека matplotlib, позволяющая визуализировать поступающие данные, после обработки в Pandas. На рисунке 2 можно увидеть результаты обработки подсчета количества пациентов состоящих на учете с диагнозом СД по регионам РК.

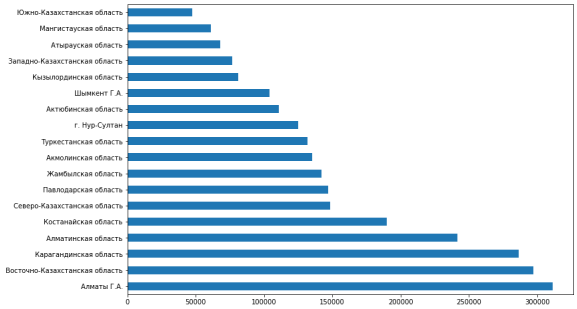


Рис. 2 Визуализация количества пациентов по регионам

Также в результате обработки и визуализации были получены числовые значения количества пациентов с диагнозом СД по регионам РК.

```
In [43]: obl
Out[43]: Алматы Г.А.                    311212
         Восточно-Казахстанская область 297488
         Карагандинская область         286442
         Алматинская область            241780
         Костанайская область           189781
         Северо-Казахстанская область   148549
         Павлодарская область           146734
         Жамбылская область             142321
         Акмолинская область            135296
         Туркестанская область          131831
         г. Нур-Султан                  124775
         Актюбинская область            110776
         Шымкент Г.А.                   104041
         Кызылординская область          81184
         Западно-Казахстанская область   76792
         Атырауская область              68047
         Мангистауская область           61018
         Южно-Казахстанская область      47626
         Name: Регион, dtype: int64
```

Рис. 3 Результаты числовых значений

В продолжении осуществлен подсчет количества всех зарегистрированных пациентов по РК с 2009 г. по 2019 г.

```
In [40]: year
Out[40]: 2019    373183
         2018    331901
         2017    309248
         2016    287189
         2015    260627
         2014    241496
         2013    220621
         2012    198728
         2011    178594
         2010    160840
         2009    143266
         Name: Год, dtype: int64
```

Рис. 4 Числовые значения зарегистрированных пациентов по РК

Для более глубокого исследовательского анализа данных, используя два файла состоящие из двух частей за 2019 год, исследуем данные по регионам, полу,

возрасту и т.д. Далее можно загрузить предоставленные Excel файлы в DataFrame (data1 и data2).

```
In [2]: files = [f for f in os.listdir("./") if f.endswith(".xlsx")]

data1 = pd.read_excel(files[0],encoding = "cp1251", skiprows = range(0,7)).drop([0]).reset_index(drop=
True)
data2 = pd.read_excel(files[1],encoding = "cp1251", skiprows = range(0,7)).drop([0]).reset_index(drop=
True)
```

Рис. 5 Загрузка data1 и data2

Последняя строка data1 совпадают с первой строкой data2. Это позволяет нам объединить эти два отдельных DataFrames в один DataFrame (combined_data).

```
In [8]: combined_data = pd.concat([data1.drop([len(data1)-1]), data2]).reset_index(drop=True)
combined_data
```

Рис. 6 Объединение двух файлов

После объединения двух файлов, получаем 112626 строк и 41 столбец данных. Информация, хранящаяся в объединенных файлах позволяет исследовать данные о месте прохождения лечения пациентов по РК. С помощью визуализации можно наблюдать результаты обработки на рисунке 7.

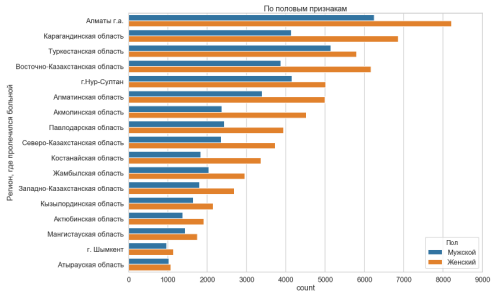


Рис. 7 Статистика регионов, где проходили лечение пациенты

Используя данные базы Диспансерного учета по диабету за 2019 года был просчитан возраст специфической распространённости стандартизированная по возрасту. Наблюдается резкий рост распространённости СД у двух полов с возрастной группы 55-59 лет и доходит пика в группе 65-69 лет. Женщин, состоящих на Д учете, выше чем мужчин начиная с группы 50-54 и с каждой возрастной группой отмечается значительная разница.

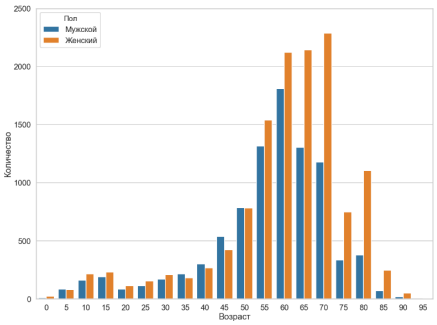


Рис. 8 Распространенность СД у женщин и мужчин по возрастным группам в РК за 2019г

В РК на конец 2019 года на Д-учете с диагнозом СД состоит 373 183 человек. Медиана возраста пациентов, состоящих на Д-учете с СД, составляет 62 года, а межкратильный интервал (55 и 69 лет). То есть 50% от всех пациентов, состоящих на Д-учете с СД входят в возрастной интервал между 55 и 69 лет.

Скорая помощь и самообращение характеризуются экстренной доставкой пациента, тогда как первичная медико-санитарная помощь (ПСМП) и консультативно-диагностическая помощь (КДП) и прочие - по большей части были плановыми. Важно отметить, что около 45% госпитализированных пациентов с СД были направлены сотрудниками ПМСП, 22% скорой неотложной помощью, 13,8% по самообращаемости. Следующим примером для вычислений были использованы данные о количестве койко-дней в среднем на рисунке 9.

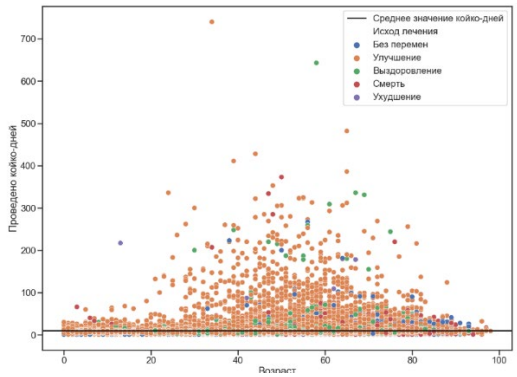


Рис. 9 Среднее значение проведенных койко-дней пациентам

Согласно рисунку 9 несмотря на некоторые значения в более 200 дней, средним значением койко-дней является значение около 10 (отмечено черной линией). Диаграмма показывает, что в возрасте от 30 до 70 лет вероятность провести более 50 койко-дней возрастает.

После проведенных исследований можно сделать выводы, что отставание в продолжительности жизни в Казахстане от развитых стран определяется чрезмерной смертностью от неинфекционных заболеваний (НИЗ). Так же можно отметить, что чрезмерная преждевременная смертность от НИЗ в Казахстане вызвана преимущественно поведенческими факторами. Рост потребления сахаросодержащих напитков и продуктов быстрого приготовления в Казахстане, как и во всем мире, приводит к росту ожирения и СД у все более молодых групп населения, с последующими увеличениями заболеваемости и смертности от СД и НИЗ. Исходя из мульти-факторной теории программа борьбы с НИЗ должна включать как медикаментозную терапию, так и меры по ограничению потребления сахаросодержащих напитков и продуктов быстрого приготовления.

По результатам работы была осуществлена эпидемиологическая оценка зарегистрированных пациентов в РК с помощью статистических инструментов, где было выявлено, что рост заболеваемости неуклонно растет. А для усовершенствования анализа эпидемиологической ситуации были использованы передовые информационные технологии в области анализа и обработки данных для визуализации различных задач. Публикации авторов, использованных в процессе

работы о прогнозировании на 2019 год, подтвердились исследованиями, описанными в этой статье.

Литература

1. Агентства Республики Казахстан по статистике. Методика расчета стандартизированных коэффициентов рождаемости и смертности // Методическое руководство. – Астана, 2012. – С. 1-10

2. ВОЗ - Информация о странах с диабетом, 2016. https: //www.who.int/diabetes/country-profiles/kaz_ru.pdf?ua=1 (03.08.2021)

3. Глобальные показатели диабета растут по мере распространения ожирения. https://www.nytimes.com/2015/06/08/health/research/global-diabetes-rates-are-rising-as-obesity-spreads.html. (01.08.2021)

4. *Давлетов К.К., Беркинбаев С.Ф., Амиров Б.Б.* Стандартизация показателей смертности от БСК в Казахстане // Методические рекомендации. – Астана, 2014. – С. 1-32

5. Диабет во всем мире. https://www.diabetesaustralia.com.au/diabetes-globally. (01.06.2020)

6. *Туякбаева А.С.* Состояние проблемы и пути профилактики сахарного диабета //Центрально-Азиатский журнал по общественному здравоохранению. – Том 11. – №2 – Алматы. – 2012.-с.8

7. *Mukasheva, A., Saparkhojayev, N., Akanov, Z.* et al. Forecasting the Prevalence of Diabetes Mellitus Using Econometric Models. Diabetes Ther 10, 2079–2093 (2019)

8. United Nations General Assembly. Resolution adopted by the General Assembly on 27 July 2012: the future we want (A/RES/66/288). http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/66/288&Lang=E Date: Sept 11, 2012 Date accessed: March 3, 2018

ОБРАБОТКА ГОЛОСОВОЙ ИНФОРМАЦИИ ДЛЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ

М.С. Әлиасқар[2], Т.Ж. Мазаков[1,2], Г.С. Байрбекова[1], Н.Т. Исимов[1], Т.С.Шорманов[2], Д.К. Мухаев[2]
87019931011@mail.ru
[1]*Институт информационных и вычислительных технологий КН МОН РК, Казахстан*
[2]*Казахский национальный университет имени аль-Фараби, Казахстан*

***Аннотация**. Потребность в проверке личности людей с помощью надежных методов и параметров быстро возрастает во всем мире в эту информационную эпоху из-за желания сообщества выполнять повседневные процессы, такие как перевод денег или запрос услуги с использованием удаленных систем или колл-центров. Используя наши биометрические функции, методы аутентификации теперь могут выполняться только с использованием смартфонов, камер или только микрофона. Принимая во внимание рост числа мошеннических атак в последнее время из года в год и возможность его аутентификации, не сталкиваясь лицом к лицу с истцом, неудивительно, что использование технологии голосовой аутентификации растет в сфере банковских услуг и центров обработки вызовов. Это исследование представляет собой краткий обзор основных методов и исследований в области биометрии для личной идентификации.*

***Ключевые слова**: биометрические технологии, голосовая аутентификация, извлечение голосовых характеристик, моделирование динамиков.*

Введение. В современном мире все больше проявляется интерес к голосовым технологиям, в частности, к идентификации личности. Это объясняется, с одной стороны, появлением высокопроизводительных вычислительных систем на базе персональных компьютеров и аппаратных средств, позволяющих производить ввод сигнала в компьютер, а, с другой стороны, высокой потребностью систем аутентификации в разных областях.

Метод опознавания личности по голосу существует с тех пор, как человек научился говорить. Поэтому достоинства и недостатки этого метода известны всем. Как не всегда по ответу на вопрос «Кто там?» мы можем определить, что за дверью стоит знакомый человек, и приходится развеивать свои сомнения, заглянув в дверной глазок, так и техническая система идентификации может ошибаться в силу изменения голоса отдельного человека.

Привлекательность данного метода - удобство в применении. Метод проверки голоса имеет два положительных отличия от остальных биометрических методов. Во-первых, это идеальный способ для телекоммуникационных приложений. Во-вторых, большинство современных компьютеров уже имеют необходимое аппаратное обеспечение. Продукты с проверкой голоса сейчас предлагают банки и другие компаний.

Основная проблема, связанная с этим подходом, - точность идентификации. Однако это не является серьезной проблемой с того момента, как устройства

идентификации различают характеристики человеческой речи. Голос формируется из комбинации физиологических и поведенческих факторов.

Идентификация по голосу удобный, но в тоже время не такой надежный, как другие биометрические методы. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. Существует также возможность воспроизведения звукозаписи.

Методы исследования. Биометрическая система, по существу, распознает или извлекает шаблоны определенных физиологических или поведенческих характеристик, которыми обладает целевой человек, и использует эти шаблоны для сопоставления с заданными данными.

К настоящему моменту у нас и за рубежом реализованы системы автоматической идентификации по голосу, большинство из которых строятся по единой концептуальной схеме:

- производится регистрация пользователя и вычисляется шаблон;
- выбираются участки речевого потока для дальнейшего анализа;
- осуществляется первичная обработка сигнала;
- вычисляются первичные параметры;
- строится «отпечаток» (шаблон) голоса;
- производится сравнение «отпечатков» голосов и формируется решение по идентичности голосов или «близости» голоса к группе голосов [1].

Гипотетически биометрическая система состоит из двух основных модулей: регистрации и идентификации. Система сканирует особенности или, другими словами, биометрические характеристики человека с помощью биометрического датчика, получает цифровое представление этих функций и сохраняет его в качестве шаблона в центральной базе данных или на смарт-карте на этапе регистрации.

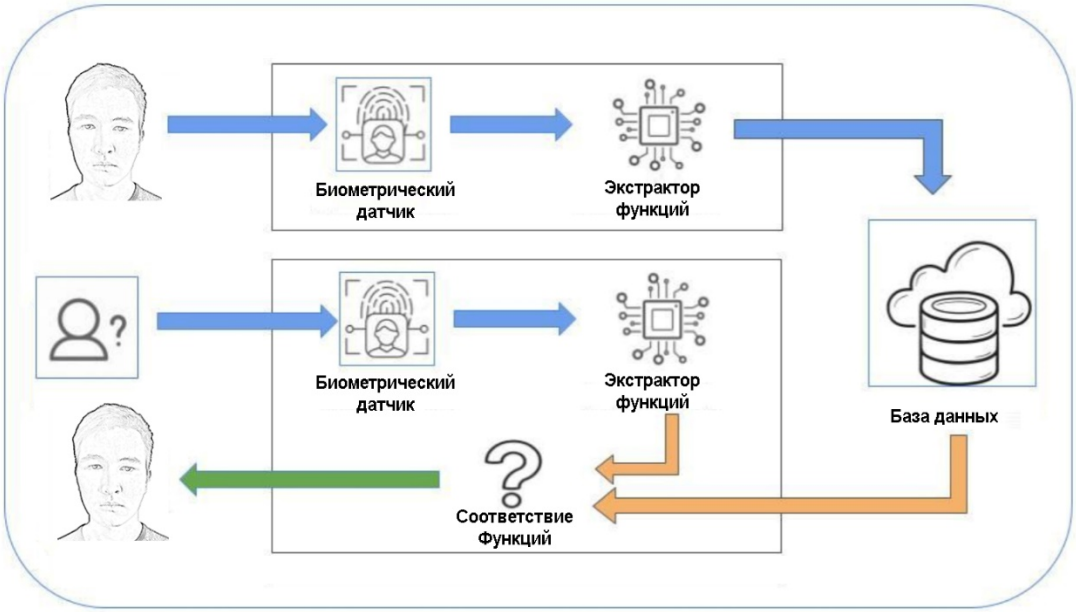


Рисунок 1 – Гипотетическая биометрическая система

Модуль распознавания снова сканирует биометрические характеристики целевого человека и преобразует их в цифровой формат, который используется на этапе регистрации. Затем система использует эти данные для сопоставления

характеристик, что означает сравнение полученных данных с шаблонами для определения личности человека.

Общая производительность биометрической системы оценивается по ее показателю точности, скорости и хранению. Биометрические системы могут принять мошенника как действительного человека, и это называется «ложным совпадением» или, наоборот, система может отказать действительному лицу, и это называется «ложным несоответствием» [2].

Образец голоса – это индивидуальная характеристика, и невозможно найти двух людей с точно такой же спектрограммой. Спектрограмма – это визуальная запись речи, проанализированная по частоте, продолжительности и амплитуде. Поскольку голосовой отпечаток уникален для своего владельца, его можно использовать для уникальной идентификации.

Необходимое оборудование для голосовой аутентификации – это просто микрофон, поэтому его стоимость настолько мала, им легко пользоваться, и технология распознавания голоса сегодня присутствует в наших смартфонах. Но, конечно, он не идеален, как другие биометрические характеристики. Самый большой недостаток голоса в том, что он меняется в зависимости от возраста, и при переходе от детства к подростковому возрасту могут произойти резкие изменения. Также на голос могут негативно повлиять болезнь и мгновенные эмоции, акустика помещения и окружающий шум [3].

Голосовая аутентификация рассматривается как проблема распознавания образов, которая является ветвью машинного обучения. Основная задача при разработке системы голосовой аутентификации - извлечение речевого сигнала. Для извлечения речевых характеристик из речевого сигнала доступны некоторые методы. Модели динамиков создаются для отдельных лиц и сохраняются в виде голосовых баз данных после извлечения функций. Для создания моделей динамиков могут использоваться методы моделирования, включая векторное квантование (VQ), GMM (модели гауссовой смеси), HMM (скрытые марковские модели) и т.д.

Задача аутентификации говорящего состоит из двух компонентов: извлечения функций и сопоставления их, как упоминалось ранее. После извлечения уникальных характеристик из входной речи функции сравниваются с шаблонами выступающих, которые создаются с помощью различных методов моделирования и сохраняются [4].

Рисунок 2 – Блок-схема системы распознавания говорящих

Методы сопоставления функций используются как на этапе обучения, так и на этапе тестирования. Чтобы построить модель динамика, система обучается с использованием извлеченных функций на этапе обучения. Эта модель проверяется системой на этапе тестирования посредством распознавания выступающих.

Наиболее часто используемые методы построения моделей: векторное квантование (VQ), скрытая марковская модель (HMM) и модель гауссовой смеси (GMM) [5].

Векторное квантование (VQ): векторное квантование, пожалуй, самый простой алгоритм для сопоставления признаков и создания моделей с использованием векторов признаков. Тип VQ – это алгоритм обучения без учителя. Он создает кластеры, которые представляют модели зарегистрированных спикеров.

Во-первых, полученные векторы признаков классифицируются в разные кластеры. Кластеры включают в себя векторы признаков со схожими свойствами, и эти похожие векторы моделируют атрибуты говорящих. Сначала получаются векторы признаков, затем они сравниваются с центроидами уже существующих кластеров. Для этого используется расчет евклидова расстояния. Алгоритм помещает вектор признаков в кластер с минимальным расстоянием. После назначения вектора кластеру центроид кластера обновляется. Другой термин для центроидов – это «кодовые слова», а термин «кодовая книга» используется для набора кодовых слов.

Скрытая марковская модель (HMM): HMM может моделировать статистические вариации характеристик, давать статистическое представление о том, как динамик воспроизводит звук [6]. Следовательно, HMM является более эффективным алгоритмом сопоставления признаков по сравнению с традиционной моделью VQ.

Модели HMM – это статистические модели, основанные на идее, которая является «распределением вероятностей состояния для времени x, условно независимого от всех предыдущих состояний, когда состояние во время x-1 задано. Кроме того, мы не можем напрямую определить состояния, для которых они невидимы. используйте или, другими словами, они «скрыты», но мы можем использовать параметры наблюдения для прогнозирования состояний. Цель состоит в том, чтобы определить эти скрытые значения состояния с помощью наблюдаемых параметров.

HMM - один из лучших методов анализа голоса, потому что он имеет четко определенную математическую структуру, не требует экспертных знаний о речевом сигнале, не накапливаются ошибки в анализе и не требует большого количества шаблонов.

Модель гауссовой смеси (GMM): модель гауссовой смеси - один из наиболее распространенных и успешных методов моделирования динамиков. Речевые атрибуты легко могут быть распределены по Гауссу, поэтому GMM - очень эффективный способ моделирования [7]. Плотность гауссовой смеси представляет собой взвешенную сумму M плотностей компонентов, где M представляет собой количество гауссианов. Каждого говорящего можно эффективно смоделировать и представить с помощью GMM, и на него ссылается модель, связанная с ним / ней.

Выводы. Биометрические – это общее название процессов, используемых для проверки и идентификации людей путем измерения их физиологических и поведенческих характеристик. Биометрические идентификаторы более надежны по сравнению с методами, основанными на знаниях и токенах, поскольку они обладают такими сильными характеристиками, как универсальность, уникальность, постоянство и возможность сбора. Наиболее часто используемые биометрические параметры – это отпечатки пальцев, геометрия руки, распознавание лиц, сетчатка, радужная оболочка глаза, голос, и каждая из них имеет свои плюсы и минусы по сравнению с другими.

Голосовая аутентификация может быть объяснена как распознавание говорящего с использованием информации, уникальной для человека. Системы распознавания громкоговорителей сначала извлекают из речевого сигнала определенные характеристики, а затем создают модели или шаблоны громкоговорителей для хранения этих функций. Наконец, система сравнивает голос, который должен быть аутентифицирован, с сохраненными шаблонами или голосовыми распечатками и пытается определить, совпадают ли они.

Системы голосовой аутентификации все чаще используют методы биометрии, потому что они не требуют никакого оборудования, кроме микрофона, взаимодействие пользователя не является обязательным и реализуется с помощью методов, основанных на сильной математической основе. Системы распознавания голоса, которые в настоящее время используются в таких областях, как судебная экспертиза и банковское дело.

Работа выполнена за счет средств программы целевого финансирования на основе договора по оказании услуг субподряда «Разработка национального электронного банка данных по научной зоологической коллекции Республики Казахстан, обеспечивающего их эффективное использование в науке и образовании».

Литература

1. Singh N., Agrawal A., Khan R.A., Голосовая биометрия: технология аутентификации на основе голоса, передовая наука, инженерия и медицина / Июль 2018

2. Todkar S.P., Babar S.S., Ambike R.U., Suryakar P.B., Prasad J.R., Методы распознавания докладчиков / 3-я Международная конференция по конвергенции в технологиях 2018 г.

3. Ahmad, K. S., Thosar, A. S., Nirmal, J. H., & Pande, V. S. «Уникальный подход к распознаванию говорящего независимо от текста с использованием наборов функций MFCC и вероятностной нейронной сети» / Восьмая международная конференция (ICAPR), 2015 г.

4. N.Dehak, P.Kenny, R.Dehak, P.Dumouchel, P.Ouellet , Front-end факторный анализ для проверки докладчика / IEEE Transactions on Audio, Speech, and Language Processing – 2011г.

5. Y. Lei, N. Scheffer, L. Ferrer, and M. McLaren, «Новая схема распознавания говорящего с использованием фонетически осведомленной глубокой нейронной сети» / Международная конференция по акустике, речи и обработке сигналов (ICASSP), 2014г.

6. Bahmaninezhad F., Hansen J., Распознавание динамиков i-Vector / PLDA с использованием опорных векторов с дискриминантным анализом / Международная конференция IEEE по акустике, обработке речи и сигналов (ICASSP), 2017 г.

7. D. Garcia-Romero, A. McCree, Анализ глубинных нейронных сетей для распознавания говорящего / Interspeech 2015г.

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ГОРОДСКИМ ТРАНСПОРТОМ ЗА СЧЕТ ВНЕДРЕНИЯ УМНЫХ ПАРКОВОК

О.Долинина, М.Мансурова, Ж.Байгараева, С.Баязитова
e-mail: zhanel.baigarayeva@gmail.com
КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛЬ-ФАРАБИ, КАЗАХСТАН

Аннотация

Быстрый рост населения и рост числа автомобилей привел к увеличению транспортных проблем в мегаполисах в том числе в связи с отсутствием достоверной информации о парковочных местах и необходимого управления парковками. Предлагается решение данной проблемы за счет создания умных парковок. В статье приведен подробный обзор существующих технологий аппаратного, программного и организационного обеспечения умных парковок. Приведены описания различных типов парковок. Отдельно рассмотрена ситуация с внедрением умных парковок в республике Казахстан. Показано, что несмотря на преобладание при реализации систем Интернета вещей облачных технологий, в настоящее время все более активно используются туманные технологии, предполагающие обработку данных непосредственно на конечных устройствах и тем самым сократить время передачи данных.

Введение

По статистике в Казахстане зарегистрировано около 450 тыс. легковых автомобилей, что составляет примерно одну машина на четыре жителя. Эту цифру пополняют автомобили иностранных граждан, не входящие в эту статистику. Быстрый рост населения привел к увеличению транспортных проблем [1], в том числе к увеличению загазованности больших городов.

Внедрение технологий умного города требуют также повышения эффективности управления городским транспортом, в том числе решения проблемы управления парковочными местами в мегаполисе. В эпоху Интернета вещей (IoT) и экосистем умных городов умная парковка и соответствующие инновационные решения необходимы для устойчивого развития городов будущего. Проблема поиска парковочных мест сегодня является острой проблемой любого крупного города, поскольку в свою очередь порождает такие проблемы как заторы на дорогах, потеря времени, загрязнение окружающей среды, лишний расход топлива. Умная парковка с помощью датчиков, встроенных в автомобили и городскую инфраструктуру, может решить проблемы парковки и обеспечить лучшее качество жизни граждан. В данной работе мы рассмотрим существующие технологии интеллектуальных парковочных систем с учетом различных городских факторов, а также опишем состояние внедрения умных парковок в Алмате.

Существующие технологии умных парковок

Обычно водители находят место для парковки, объезжая парковочные зоны, затрачивая значительное время. Технологии умной парковки как подсистемы

умного транспорта уже получили свое развитие в мегаполисах различных стран мира [2-3].

В работе [4] приводится описание четырех основных методов поиска свободных парковочных мест: самый распространенный метод слепого поиска, обмен информацией о парковке, буферизованный обмен информацией о парковке [5] и резервирование парковочных мест. Последний метод является неотъемлемой частью умной парковки, где водители могут заранее забронировать парковочное место, а задача администрации обеспечить своевременный доступ. Безусловно, для парковок закрытого типа (off-street parking) создание умных парковок требует меньших затрат, чем для обычных уличных парковок [6]. Для уличных парковок характерно разделение районов мегаполиса на зоны значимости для водителей [7] и управление стоимостью парковочных мест в зависимости от зоны, что позволяет облегчить управление парковочными местами.

В большинстве современных исследований по умным парковкам для реализации предлагаются облачные технологии. Например, описанная в работе [3] система состоит из трех уровней: прикладной уровень, коммуникационный уровень и сенсорный уровень. Прикладной уровень обеспечивает использование облачного решения. На прикладном уровне службы парковки автомобилей, такие как служба определения парковки автомобилей, служба наблюдения за парковкой автомобилей и информационная служба, связаны с информационным центром. Информационный центр обеспечивает доступ к данным, а портал интегрированных услуг интернета вещей связан с центром управления Интернетом вещей. Управление умным городом осуществляется через портал интегрированных услуг Интернета Вещей. Второй уровень-это коммуникационный уровень, который обеспечивает связь между сенсорным уровнем и прикладным уровнем.

Опыт использования смарт паркинга в территории Казахстана

По данным Forbes [23] в Казахстане с 1 августа 2018 по 20 июля 2019 средняя загрузка парковочных мест составила 55%, каждый автомобиль в среднем проводил 28 минут на парковке, в среднем 12 автомобилей парковались с нарушением правил.

В Алмате водители воспринимают парковку как основное право, в отличие от других стран/городов, где парковка рассматривается как мощный инструмент городской мобильности. Из этого следует, что в городе наблюдается несколько отклонений в использовании парковочных мест. А именно, плохое соблюдение стандартных правил, особенно в районах с высоким спросом на парковку, несогласованное ценообразование по сравнению с зонами, оборудованными парковочными счетчиками, парковка на запрещенных местах (например, тротуарах, незаконная двойная парковка даже на главных дорогах и т. д.), что может значительно снизить пропускную способность полос движения, приводит к росту безопасности на дорогах и негативному общественному мнению.

При анализе системы управления существующими парковками в Алматы выявляется прежде всего проблема неэффективной системы управления в секторах парковки. Диагностика парковки в Алматы показывает, что правила парковок не всегда согласуются и не соответствуют реальным потребностям. Анализ также показывает, что управление парковкой в административном округе гораздо сложнее: в то время как правила парковки и цена парковки на улице, фиксированная на уровне 2MAD/час (около 0,2$/час), предназначены для поощрения водителей,

которые паркуются менее чем на 2 часа (короткий срок), 90% припаркованных автомобилей превышают это время. Это, в основном, посетители центра города (торговля и услуги) и водители, ежедневно приезжающие на работу на собственных автомобилях. Массовое присутствие этих долгосрочных парков имеет два драматических последствия для центра Алматы:

• Они несут ответственность за заторы, наблюдаемые вокруг центра Алматы, что ухудшает привлекательность города, качество воздуха и жизни/работы, а также постоянно приводит к задержкам движения городского общественного транспорта;

• Они занимают самые привлекательные парковочные места в центре города. Действительно, логика "первым пришел, первым обслужен" особенно применима в секторе парковки. Пассажиры, прибывающие первыми, занимают самые востребованные места и покидают их только ночью. В дневное время водители, прибывающие в центр города, не находят свободных парковочных мест и отправляются на расстояние, которое может превышать допустимое время ходьбы для кратковременного обслуживания. Очевидно, что эти два элемента характерны не только для Алматы, но и для большинства больших городов, поскольку эта проблема наблюдалась во многих других городах тоже. Поэтому решение проблемы путем создания информационной системы управления парковками в АлмаАты позволит:

- сократить время поиска парковочного места;
- улучшить управление распределением времени парковки путем сокращения количества парковочных мест для долгосрочных парковок в центре города, вынося их в пригородные районы;
- увеличить число мест парковки для посетителей центра города при краткосрочной парковке (как правило, менее 2 часов).

В качестве аппаратного обеспечения в Алмате чаще всего предлагается оборудование компании Libellium [22]. Датчики встраиваются в дорожное полотно на места парковок и отслеживают статус парковочного места, передавая его в базу данных. Сеть таких датчиков объединяется в карту парковок, состояние которой передается пользователям смартфонов с помощью мобильного приложения. Для применения умной парковки в городе Алматы можно рассматривать многолюдные места, в т.ч. парковки общественных парков, крупных торговых центров а также крупные организации, имеющие корпоративные парковочные места, и жилые комплексы.

В Алматы проекты умного города начали реализываться также при поддержке компании Cisco Systems. Умная парковка реализована в рамках пилотного проекта для парковки на 30 мест. Система видеоаналитики получает информацию с видеокамер Cisco и с помощью алгоритмов компьютерного зрения позволяет выявлять, анализировать и информировать водителей о наличии свободных парковочных мест. Кроме того, решение позволяет определить общее количество машин на парковках, пропускную способность, самые загруженные часы и т.п. Планируется интеграция системы умной парковки в решение Cisco для умных городов Cisco Kinetic.

Заключение

Умная парковка является одной из динамически развивающихся подсистем умного города, особенно актуальных для мегаполисов. Большинство существующих решений основано на использовании облачных технологий, однако, в настоящее время все большее внимание уделяется туманным технологиям, отличительными характеристиками которых являются близость к конечным устройствам,

географическое распределение и поддержка мобильности. Такой подход позволяет снизить нагрузку на сеть и ЦОД, уменьшает задержки в обслуживании и улучшает качество сервиса. Отметим, что в большинстве случаев пока умные парковки существуют в виде пилотных или корпоративных решений.

Литература

1. Andrej Adamuscin, Julius Golej, Miroslav Panik, The challenge for the development of Smart City Concept in Bratislava based on examples of smart cities of Vienna and Amsterdam, EAI Endorsed Trans. On Smart Cities, July, 2016, vol.1, is.1, pp.1-11.

2. W. Balzano and F. Vitale, ‘‘DiG-Park: A smart parking availability searching method using V2V/V2I and DGP-class problem,’’ in Proc. 31st Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), Mar. 2017, pp. 698–703.

3. T. Delot, S. Ilarri, S. Lecomte, and N. Cenerario, ‘‘Sharing with caution: Managing parking spaces in vehicular networks,’’ Mobile Inf. Syst., vol. 9, no. 1, pp. 69–98, 2013.

4. I. G. B. B. Nugraha and F. R. Tanamas, ``Off-street parking space allocation and reservation system using event-driven algorithm," in Proc. 6th Int. Conf. Elect. Eng. Inform. (ICEEI), Nov. 2017, pp. 1-5.

5. M. Liu, J. Naoum-Sawaya, Y. Gu, F. Lecue, and R. Shorten, ``A distributed Markovian parking assist system," IEEE Trans. Intell. Transp. Syst., vol. 20, no. 6, pp. 2230_2240, Jun. 2019.

6. Leng Y.Y, Tamil E.M, Car Park System: A Review of Smart Parking System and its Technology

7. B.Jioudi, E.Sabir, F.Moutaouakkil, H.Medromi Congestion Awareness Meets Zone-based Pricing Policies for Efficient Urban Parking, IEEE Access, vol.7, 2019, pp.161510-161523, DOI 10.1109/ACCESS.2019.2951674

8. T. Wang, J. Zhou, M. Huang, M. D. Z. A. Bhuiyan, A. Liu, W. Xu, and M. Xie, ‘‘Fog-based storage technology to fight with cyber threat,’’ Future Gener. Comput. Syst., vol. 83, pp. 208–218, Jun. 2018.

9. K. Sattar Awaisi, A.Abbas, M.Zareei, H.Ali Khattak, M.UsmanShahid Khan Towards a Fog Enabled Efficient Car Parking Architecture, iEEE Access, vol.7, 2919, pp.159100-159110.

10.L. Zhang, J. Huang, X. Li, and L. Xiong, ‘‘Vision-based parking-slot detection: A DCNN-based approach and a large-scale benchmark dataset,’’ IEEE Trans. Image Process., vol. 27, no. 11, pp. 5350–5364, Nov. 2018.

11.A. Zajam and S. Dholay, ‘‘Detecting efficient parking space using smart parking,’’ in Proc. 9th Int. Conf. Comput., Commun. Netw. Technol. (ICC- CNT), Jul. 2018, pp. 1–7.

12.H.Gupta,A.V.Dastjerdi,S.K.Ghosh,andR.Buyya,‘‘iFogSim:Atoolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments,’’ Softw., Pract. Exper., vol. 47, no. 9, pp. 1275–1296, 2017.

13.M.M. Shurmanand, M.K.Aljarah,‘‘Collaborative Execution Distributed mobile and IoT applications running at the edge,’’ in Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA), Nov. 2017, pp. 1–5.

14.E.K.Markakis,K.Karras,N.Zotos,A.Sideris,T.Moysiadis,A.Corsaro, G. Alexiou, C. Skianis, G. Mastorakis, C. X. Mavromoustakis, and E. Pallis, ‘‘EXEGESIS: Extreme edge resource harvesting for a virtualized fog environment,’’ IEEE Commun. Mag., vol. 55, no. 7, pp. 173–179, Jul. 2017.

15.S. Yi, Z. Hao, Z. Qin, and Q. Li, ‘‘Fog computing: Platform and appli-cations,’’ in Proc. 3rd IEEE Workshop Hot Topics Web Syst. Technol. (HotWeb), Nov. 2015, pp. 73–78.

16.F.T.Zohora, M.R.R.Khan,M.F.R.Bhuiyan,andA.K.Das,‘‘Enhancing the capabilities of IoT based fog and cloud infrastructures for time sensitive events,’’ in Proc. Int. Conf. Elect. Eng. Comput. Sci. (ICECOS), Aug. 2017, pp. 224–230.

17.L.F.Bittencourt, J.Diaz-Montes,R.Buyya,O.F.Rana,andM.Parashar, ‘‘Mobility-aware application scheduling in fog computing,’’ IEEE Cloud Comput., vol. 4, no. 2, pp. 26–35, Mar./Apr. 2017.

18.T.N. Pham, M.-F. Tsai, D.B. Nguyen, C.-R. Dow, D.-J. Deng A Cloud-Based Smart Parking System Based on Internet-of-Things Technologies, IEEE Access, vol. 3, 2015, pp.1581-1591.

19.K.Karthika.Sridevi,and C.Vivek,‘‘Image Processing Based Intelligent parking system,’’ in Proc. IEEE Int. Conf. Electr., Instrum. Commun. Eng. (ICEICE), Apr. 2017, pp. 1–4.

20.P. G. V. Naranjo, Z. Pooranian, M. Shojafar, M. Conti, and R. Buyya, ‘‘Focan: A fog-supported smart city network architecture for management of applications in the Internet of everything environments,’’ J. Parallel Distrib. Comput., vol. 132, pp. 274–283, Oct. 2019.

21.M. G. D. Ogás, R. Fabregat and S. Aciar, Survey of Smart Parking Systems, Applied Sciences, 2020, 10, 3872; DOI:10.3390/app10113872.

22.www.libelium.com

23.Искусственный интеллект покажет алматинцам свободное место парковки, 23/08/2019, https://forbes.kz/auto/iskusstvennyiy_intellekt_pokajet_almatintsam_svobodnoe_mesto_parkovki/

ОБМЕН ДАННЫМИ С 1С ПРЕДПРИЯТИЕМ ПРИ ПОМОЩИ ТЕХНОЛОГИИ HTTP СЕРВИСОВ

Тен В.В.
email: v.ten@aues.kz
Институт информационных технологий Алматинского университета энергетики и связи имени Гумарбека Даукеева, Алматы, Казахстан

Аннотация. *В статье представлена информация о передаче цифровых данных с 1С предприятия, ее актуальность на сегодняшний день в сфере IT-технологий, а также основные задачи и цели http сервисов.*

В настоящее время множество различных систем получают информацию с 1С предприятия. Передача данных производится, как в как в файловом варианте (txt, xml, mxl, json), так и через SOAP web-сервисы, http-сервисы или o-Data. В данной статье более подробно описано создание http-сервисов в 1С предприятии и их приимущества.

После создания 1С платформы 8.3.5 стало возможно создавать HTTP-сервисы. HTTP-сервисы имеют ряд преимуществ в отличие от SOAP web-сервисов:

1. Позволяет упростить создание клиентских приложений;
2. Уменьшить объем передаваемых данных;
3. Уменьшить вычислительную нагрузку;

Основной задачей любой интеграции является передать данные, обработать их и вернуть ответ. Вот в таком формате работает новая технология под названием HTTP -сервисы.

В дереве метаданных 1С предприятия HTTP-сервисы располагаются в ветке общие (см. рисунок 1):

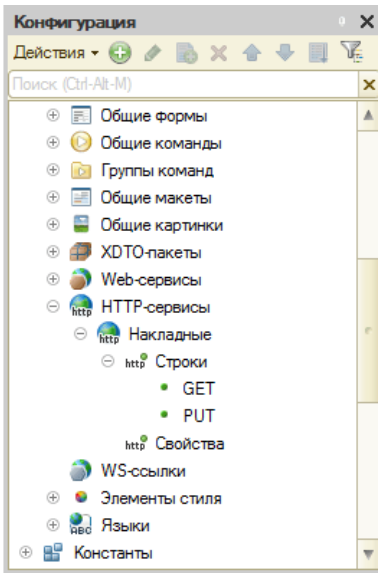


Рис. 1 HTTP-сервисы

При создании HTTP-сервиса создается URL. URL – это унифицированный указатель ресурса, система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса. Используется как стандарт записи ссылок на объекты в Интернете. URL состоит из 6 частей: *host*, *base*, *hs*, *корневойURL, относительныйURL, ПраметрыЗапроса.* В таблице 1 представлены названия и их определения.

Таблица 1. Определения URL

Название URL	**Определение**
host	IP адрес или доменное имя веб сервера.
base	Указывается имя базы при публикации 1С предприятия.
hs	Признак того, что выполняется обращение к HTTP-сервису.
корневойURL	Имя ресурса, определяющая группу ресурсов, связанных общим смыслом.
относительныйURL	Определяет ресурс, к которому будет выполняться обращение. Относительный URL, который указан в запросе, используется для определения конкретного ресурса, к которому выполнялось обращение. В объекте Шаблон URL задается правило сопоставления.
ПраметрыЗапроса	Не всегда обязательные параметры передаются после знака «?», чаще всего дополнительные параметры или параметры выборки, например формат ответа(format=json или format=atom).

Формат опубликованного HTTP-сервиса должен выглядеть следующим образом:
http://host/base/hs/корневойURL/относительныйURL?ПараметрыЗапроса

В 1С предприятии каждый HTTP-сервис содержит шаблоны от одного до несколько штук. Для каждого шаблона можно создать один или несколько методов, выполняющих обработку данных (см. рисунок 2).

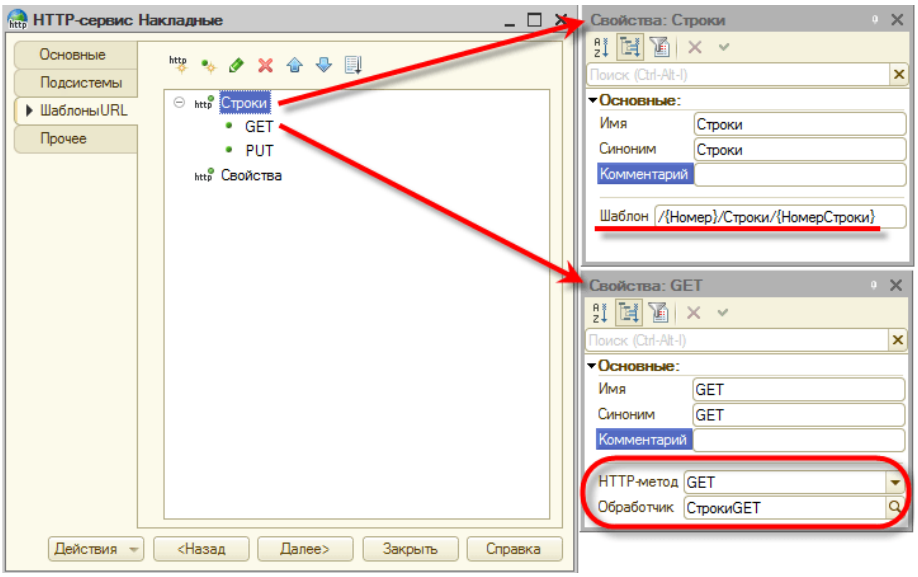


Рис.2 Шаблоны HTTP-сервиса

Для получения данных с 1С предприятия необходимо для каждого метода указать обрабатываемый HTTP метод и создать процедуру на встроенном языке программирования 1С, которая будет выполнять обработку данных. Метод состоит из двух частей:

1. Запрос, который получает данные с 1С предприятия (см. рисунок 3).

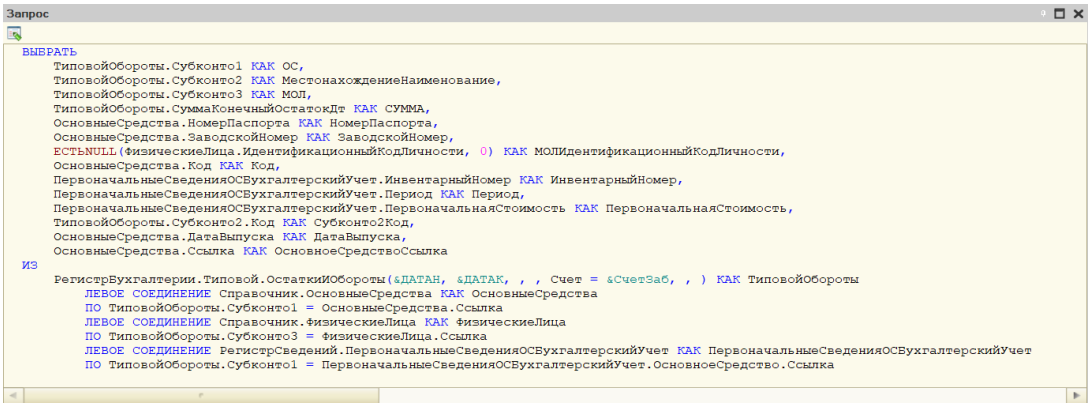


Рис. 3 Запрос HTTP-сервиса

2. Сериализация массива данных полученных из запроса в формат, который нам необходим. В данном случае в формат JSON (см. рисунок 4).

```
ЗаписьJSON = Новый ЗаписьJSON;
ЗаписьJSON.УстановитьСтроку();
ЗаписатьJSON(ЗаписьJSON, МассивКлиентов);
СтрокаДляОтвета = ЗаписьJSON.Закрыть();
//3. формируем ответ
Ответ = Новый HTTPСервисОтвет(200);
Ответ.Заголовки.Вставить("Content-type", "application/JSON;  charset=utf-8");
Ответ.УстановитьТелоИзСтроки(СтрокаДляОтвета, КодировкаТекста.UTF8, ИспользованиеByteOrderMark.НеИспользовать);
Возврат Ответ;
Ответ = Новый HTTPСервисОтвет(200);
```

Рис. 4 Код для сериализации массива данных JSON

Помимо сериализации массива данных, необходимо описать структуру передаваемых данных, согласно тому, как другая система будет их получать. Обычно описание структуры производится по каждому реквизиту отдельно (см. Рис. 5).

```
ДанныеКлиента.Вставить("id", Строка(ССылкаОС.УникальныйИдентификатор()));
ДанныеКлиента.Вставить("order_num", Строка(ВыборкаДетальныеЗаписи.ОсновноеСредствоКод));
ДанныеКлиента.Вставить("inventory_num", Строка(ВыборкаДетальныеЗаписи.ИнвентарныйНомер));
ДанныеКлиента.Вставить("name", Строка(ВыборкаДетальныеЗаписи.ОсновноеСредство));
ДанныеКлиента.Вставить("account", "2410");
ДанныеКлиента.Вставить("date_bought", (Формат(ВыборкаДетальныеЗаписи.Период,"DF=dd.MM.yyyy")));
ДанныеКлиента.Вставить("cost_aquired", Число(ВыборкаДетальныеЗаписи.ПервоначальнаяСтоимость));
ДанныеКлиента.Вставить("cost_left", Число(ВыборкаДетальныеЗаписи.ОстаточнаяСтоимость));
ДанныеКлиента.Вставить("iin_respon_person", Число(ВыборкаДетальныеЗаписи.МОЛИдентификационныйКодЛичности));
ДанныеКлиента.Вставить("fio_respon_person ", Строка(ВыборкаДетальныеЗаписи.МОЛНаименование));
ДанныеКлиента.Вставить("location_id", Строка(ВыборкаДетальныеЗаписи.МестонахождениеКод));
ДанныеКлиента.Вставить("location_string", Строка(ВыборкаДетальныеЗаписи.МестонахождениеНаименование));
ДанныеКлиента.Вставить("status","2");
ДанныеКлиента.Вставить("date_wrote_off", (Формат(ВыборкаДетальныеЗаписи.Период1,"DF=dd.MM.yyyy")));
ДанныеКлиента.Вставить("date_producted", (Формат(ВыборкаДетальныеЗаписи.ДатаВыпуска,"DF=dd.MM.yyyy")));
ДанныеКлиента.Вставить("factory_num", Строка(ВыборкаДетальныеЗаписи.ЗаводскойНомер));
ДанныеКлиента.Вставить("passport_num", Строка(ВыборкаДетальныеЗаписи.НомерПаспорта));
ДанныеКлиента.Вставить("cost_when_bought", Число(ВыборкаДетальныеЗаписи.ПервоначальнаяСтоимость));
ДанныеКлиента.Вставить("date_change", (Формат(ВыборкаДетальныеЗаписи.Период1,"DF=dd.MM.yyyy")));
```

Рис. 5 Описание структуры передаваемых данных

HTTP-сервисы обеспечивают обмен данными по протоколу HTTP. Поддерживаются два вида протокола:

1. HTTP 1.0;
2. HTTP 1.1.

Для того, чтобы передаваемые данные были зашифрованы используют протокол TLS 1.2. HTTP-соединение позволяет подключаться к веб-серверу, отправлять запросы на сервер и получать ответы. Для создания соединения необходимо предать следующие данные:

1. Порт;
2. Логин/Пароль пользователя (от которого производится соединение);
3. Адрес прокси;
4. Таймаут

Литература

1. Агапов, А.В. Обработка и обеспечение безопасности электронных данных: Учебное пособие / А.В. Агапов, Т.В. Алексеева и др. - М.: МФПУ Синергия, 2012. - 592 с.

2. Информационные технологии и вычислительные системы: Обработка информации и анализ данных. Программная инженерия. Математическое моделирование. Прикладные аспекты информатики / Под ред. С.В. Емельянова. - М.: Ленанд, 2015. - 104 с.

3. Лацис, А.О. Параллельная обработка данных, 2017. - 456 с

4. Радченко М.Г. 1С:Предприятие 8.2. Коротко о главном. Новые возможности версии 8.2

5. Гончаров Д.И., Хрусталева Е.Ю. Технологии интеграции «1С:Предприятия 8.2».

6. Радченко М.Г., Хрусталева Е.Ю. Архитектура и работа с данными «1С:Предприятия 8.2»

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ УПРАВЛЕНИЯ ПРОЦЕССАМИ БИОРЕАКТОРА

Шакерхан К.О., Мешечкин В.В.
e-mail: kapan-shakerkhan@mail.ru
Казахский гуманитарно-юридический инновационный университет, Казахстан

Аннотация. *В данной статье приводится сравнение биогазовых установок по переработке отходов различной модификации, преимущества и их недостатки, а также описание биогазовой установки собственной разработки горизонтального типа, учитывающая местные климатические и экономические условия развития фермерских хозяйств Казахстана. В статье рассмотрены применение запатентованного нами пневмороторного двигателя для перемешивания биоотходов, биореактора собственного производства и описывается анализ развития биогазовых технологий в странах дальнего и ближнего зарубежья. Проводится анализ математической модели. Рассмотрены несколько направлений математического моделирования процессов анаэробного сбраживания. Такие модели, основанные на уравнениях химических реакции, научные работы Басвелла, Мюллера, Бойля и др. Модели, основанные на эмпирических зависимостях, работы Сэфили, Вестермана. Модели, основанные на кинетических зависимостях, от концентрации субстрата и клеток, от процесса ингибирования, например работы Моно, Конто, Мозера, Чена и Хашимото.*

Ключевые слова: *биометан, биогазовая установка, биореактор, биоотходы, математическое моделирование, регрессионный анализ, корреляция*

Во многих странах к проблеме получения и использования биогаза уделяется большое внимание. За короткий срок во многих странах мира возникла целая индустрия по производству биогаза. Лидером в развитии биогазовой промышленности является Китай. С середины 70-х годов XX века в этой стране действует Национальная программа по получению биогаза из отходов животноводства. В настоящее время действует 10 миллионов фермерских метантенков. Кроме того, в Китае работает 40000 биогазовых станций, 24000 очистных сооружений, производящих биогаз, что обеспечивает работу 190 электростанций. Китай является экспортером биогаза и двигателей на его основе.

Европейская комиссия выделила биоэнергетику в самостоятельное направление общей энергетики, что было подтверждено на Всеевропейской конференции по биоэнергетике в октябре 2003 года в Будапеште.

Главными преимуществами биогаза являются его возобновляемость, наличие местных источников сырья для получения топлива, снижение парникового эффекта и экологического ущерба от систем сбора органических отходов, обеспечение экологически замкнутой энергетической системы. В таблице 1 приведены данные по производству биогаза в мире. [1, 2, 5, 9]

Таблица 1. Производство биогаза в мире

Страна	**Объем производства биогаза в год, млн. м^3**	**Суммарная мощность биоЭС на биогазе, МВт**

США	500	200
Великобритания	200	80
Франция	40	16
Россия	58	-
Казахстан (потенциальные возможности)	15	-

Из таблицы видно, что в США в настоящее время годовой объем выработки биогаза составляет 500 млн. $м^3$. Значительная часть его поступает на электростанции. Суммарная электрическая мощность установок, работающих на биогазе, составляет около 200 МВт.

В США работает более десяти крупных биогазовых заводов, один из которых (при трех откормочных комплексах на 110 тыс. голов) подает вырабатываемый биогаз в газораспределительную сеть Чикаго. Кроме этого, в США получили широкое распространение установки для использования отходов на небольших скотоводческих фермах с поголовьем крупного рогатого скота до 150 голов.

В Великобритании добывается в год около 200 млн. $м^3$ биогаза. Суммарная мощность биоЭС Великобритании составляет около 80 МВт.

Во Франции добывается в год около 40 млн. $м^3$ биогаза. На одной из свалок вблизи Парижа была построена биоТЭС, использующая биогаз, эмиссия которого составляет 1,5 тыс. $м^3$ в сутки.

Германия является лидером в производстве биогаза в Европе. Страна стремиться сократить выбросы углекислого газа на 40% и поэтапно отказывается от ядерной энергии к 2020 году. Акты правительства, в котором излагаются стратегии, о сокращение выбросов, включают национальные цели для производства биометана – 6 миллиардов кубометров газа в год до 2020 и 10 млрд. кубометров в год к 2030 году. В связи с этим ожидается дальнейшее значительное расширение немецкого производства биогаза.

Правительство Дании предоставляет значительные налоговые льготы для производителей биогаза: около 20% капитальных инвестиций для централизованного биогаза и 30% для индивидуальных станций или установок. Суммарная годовая энергетическая мощность производителей биогаза Дании, получаемого из всех источников, в настоящее время составляет до 4ПДж. Планируется дальнейшее увеличение его производства до 6ПДж. В настоящее время в Дании эксплуатируются 18 биогазовых заводов, способных ежегодно обрабатывать 1,2 млн. т биомассы (75% отходов животноводства и 25% других органических отходов), давая до 45 млн. $м^3$ биогаза, что эквивалентно 24 млн. $м^3$ природного газа. [1, 2, 3, 5, 11]

В России нет национальной программы поддержки строительства биогазовых установок, ни одного централизованного биогазового завода. Вместе с тем на внутреннем рынке имеются модели малых биогазовых установок отечественного производства, предназначенные для использования в личных подсобных и фермерских хозяйствах.

Компания «Фактор Лтд» (Москва) разработала и внедрила на Балахнинской птицефабрике (Нижегородская обл.) опытный образец биогазовой установки. При вместимости реактора 5 $м^3$ она способна перерабатывать 1 тонну помета в сутки и производить до 60 $м^3$ биогаза. В ближайшее время компания готова приступить к серийному производству биогазовых установок с реакторами вместимостью до 500 $м^3$.

АО «Центр «ЭкоРос» в 1994 г. при животноводческом комплексе КРС «Поярково», АО «Агрофирма «Искра» Солнечногорского района Московской области ввели в эксплуатацию автономный энергетический блок-модуль БИОЭН-1 по переработке отходов 20-25 голов КРС (рисунок 1). [2, 4, 18]

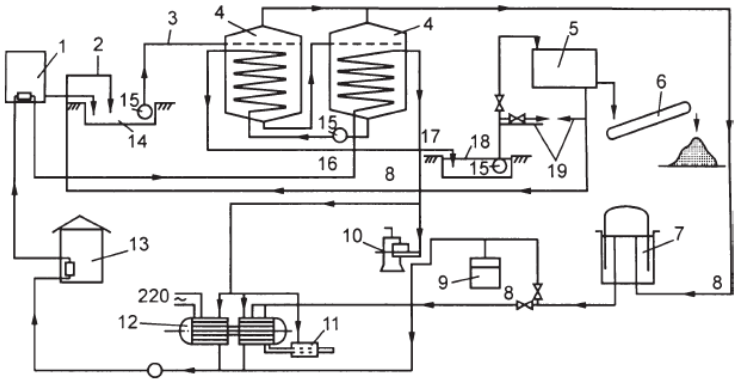


Рис. 1. Технологическая схема автономного биоэнергетического блок - модуля БИОЭН – 1: 1 – ферма; 2 – линия подачи жидкой фракции удобрений (после разделения); 3 – линия подачи сырья в биореактор; 4 – биореакторы; 5 – центрифуга; 6 – транспортер твердой фракции удобрений; 7 – газгольдер; 8 – линия подачи биогаза; 9– газовая плита; 10 – отопительный аппарат; 11 – рекуператор тепла выхлопных газов; 12 –электрогенератор; 13 – отопление помещений; 14 – емкость для хранения и подготовки сырья; 15– насосы; 16 – линия подачи горячей воды в рубашки биореакторов; 17–линия вывода охлажденной воды из биореакторов; 18–емкость для хранения жидких удобрений; 19 – линия выгрузки жидких удобрений.

В Казахстане также развивается энергетика ВИЭ, в том числе и биогазовая энергетика. 18 млн кВт/ч или 0,75% всей электроэнергии ВИЭ было выработано в 2019 году тремя биогазовыми станциями (БГС) общей мощностью 2,42 МВт, за которыми Минэнерго РК ежеквартально осуществляет мониторинг. С текущего года в этот перечень включена еще одна БГС – ТОО «Водные ресурсы-Маркетинг» с установленной мощностью 0,4 МВт на канализационных очистных сооружениях г. Шымкента. Таким образом, по данным Минэнерго, в 2020 году под мониторинг попадают 2,82 МВт биогазовых мощностей. Одна из включенных в перечень – биогазовая станция на 1 МВт, смонтированная из железнодорожных цистерн, – принадлежит карагандинскому ТОО АПК «Волынский». Сырье для ее работы – отходы свиноводческой фермы; выработанная электроэнергия поддерживает работу рыбного цеха комплекса. Биогазовая станция на 0,35 МВт ТОО «Караман-К» расположена в Костанайской области и работает на отходах животноводческой фермы КРС; выработанная электроэнергия направляется на собственные нужды. Разработкой проекта и доставкой оборудования этой станции занималось ООО «Зорг Биогаз Украина». Этот же поставщик оказал аналогичные услуги карагандинскому ТОО «Агрофирма Курма» для возведения БГС мощностью 1,07 МВт. [6, 8]

В настоящее время разработаны биогазовые установки с различными конструктивными и технологическими особенностями. Существуют

промышленные и кустарные установки. Промышленные установки отличаются от кустарных наличием механизации, систем подогрева, гомогенизации, автоматики. Типы биогазовых установок классифицируются по методам загрузки сырья, методам сбора биогаза, по используемым для их сооружения материалам, использованию дополнительных устройств, горизонтальному или вертикальному расположению реактора, подземной или наземной конструкции. Применяются двухстадийные и одностадийные биогазовые комплексы. Одностадийная технология используется для большинства субстратов и такую технологию можно считать базовой. По количеству ступеней процесса установки бывают одноступенчатыми, двухступенчатыми и многоступенчатыми. Одноступенчатые установки состоят из одного биореактора, в котором происходит полное сбраживание биомассы. В двухступенчатых системах процесс проходит в главном биореакторе брожения и в реакторе окончательного сбраживания и осаждения шлама. Многоступенчатые системы включают различное количество основных бродильных биореакторов и реакторов дображивания.

По режиму работы можно выделить непрерывные, полунепрерывные и периодические установки.

Установки периодического действия состоят из одного биореактора, который полностью загружается исходным субстратом, а затем после определенного времени процесса полностью опорожняется. В установках полунепрерывного режима процесс получения биогаза протекает в двух и более реакторах, которые работают по очереди.

При непрерывном режиме субстрат подается в биореактор непрерывно или через короткие промежутки времени, при этом соответствующий объем перебродившего субстрата удаляется. Установки, работающие в непрерывном режиме, отличаются стабильностью и высокой производительностью по сравнению с другими режимами.

По положению биореакторы бывают вертикального, горизонтального и наклонного расположения. Выбор расположения реактора зависит от режима работы и наличия свободной территории. В нашем случае мы используем биореактор горизонтального типа, полуподземного расположения с непрерывным режимом работы. Такой биореактор позволяет экономить энергию на перемешивания и сохранять тепло в холодных погодных условиях.

В биогазовых установках используют биореакторы овальной, цилиндрической и кубической формы. Наш предлагаемый биореактор представляет собой одноступенчатый, цилиндрической формы резервуар. Резервуары цилиндрической формы намного эффективнее сокращают расход энергии на перемешивание, в отличие от овального и кубического, что подтверждается большинством лабораторных исследований.

Также биогазовые установки различают по способу подвода тепла и способу перемешивания. Подвод тепла необходимого для протекания процесса может осуществляться прямым и непрямым способами. Для нашего биореактора мы используем непрямой способ. Т.к. прямой метод производится непосредственно подачей горячей воды или пара под давлением в бродильную массу. Для подогрева биомассы данным способом требуется установка парогенерирующей системы, что ведет к дополнительным затратам. Кроме того, при подаче пара или воды происходит неравномерное распределение температуры в реакторе, в результате чего происходит перегрев биомассы [10].

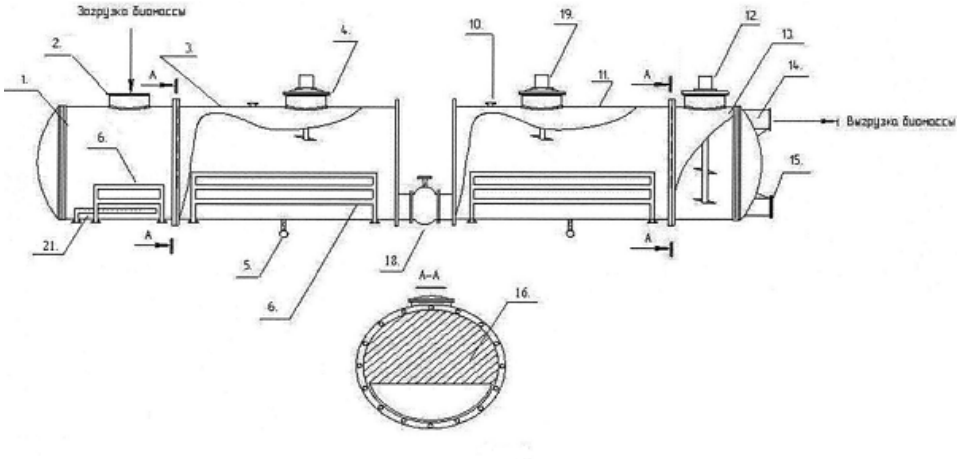


Рис. 2. Схема простейшей биогазовой горизонтальной установки

Биогазовая установка (см. рис. 2) предлагаемая нами для небольших фермерских хозяйств. Объем реактора от 16 м^3, рассчитанный на переработку 500-1000 кг навоза в сутки. Установка содержит несколько составных частей для обеспечения процесса переработки навоза и получения биоудобрений и биогаза. И работает она в мезофильном температурном режиме от 20 ºС до 35 ºС. Вырабатываемый установкой биогаз сразу направляется на использование в энергетических установках. Переработанная масса удаляется из реактора через выгрузочную трубу в момент загрузки очередной порции сырья или за счет давления биогаза. Выгружаемая сброженная масса попадает в емкость для временного хранения, которая по объему должна быть не менее объема реактора [7, 8].

Для реалии Казахстана, учитывая экономические и климатические факторы нами изобретено биореактор отечественного образца. Биореактор, выполнен трубчатой формой, расположен горизонтально и разделен на три секции: загрузочную, рабочую и выгрузочную, рабочая секция состоит из одного или нескольких модулей, в каждом модуле рабочей секции смонтированы мешалки с приводом и теплообменник, ***отличающийся тем, что*** каждый модуль снабжен поплавковым устройством, в котором монтируется мешалка с приводом с возможностью поворота относительно горизонтальной оси, причем в верхней части каждого модуля на горизонтальных направляющих установлена тележка с приводом, к которой посредством вертикальных штанг подсоединено (встроено) поплавковое устройство (см. рис. 3).

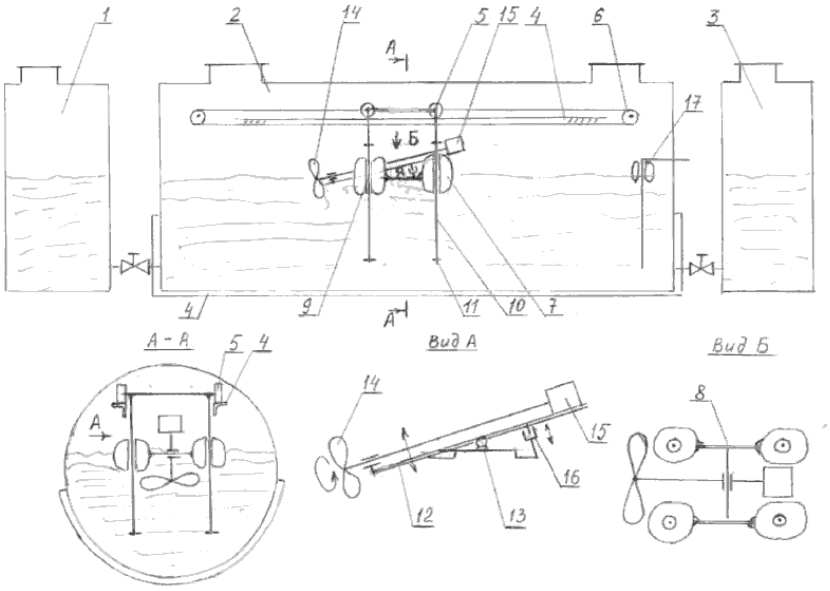


Рис. 3. Биореактор горизонтального типа с поплавковым перемешивающим устройством на пневмодвигателе, работающего на сжатом воздухе.

Технический результат достигается за счет того, что в конструкцию биореактора вводится дополнительный элемент в виде поплавкового устройства, в которое монтируется мешалка с приводом, с возможностью перемещения вдоль биореактора и поворота относительно горизонтальной оси в вертикальной плоскости [6, 7].

На рисунке 5 изображен биореактор с одним модулем:
1 - загрузочный сектор;
2 – рабочий сектор (модуль);
3 – разгрузочный сектор;
4 – теплообменная рубашка;
5 – тележка;
6 - привод тележки;
7 - поплавок;
8 – горизонтальные тяги;
9 – втулки;
10 – штанга вертикальная;
11 – ограничители;
12 – рычаг;
13 – ось рычага;
14 – мешалка;
15 – привод мешалки;
16 – гидро (пневмо) цилиндр;
17 – датчик уровня.

Биореактор состоит из трех секций: загрузочной 1, рабочей 2 и разгрузочной 3 (рисунок 5).

Рабочая секция может состоять из нескольких модулей. Модуль в нижней части имеет теплообменную рубашку 4.

В каждом модуле в ее верхней внутренней части смонтированы тележка 5 с приводом 6. Внутри каждого модуля на поверхности биомассы располагается поплавковое устройство, состоящее из поплавков 7 жестко скрепленных между собой горизонтальными тягами 8, при этом каждый поплавок 7 посредством втулок 9 подвижно встроен в вертикальную штангу 10. Вертикальные штанги 10 снабжены ограничителями 11перемещения поплавков 7 вдоль штанг.

На горизонтальных тягах 8 поплавкового устройства на рычаге 12 с осью 13 смонтирована мешалка 14 с приводом 15. Рычаг 12 снабжен гидро (пневмо) цилиндром 16. Для контроля уровня биомассы внутри каждого модуля имеется датчик уровня 17 электрически связанный с системой управления гидро (пневмо) цилиндром 16.

Перемешивание биомассы в каждом модуле происходит следующим образом.

Мешалка 14 с приводом 15, установленная на поплавковом устройстве, перемешивает биомассу по всей длине модуля, перемещаясь вдоль нее посредством тележки 5, которая может двигаться, например, с помощью трособлочного привода 6. Вертикальные штанги 10 обеспечивают устойчивое перемещение поплавкового устройства вдоль модуля. Ограничители 11 не позволяют поплавковому устройству опуститься ниже критической отметки, при которой мешалка могла бы задевать стенки модуля.

Мешалка 14 с приводом 15, проворачиваясь с помощью гидро (пневмо) цилиндра 16 относительно горизонтальной оси 13 позволяет перемешивать биомассу по всей высоте модуля.

Угол поворота рычага 12 с размещенной на ней мешалкой 14 с приводом 15 относительно горизонтальной оси 13 координируется в зависимости от уровня биомассы в рабочей секции 2 с помощью датчика уровня 17.

Таким образом, изобретение позволяет повысить качество перемешивания биомассы по всему объему модуля биореактора, сократить энергозатраты на его работу. А подземное расположение предусматривает горизонтальную конструкцию биореактора из-за очевидно меньших материальных затрат по сравнению с малой надежностью и неэффективностью маловысотной вертикальной конструкции. Кроме того, по нашим предварительным расчетам, железобетонная конструкция в условиях Казахстана оказывается в 1,5-2 раза дешевле стальной.

В результате анализа рынка биогазовых установок нами были установлено следующее: в Казахстане на сегодняшний день нет предприятий, выпускающих биогазовое оборудование (а тем более комплексы). Зарубежное оборудование очень дорогое, его не могут позволить себе купить даже относительно крупные фермерские хозяйства (около 1000 голов КРС). Например, стоимость биогазового комплекса в Костанайской области составила 400 млн. тенге, то есть более 1 млн. долларов США для фермерского хозяйства, где в наличии порядка 1000 голов к.р.с. Важно заметить, большинство поставщиков БГУ за рубежом, включая РФ, как и индивидуальные предприниматели в РК [19], широко рекламируют и продают БГУ (причём дорого, около 1300 долларов США за 1 $м^3$ биореактора), не включая в комплект такое важное и необходимое для нормального осуществления технологического процесса оборудование как измельчитель сырья. Измельчители нашей разработки [3] эффективны, практичны и недороги в сравнении с зарубежными аналогами (например, германский измельчитель средней

производительности имеет стоимость порядка 13000 евро). Также не включаются в комплект в большинстве случаев система очистки биогаза и другое оборудование. Кроме того, часто встречаются БГУ с неэффективным энергопотреблением перемешивающего устройства (до 3,4 кВт на 1 м^3 объёма биореактора). [13, 14]

На этом фоне предлагаемая разработка биореактора представляется действительно эффективной и максимально учитывающей экономические и климатические особенности региона.

Наличие оптимальной и адекватной математической модели позволяет оценить анаэробный процесс переработки отходов со всех его сторон, без проведения полномасштабных экспериментов, где соблюдаются пределы указанных и принятых ограничений. Актуальной задачей математического моделирования процесса метаногенеза является разработка универсальной модели, которая могла бы учитывать все параметры и факторы, связанные с процессом анаэробного брожения субстрата.

К настоящему времени математическое моделирование процесса анаэробного сбраживания рассматривается в нескольких направлениях.

Основой первого направления являются модели, основанные на уравнениях химических реакций. К ним относятся работы Басвелла, Мюллера, Бойля и других. Например, Басуэлл и Мюллер берут модель в качестве основы для определения количества произведенного биогаза в зависимости от исходного субстрата, а именно от химического состава:

$$C_nH_aO_b + (n - \frac{a}{4} - \frac{b}{8})H_2O \leftrightarrow \left(\frac{n}{2} - \frac{a}{8} - \frac{b}{4}\right)CO_2 + \left(\frac{n}{2} + \frac{a}{8} - \frac{b}{4}\right)CH_4 \quad (1)$$

где, $C_nH_aO_b$ - органическое вещество, H_2O - вода, CO_2 - углекислый газ, CH_4 - метан, a, b, n – безразмерные коэффициенты

Второе направление состоит из моделей, основанных на эмпирических зависимостях. В тоже время эти модели не учитывают параметры, которые влияют на конечный выход биогаза, и поэтому не раскрывают подробно процесс разложения органического вещества. Работы Сэфили и Вестермана предлагают эмпирическую зависимость выхода метана от температуры анаэробного сбраживания отходов в психофильном режиме:

$$CH_4 = 0{,}216 + 0{,}00934 * T \quad (2),$$

где CH_4 – выход метана, м^3/кг, Т – температура процесса сбраживания, ^{0}С.

Третье направление включает модели, основанные на кинетических зависимостях моделей Моно и Конто. Моно описывает процесс анаэробного разрушения ферментированного субстрата в зависимости от удельной скорости роста микроорганизмов:

$$\mu = \mu_M \frac{S}{K_s + S} \quad (3)$$

где, $\mu_м$ – максимальный удельный темп роста микроорганизмов, сут$^{-1}$; K_S – константа Моно, при которой темп роста составляет 0,5 от максимума.

На основе модели Моно Эндрюс, Мозер и другие разработали свои модели. В их работе также описывается выход биогаза в зависимости от концентрации субстрата, но с введением дополнительной функции в формулу как ингибирование у Эндрюса и с введением сигмоидального фактора в Мозер. Вышеприведенные формулы являются лишь частью, которая характеризует биологическую фазу:

$$\frac{dx_1}{dt} = \frac{F}{V}(X_0 - X_1) + \mu * X_1 - k_T * T_{x1} (4)$$

$$\frac{dS_1}{dt} = \frac{F}{V}(S_0 - S_1) - \frac{\mu}{Y_{\frac{X}{S}}} * X_1 (5)$$

$$\mu = \frac{\mu_{XX}}{1 + \frac{K_S}{HS} + \frac{HS}{K_1}} (6)$$

где X_0, X_1 – концентрация микробной популяции на входе и на выходе соответственно, кг/м^3; F,V – скорость подачи субстрата и объем субстрата в реакторе, м^3/с; μ - удельный темп роста микроорганизмов, сут$^{-1}$; k_T – коэффициент токсичности, сут$^{-1}$; T_{x1} – концентрация токсического вещества, кг/м^3; S_0, S_1 – концентрация ацетата на входе и на выходе, соответственно, кг/м^3; $Y_{x/s}$ – экономический коэффициент, характеризующий рост микробной популяции по мере потребления субстрата; HS – концентрация уксусной кислоты, кг/м^3; K_1 – константа ингибирования роста микроорганизмов уксусной кислоты, кг/м^3.

Модель Конто описывает скорость роста микроорганизмов в зависимости от концентрации субстрата и клеток бактерий. Отличительной особенностью модели Моно является учет процесса ингибирования:

$$\mu = \mu_м \frac{S}{K_S X + S} (7)$$

где X – концентрация клеток бактерий.

На основе модели Конто была разработана модель Чена и Хашимото. Чтобы определить скорость выхода биогаза в математической модели, основные параметры процесса анаэробной ферментации были введены как отдельные функции:

$$V = \frac{B_0 S}{\tau} * (1 - \frac{k}{\mu_m \tau - 1 + K}) (8)$$

где B_0 – максимальный выход метана за сутки из 1 кг органического вещества, м^3 CH_4/кг;

S – концентрация субстрата, кг/м^3; τ – продолжительность сбраживания, сут; К – кинетический параметр. Здесь параметр $\mu_м$ = 0,013 Т – 0,129.

Все приведенные выше модели учитывают выход биогаза (качество анаэробного процесса) на основе химического состава и массы исходного сырья, количества и скорости роста микроорганизмов или продолжительности ферментации. [15, 16, 17]

Также имеются предложенные модели Друзьяновой В.П., которая описывает среднюю скорость всплытия пузырьков газа из биореактора при психрофильном режиме:

Уравнение скорости всплытия биогазового пузыря

$$\vartheta_n = \frac{e^{\frac{t(\sqrt{l^2-4ac})}{b}(l-\sqrt{l^2-4ac})-l-\sqrt{l^2-4ac}}}{2a(1-e^{\frac{t(\sqrt{l^2-4ac})}{b}})} \quad (9)$$

Тем самым определяя, скорость всплытия пузырьков газа и их количества, и образующиеся осадки, можно определить мощность при спонтанном перемешивания и далее спрогнозировать объем ожидаемого биометана в ферментаторе:

Мощность спонтанного перемешивания

$$N_{сп} = m_{суб} g(\vartheta_n + \sqrt{\frac{4gd(\rho_T - \rho_{ж})}{\xi \rho_{ж}}}) \quad (10)$$

$m_{суб}$ - масса субстрата, ϑ_n - скорость всплытия пузырька, ξ - коэффициент лобового сопротивления, ρ_T - плотность твердой частицы, $\rho_{ж}$ - плотность жидкости, d – диаметр пузырька, g – ускорение свободного падения.

Существует модель Егоровой Е.Н., которая учитывает зависимость образования продукта метаболизма от скорости массообмена субстрата и скорости продуктов метаболизма, как основные факторы, интенсивно воздействующие на процесс эффективной деструкции органического навоза. Таким образом можно говорить, что выход биогаза определяется перемешиванием субстрата:

$$\nu_б = \int(N_{перем}), \quad (10) \text{ где}$$

$N_{перем}$ – мощность перемешивания в метантенке

Мощность перемешивания $N_{перем}$, по матмодели Егоровой Е.Н. необходимую на перемешивание субстрата внутри метантенка, определяется с учетом необходимого количества лопастей, крутящего момента на валу мешалки, коэффициента лобового сопротивления, плотности субстрата и т.п.:

$$N_n = (M_{кр} * \omega) * Z_л = \left(\frac{C_x \rho \omega^3 a b^4}{8}\right) * Z_л, \quad (11)$$

где

$M_{кр}$ – крутящий момент, возникающий на валу мешалки, Н*м;

C_x – коэффициент лобового сопротивления лопастей;

ρ – плотность перемешиваемой среды, кг/м^3;

ω - угловая скорость вращения мешалки, с$^{-1}$;

$Z_л$ – количество лопастей, ед;

a – высота лопасти, м;

b - высота лопасти, м.

В моделях Друзьяновой В.П. и Егоровой Е.Н. описаны обобщающие модели, полученные в лабораторных установках. В первом случае для определения выхода биогаза в зависимости от мощности биореактора при психрофильном режиме, а во втором случае в зависимости от мощности перемешивания в метантенке. Но все эти математические модели, сложно применяемые в промышленных масштабах для точного прогнозирования выхода биогаза с учетом различных параметров. [18, 19]

В нашей исследовательской работе по анализу оптимальной математической модели для более точного прогнозирования выхода биогаза при анаэробном брожении были использованы статические данные из биогазовой станции с. Курма, Карагандинской области и аналитические данные получены на примере биогазовой станции в провинции Манитоба, Канада. В предложенную нами в математическую модель, для ее широкого использования в промышленных масштабах и практического применения, использованы от 20 и до 26 различных параметров, существенно влияющих на качество анаэробного брожения, и соответственно на высокий результат выхода биогаза. Предлагается включить такие параметры в математическую модель, как показатели макро и микроэлементов (K-калий, Na-натрий, Ca-кальций, Mg-магний, Fe-железо, Cu-медь, Zn-цинк, Ni-никель, Co-кобальт, Mo-молибден, Cr-хром, Cd-кадмий), показатели C-углерода, N-азота, P-фосфор, C/N-соотношение углерода к азоту, L-концентрация питательных веществ, n-степень измельчения, VFA-содержание жирных кислот, τ-период брожения, m-масса субстрата, t-температура, pH-показатель кислотности, φ-влажность, S-сера, H_4N+ - аммоний. [20]

Из полученных стат.данных сформировали свою математическую модель с учетом предложенных параметров, оказывающих влияние на анаэробное брожение. Из всех изученных моделей для анаэробного брожения, нами предложена линейная регрессионная модель. Т.к. в ходе экспериментальных и математических исследований выяснилось, что данная модель является более практичным и эффективным при широком промышленном производстве биогаза. Выделяют несколько разновидностей регрессий: линейная, гиперболическая, множественная, логарифмически линейная, нелинейная, обратная, парная. Экспериментальные исследования показывают, что влияние различных параметров на выход биогаза имеет линейную зависимость.

Предложенная нами математическая модель представляет собой линейное дифференциальное уравнение эмпирических соотношений каждого параметра, полученное путем регрессионного анализа. Модель линейной регрессии имеет следующий вид (см. формула 12):

$$y = a_0+a_1x_1+a_2x_2+\dots a_nx_n \quad (12)$$

В данном уравнении:

- *Y* – переменная, влияние на которую нужно найти;
- X – факторы, влияющие на переменную;
- A – коэффициенты регрессии, определяющие значимости факторов;
- N – общее количество факторов.

Литература

1. Barbara Edery, Heinz Schultz. Biogas plants. Practical guide. Pages 1996 - 268. http://libed.ru/knigi-nauka/350087-1-barbara-eder-haync-shulc-biogazovie-ustanovki-prakticheskoe-posobie-osnovi-planirovaniya-stroitelnie-raboti-t.php

2. Vedenev A. G., Vedeneva T. A.-B.: A guide to biogas technologies. - "ДЭМИ", 2011 - 84 p. http://www.fluid-biogas.com/wp-content/uploads/2020/03/Rukovodstvo-biogas_2017.pdf

3. Iskakov S. K. Mobile biogas plant. // Энергосовет – 2015. – №4 – С. http://www.energosovet.ru/bul_stat.php?idd=551

4. Biomass as a renewable energy source. https://esa-conference.ru/wp-content/uploads/files/pdf/Kozlov-YUrij-Pavlovich.pdf

5. Development of an industrial-scale bioreactor in the context of a global pandemic. Shakerkhan K. O.Meshechkin V. V.Sagindykov K. M.Konyrkhanova A. A.Abilmazhinov E. T. IOP Conference Series: Earth and Environmental Science (2021). DOI:10.1088/1755-1315/723/4/042034

6. Prospects of biogas production in Kazakhstan. https://cyberleninka.ru/article/n/perspektivy-proizvodstva-biogaza-v-kazahstane/viewer

7. Биогазовая установка https://kazpatent.kz/images/bulleten/2018/gazette/ru201819/html/b0025684.htm

8. Казахстанская биогазовая энергетика. https://eenergy.media/2020/03/11/kak-razvivaetsya-kazahstanskaya-biogazovaya-energetika/

9. Китайская система стимулирования биогазовой энергетики. https://agroserver.ru/articles/1831.htm

10. Классификация биогазовых установок по конструктивным и технологическим признакам. https://cyberleninka.ru/article/n/klassifikatsiya-biogazovyh-ustanovok-po-konstruktivnym-i-tehnologicheskim-priznakam/viewer

11. Energetic and economic analysis of biogas plant with using the dairy industry waste. Kozłowski K.Pietrzykowski M.Czekała W.Dach J.Kowalczyk-Juśko A.Jóźwiakowski K.Brzoski M.Energy (2019). DOI: 10.1016/j.energy.2019.06.179

12. A Hybrid Method for the Development of Mathematical Models of a Chemical Engineering System in Ambiguous Conditions. B.B. Orazbayev, E.A. Ospanov, K.N., Orazbayeva, L.T.Kurmangazieva //Mathematical Models and Computer Simulations. Moscow, Russia. 2018 – Vol.10, Issue 6. – pp. 748-758 DOI: 10.1134/S2070048219010125

13. Analysis of heat loss of a biogas anaerobic digester in weather conditions in poland. Teleszewski T. J.Z˙ukowski M. Journal of Ecological Engineering (2018). DOI: 10.12911/22998993/89660

14. Digitalization and innovative development of mining processes. Stenin D.Stenina N.Akanov A.Sagindikov K. E3S Web of Conferences (2019). DOI: 10.1051/e3sconf/201910503012

15. Mathematical modeling and decision-making on controlling modes of technological objects in the fuzzy environment. B.B.Orazbayev., Y.A. Ospanov, K.N.Orazbayeva, N.S Mukataev, A.I. Demyanenko // Proceedings of the 12th World Congress on Intelligent Control and Automation. (WCICA) Guilin, China. 2016. – pp.103-109 DOI: 10.1109/WCICA.2016.7578783

16. Control of Fuzzy Technological Objects Based on Mathematical Model. B.B. Orazbayev, Y.A. Ospanov, K.N. Orazbayeva, T. Gancarzyk, A. Shaikhanova // 16th International Conference on Control, Automation and Systems (ICCAS 2016). – Gyengju, Korea, 18–19 October 2016. –P. 1487–1493. DOI: 10.1109/ICCAS.2016.7832501

17. Review of the mathematical description of the process of methanogenesis in a bioreactor. M.B. Tlebaev, N.K. Kalinchun, D.U. Mamataeva. International scientific journal (ISSN 2072-0297) № 4.1(138.1)/2017. http://www.rusnauka.com/pdf/246610.pdf

18. Energy-saving technology for processing cattle manure. Dissertation work / Ulan-Ude / 2016, V.P. Druzyanova. https://www.esstu.ru/uportal/dissertation/downloadFile.htm?type=dissertation&typeId=499

19. Substantiation of the parameters of a small-volume digester with a stirring device for the conditions of the Republic of Sakha (Yakutia). Dissertation work / Blagoveshchensk / 2017, E.N. Egorova. https://www.dissercat.com/content/obosnovanie-parametrov-metantenka-malogo-obema-s-peremeshivayushchim-ustroistvom-dlya-uslovi

20. Parameters of the distributed databases of information systems when splitting data with application of algorithms of multidimensional parity. Karipzhanova A. Z.Sagindykov K. M.Gudov A. M.Dimitrov K. News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences (2019). DOI:10.32014/2019.2518-170X.128

CLASSIFICATION OF LMS CONTROL AND MONITORING SERVICES

Yevgeniy Fedkin, Saule Smailova, Vitaly Zuev, Saule Kumargazhanova, Natalia Denissova, Elvira Aitmukhanbetova*

D. Serikbayev East Kazakhstan technical university, Astana IT University
The Republic of Kazakhstan*

Abstract

In the article, the authors produced an analytical review of existing LMS and proposed a classification of monitoring and control services based on the criterion of the level of coverage of users and elements. A reference model is proposed, which includes 6 levels of services, which are grouped into 3 groups: firmware services (software and hardware levels), basic services (user level and content level), and management and analysis services (administrative and analytical levels). The authors also proposed an approach for clustering services using semantic similarity on the example of LMS VKTU. An algorithm of calculating the semantic similarity of services based on the processes in which they participate and the entities with which they interact was used, was used for clustering. Based on the obtained estimates of semantic similarity, the clustering of services was performed using the FOREL algorithm with different radii.

1 Analysis of the global e-learning systems

The use of modern information and communication technologies as a means of teaching schoolchildren and students has become a popular trend. It uses a special type of web-based content management systems called Learning Management Systems (LMS). Various types of systems have been introduced on the market today, which often provide similar functions, making it difficult for the user to choose. There are many methodologies for assessing the quality of e-learning in the scientific literature.

Some of current LMS systems are cloud-based and do not require a system administrator with experience in installing and maintaining software; however, there are also systems in which deep knowledge of programming languages such as PHP, JavaScript, knowledge of database management and administration, such as MySQL, Microsoft SQL Server are absolutely necessary.

Over the past few years, the most interesting approach to software development has been based on user preference and experience, the so-called user-centered design [1], [2]. This method is gaining more and more popularity among software developers, including those designed for training [3].

Recently, a new type of e-learning system has appeared, based on automatic recognition and prediction of user preferences, and self-adaptation to user requirements. This type of system is called learning management adaptive. Some researchers base learning on the use of social networks and communication between learners (students) and learners (teachers) [4] - [6].

For a comparative analysis of LMS platforms, it is necessary to determine the main characteristics for evaluating such systems (table 1) in three areas or sections.

The "Learning Tools" section includes e-learning functions that provide interaction between students and the teacher, as well as tools for self-study of the material.

The "Support Tools" section brings together platform resources intended for the development and administration of developed courses.

A set of technical requirements, the fulfillment of which is necessary for the correct and full-fledged operation of the e-learning system, is presented in the "Technical Specifications" section.

1 Table - Criteria for evaluating LMS platforms

Learning tools	Communication tools	Productivity support
- SCORM compliant - Lectures in the form of web pages, documents, presentations, video, etc. - Examples and tasks such as web pages, documents, presentations, videos, etc. - Assignments and exercises in the form of web pages, documents, quizzes - Gamification - Assessment	- Chat - Forum - Email	- Upload / download various types of documents - Add, edit, delete data for students - Analysis of the achievements and results of students - Cross-platform - Security and protection of user data - Creation of a backup data copy - Need for a system administrator able to manage user roles in LMS - Web technology software development - Necessity of installation - Self-registration

According to the latest data, several hundred paid and free e-learning platforms have been developed in the world, among which the most popular are: Blackboard, Moodle, Sakai, Canvas, Open EdX, Yo-Studi, Dokeos, ATutor, LAMS, Claroline, OLAT, iSpring Online, OpenACS, TalentLMS, Inkling, Versal, WebTutor, and others.

- 36 LMS frameworks were selected for analysis. Based on the analysis performed, the following conclusions can be drawn:

- very few of the studied LMS systems are open source, such as ATutor, Chamilo, Sakai, Open edX. Some systems provide free versions of the software as well as paid versions. Almost all studied LMS platforms meet the requirements described in SCORM (Sharable Content Object Reference Model), except for Cornerstone OnDemand, Edmodo SkillSoft, Thinkific, WorkWize.

- Most modern LMS systems provide multilingual interface support, making it easier for users to use their native language. For example, only 28% of the LMS platforms studied support up to 10 different languages, and the remaining 72% of them support more than 10 languages. Only 3 platforms, namely Tortal Training LMS, iSpringLearn, and BizLibrary only support the English language interface.

Analysis confirms that 89% of platforms are SCORM compliant. Despite the variety of social networks and instant messaging applications, only 47% of the analyzed systems provide a chat facility, and 69% of them support a forum. Unless there is a change in future LMS systems, it is possible that the influence of social networks in education will increase, leading to the creation of social network learning management systems. Another problem is data backup. For example, cloud LMS users are unlikely to be able to automate the backup process.

In modern systems, there is the widespread use of web technologies to develop new platforms. Some systems offer support for self-registration and the creation of new user profiles. Consequently, more people can have equal access to education.

Thus, the main trends of modern LMS platforms can be summarized as follows:

- providing cross-platform support;
- asynchronous work;
- multilingual interface support;
- support of user self-registration - the user can create an account without a prior request to the administrator;
- improved gamification;
- improved communication between users, for example, the exchange of text and multimedia information, as well as approaching modern LMS systems to the concept of social networks;
- leveraging cloud technology to build LMS platforms, reducing the need for specialized hardware such as web servers, web addresses, and network administrators to support them;
- the ability to easily create and manage lectures, exercises, and assignments and facilitate the solution of these problems by students using interactive management models.

Despite the variety of LMS platforms, no one off-the-shelf solution fully covers all user requirements. This article proposes an approach to defining LMS functionality by comparing the classification of monitoring and control services based on the proposed LMS reference model.

2. Classification of LMS monitoring and control services

When working in LMS, different categories of users perform various actions in the system, which are recorded in the activity log, and generate various artifacts (files, records in the database, etc.).

To regulate and analyze user activity and artifacts that they create in the LMS, generally, various monitoring and control services are used. These services can cover various aspects of the system operation in different viewpoints.

Monitoring and control services can be classified based on various criteria; in this study, the level of reaching users and LMS elements will be used as a criterion for classifying services.

Based on this criterion for the classification of monitoring and control services, the following categories of services can be distinguished:

1) Services for monitoring and controlling users. These services are aimed at assessing the activity of users in the system according to various criteria: assessment of the performance of a separate task, assessment of activity in a separate course, overall student activity in the system, teacher activity in a separate course, and the system in general, the teacher's work with students, the correctness of the course shaping, holding various forms of control of students and, assessing an overall grade for passing the course based on them, etc.

2) Services for monitoring and controlling the content. These services are focused on tracking and controlling the correctness of the methodological support of courses in LMS based on the requirements that are set for various types of courses. Evaluation of methodological support can be conducted both in automatic mode (for example, the availability of certain types of resources and tasks on the course), and in manual mode (methodical evaluation of the course by experts).

3) Services of operational management and administration. This category of services is focused on the operational management based on various criteria: the presence of courses in the system, student registration for courses, the filling of courses with various resources and tasks, identification of problems; monitoring and controlling the LMS hardware and software, which allows you to monitor and respond to problems that may occur in hardware or software. Consistently, these services are implemented as a separate system for collecting and analyzing information coming from various hardware and software components operating in the network.

4) Analytical processing services. These services are focused on the analytical processing of information received from the LMS and the construction of various analytical reports and recommendations. These services and the services of administrative monitoring and control, are implemented in separate systems since they require special software to calculate and build analytical models.

Based on the dedicated services and for the implementation of all user requirements, the authors propose a reference model for control and monitoring services.

3. Reference model

The reference model presented in Figure 1 is divided into blocks: software and hardware services; basic services; management and analysis services.

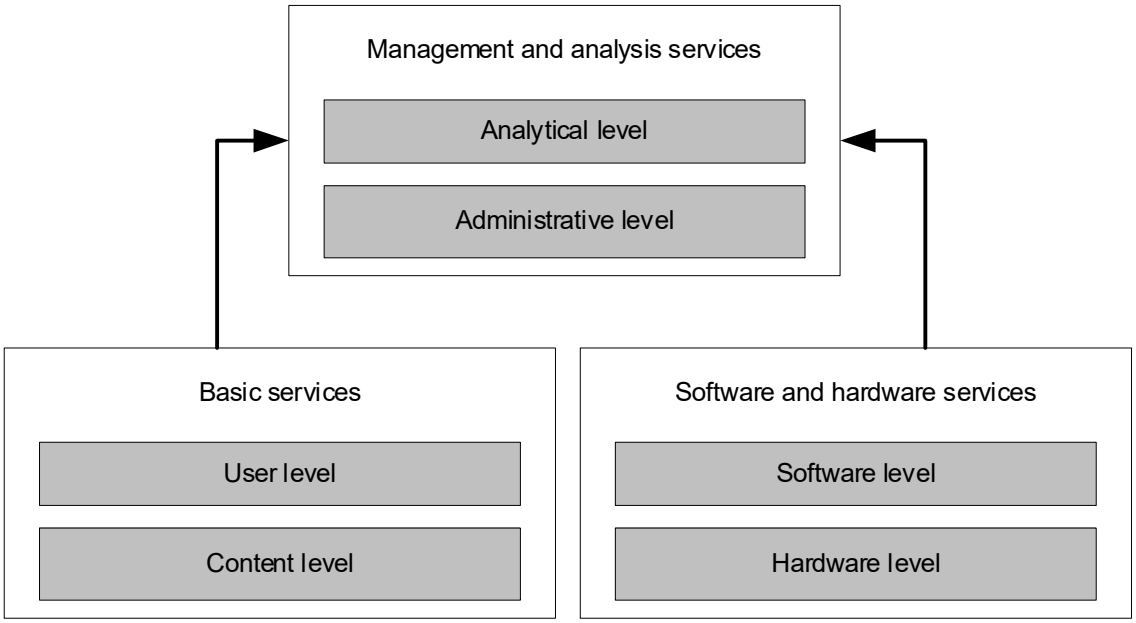


Figure 1 - Reference model for monitoring and control services

Software and hardware services. These services are aimed at monitoring and controlling LMS software and hardware. These services are divided into:

A) Hardware level - at this level, various services control the hardware that is involved in the operation of the system (network equipment, server equipment, etc.)

B) Software level - at this level, services monitor the operation of the LMS software (Application Servers, Web Services, Database Management Systems).

Basic services. These monitoring and control services are associated with the main function of the LMS system - training. These services are divided into:

A) Content level - this level includes services focused on controlling the content of educational materials in the system, conducting control activities, etc.

B) User level - this level includes services aimed at logging user activity in the system, collecting artifacts generated by users when working in the system, etc.

Management and analysis services. These services are intended for general system control and analysis based on the data recorded in the software, hardware and basic services. These services are divided into:

A) Administrative level - this level includes services for the operational management of the educational process in the LMS.

B) Analytical level - this level includes services for conducting analytical research based on data collected as part of the system's functioning.

VKTU successfully implements its own developed LMS. Analysis of the existing LMS VKTU software modules, depending on the proposed classification of services, will make it possible to upgrade the system, which will make it possible to increase the efficiency of the VKTU LMS during the pandemic.

In the presented reference model in this article, we will consider in detail the basic services and services of management and analysis, since these services provide the basic functionality of the LMS associated with its main goal - to ensure the educational process.

LMS operates in a certain software and hardware environment; thus, the software and hardware services allow monitoring and control of the effectiveness of using this environment when using the system. The software and hardware environments within which it is possible to support LMS operations can have various configurations; as a result, the list of monitoring and control tools is determined by the configuration in which it operates. In addition, in this environment, other systems that are required to ensure the operation of the university; therefore, these parts will not be considered extensively in this article.

4. Analysis of existing software modules LMS VKTU, depending on the proposed classification of services

LMS VKTU has the following monitoring and control software modules:

1) Academic performance - data on student performance is available. The report is equipped with filters by semester, a search system by discipline, by group, by the student's full name;

2) Ungraded papers and appeals - generating a report on ungraded papers and submitted test appeals;

3) Schedule of assignments - downloading graded assignments and distance course tests;

4) Control of students and faculty following the schedule of classes, storage of information about the educational process over extended time;

5) Active tests - contains data on students with active unfinished tests;

6) Export of progress - export of students' progress by control points to the database of the educational portal;

7) Flexibility of setting up the assessment system of students' papers - allows you to customize the assessment of test items by the training system;

8) Proctoring - allows you to verify (confirm) the identity of the test taker, and to observe his/her behavior and what is happening on his/her computer screen to make sure

that students are not cheating, does not use the help of other people, does not look up for answers over the Internet;

9) Group management - combining several groups by discipline for one course;

10) Testing - loading tests for automatic control of students; management of the educational process: traditional, distance;

11) Teachers - generating a report that allows you to view the activity of teachers in the online learning system. It is equipped with filters by semester, and teaching staff inactivity by day, by the teacher's full name;

12) Student activity - the history of student visits allows you to see a log of user activity;

13) Test tasks - generating a report on uploaded tests for courses, equipped with filters by semester, only distance - generating a report by groups of students;

14) Courses by type – creating a report by quantitative indicators on the uploaded resources per course in the context of a semester, the form of study, school, department

15) All courses - creating a report with data on all courses on filling the course content by the parameters of technical expertise, equipped with filters in the context of a semester, schools, departments and a search system by discipline, teacher, group;

16) Service for technical and methodological expertise - methodological expertise of the course content and technical expertise in the quantitative indicators of the course resources;

17) Course progress - viewing the progress of students in the group;

18) File storage - a file exchange service that provides the user of the distance learning system with a space for his/her files and 24-hour access to them;

19) Video greeting - allows you to upload a video greeting of the teacher with brief information about the course, requirements in any video format;

20) Course Forum - allows you to discuss course topics offline;

21) Chat - allows you to discuss course topics online;

22) Private messages - allows you to receive and receive messages from users;

23) Tasks - allows you to download a task for two-way communication;

24) User activity - based on the data of the log of user actions in the LMS, a diagram of activity in the E-Monitoring system is built, analytical diagrams are formed according to the activity of various categories of users in the LMS;

25) Final examination - Qualitative analysis - Creation of an analytical diagram based on the results of final examination in the E-Monitoring system;

26) Final examination - Progress - Creation of an analytical diagram on the progress of students in the context of courses in the E-Monitoring system;

27) Final examination – Failed examination - Creation of an analytical chart on the failed examination of students in the E-Monitoring system;

28) Video stream - allows you to conduct video conferencing;

29) Virtual whiteboards - a tool that allows you to visualize educational material.

The classification of described monitoring and control services of the LMS VKTU is shown in Figure 2.

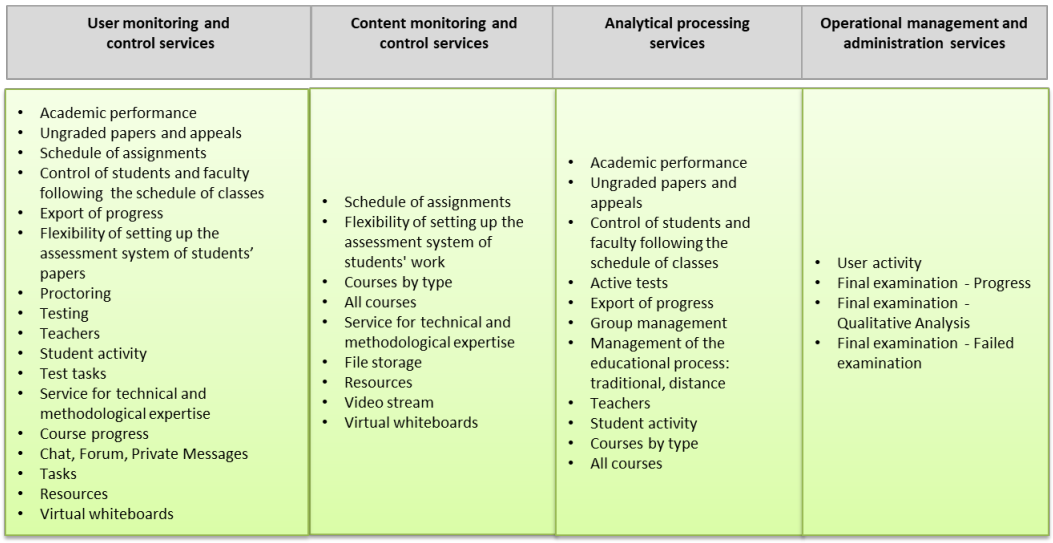


Figure 2 - Service groups. The existing set of LMS VKTU services

Based on the conducted research and the experience of the LMS VKTU, the authors identified the following elements that are required for the implementation of the LMS presented in Table 2.

The overall scheme of the monitoring and control services of the LMS VKTU, containing the proposed extended set of services, is shown on the Figure 3. The blocks implemented in the VKTU are marked in green, and the blocks containing the missing functions of the system are noted in red.

2 Table - Proposed changes for LMS

№	Proposed changes for LMS
1	Assignment of students to individual teachers to conduct contact classes, to check and to evaluate the work performed
2	Updating the content of tasks with saving the history of changes
3	Management of individual assignments on the course in automatic (assignments are assigned randomly from possible options) and manual (assignments are assigned by the teacher separately for each student) modes (for example, assignment or topic for a course work or project).
4	Implementation of the mobile version of the system with the maximum possible system functionality for mobile devices
5	Design and implementation of mechanisms for integration with external systems
6	Implementation of interaction with external systems for conducting contact classes (Zoom, BBB, etc.), as well as collecting data for analyzing the conduct of such classes
7	Development and implementation of mechanisms for notifying system users about new events (e-mail, push notifications, SMS, etc.)
8	Implementation of control over the sequence of task execution on the course according to the conditions (for example, some task is performed only after completing another task and / or tasks and / or after viewing the resource on the course)

9	Implementation of built-in playback of video and audio materials on the course in online (video broadcast) and offline (resources on the course) mode
10	Support working with a virtual whiteboard in online mode
11	Possibility of displaying individual resources on the course in automatic (according to specified conditions, for example, if a student received an assessment on a task below a certain level) and in manual (opened by the teacher to individual students) modes

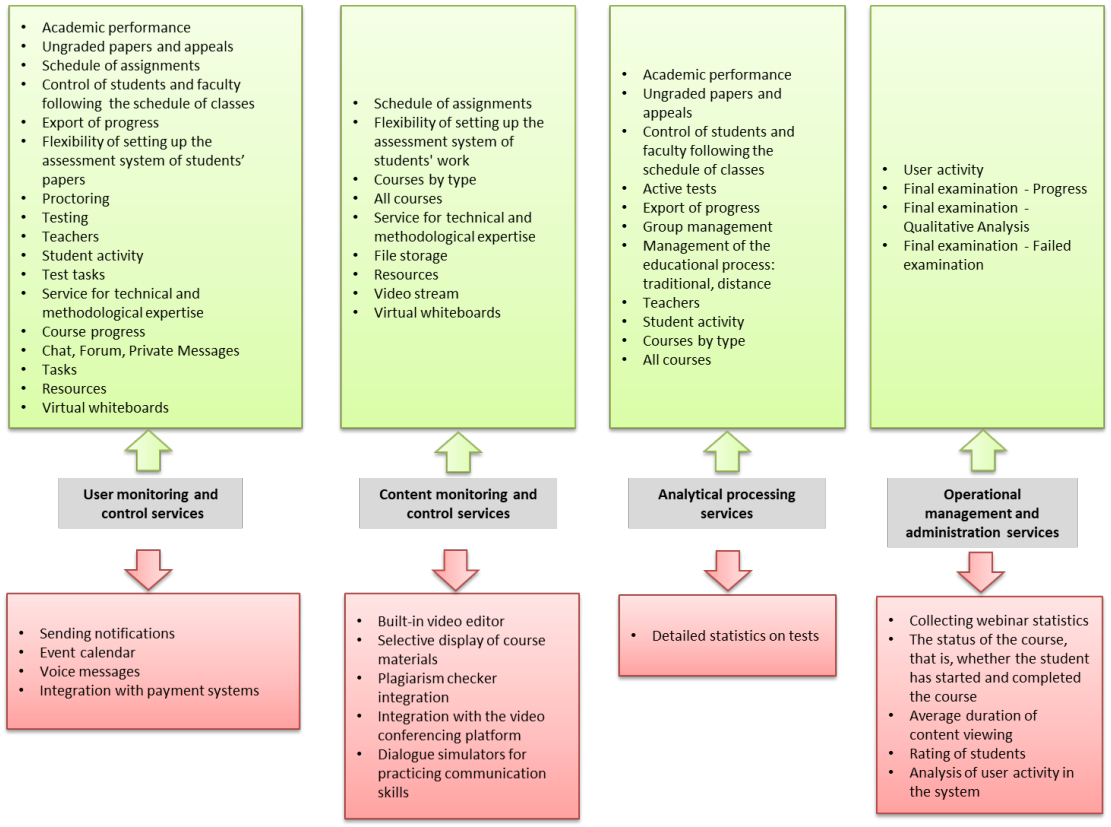


Figure 3 - Service groups

VKTU uses the hybrid architecture: the monolithic architecture of the system is supplemented with a set of functions for integration, both in the local and in the cloud environment, which allows the use of elements of microservice architecture. Consequently, the modernization of the LMS VKTU to the proposed model is possible. The proposed services will be implemented: as part of the system, as separate services, third-party integrated into the LMS, third-party cloud services, which will allow organizing a better system operation and expanding the capabilities of the LMS.

Next, we will analyze the correspondence between the set of services LMS VKTU, which we described in this section, and the reference model of services presented in the

previous section. The result of this analysis is shown on the diagram shown in Figure 4. Consider this diagram in more detail:

1) Firmware services. The VKTU has its server platform, in which various information systems of the university operate. This server site is maintained by a special subdivision that provides resources for the LMS. To ensure effective functioning of LMS in a network environment, this service uses various special software and hardware tools and, as we indicated in the previous section, these tools are specific to some configurations.

2) Basic services. In LMS VKTU, following the requirements of the reference modules, these services are represented by services for monitoring and controlling users (user level) and content (content level)

3) Management and analysis services. These services in the LMS are represented by services of operational management and administration (administrative level) and analytical processing (analytical level).

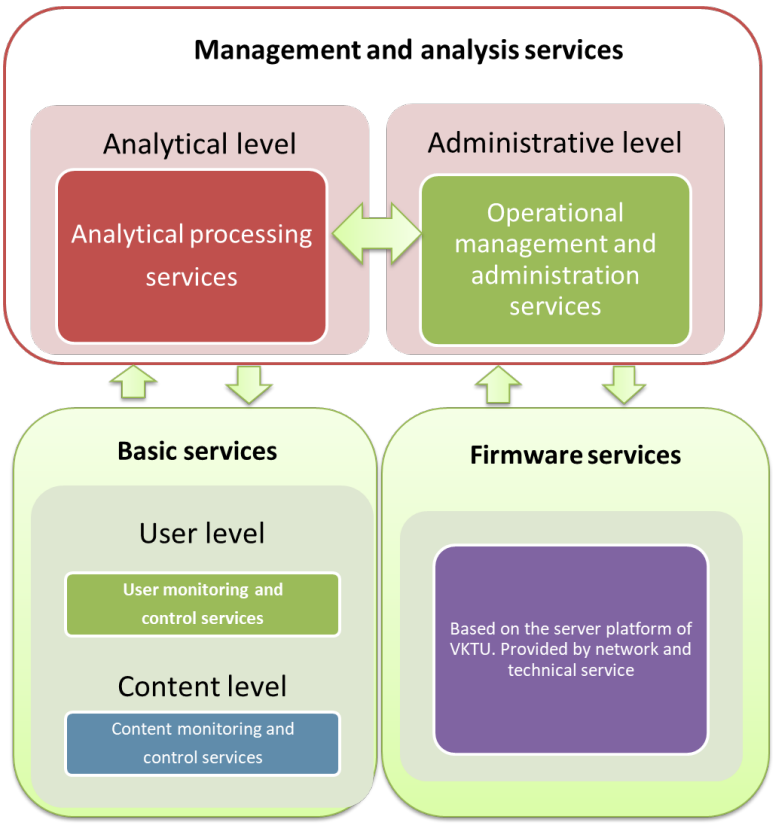


Figure 4 - Scheme of compliance of the reference model with the monitoring and control services LMS VKTU

Based on our analysis of the compliance of the reference model with the available monitoring and control services and proposed modernization in the LMS VKTU, we can conclude that the LMS is fully consistent with the reference model, which enables effective functioning of the system to implement its main function - to ensure the educational process.

5. Clustering monitoring and control services

At the final stage of this study, we will cluster the monitoring and control services based on their semantic proximity.

Semantic proximity of two services is determined by the following formula 1 [7]:

$$SI(f_x, f_y) = \sum_{i=1}^{n} w_i SI_i \quad (1)$$

where, SI^i – a measure of the i-connection between services,

w_i – the weighting factor for the i-link (for weighting factors in the formula, the condition $\sum w_i = 1$ must be satisfied).

The measures of links between services and the weights for them, which have been determined by an expert, for the analysis will be as follows:

1) SI_{BP} – the ratio of the cardinal set of processes using both services to the cardinal number of the set of processes using at least one service. The weighting factor for this measure is 0.5.

2) SI_{ER} – is the ratio of the cardinal set of entities that are read in both services to the cardinal number of the set of services that are read by at least one of the services. The weighting factor for this measure is 0.27.

3) SI_{EW} – is the ratio of the cardinal set of entities that change in both services to the cardinal number of the set of services that change the entity at least by one of the services. The weighting factor for this measure is 0.23.

To cluster LMS VKTU services, the following initial data are used:

1) Services: Progress (F1), Ungraded papers and appeals(F2), Schedule of assignments (F3), Monitoring of students and faculty following the schedule of classes (F4), Active tests (F5), Export of progress (F6), Flexibility settings of the assessment system of students' work (F7), Proctoring (F8), Group management (F9), Testing (F10), Teachers (F11), Student activity (F12), Test tasks (F13), Courses by type (F14), All courses (F15), Technical and methodological examination service (F16), Course progress (F17), File storage (F18), Video greeting (F19), Course forum (F20), Chat (F21), Private messages (F22) , Tasks (F23), User Activity (F24), Final examination - Qualitative Analysis (F25), Final examination - Academic Performance (F26), Final examination – Failed examination (F27), Video Stream (F28). Virtual whiteboards (F29).

2) Entities: Student (S1), Teacher (S2), Content (S3), Progress (S4), User Activity (S5)

3) Processes: Formation of course content (P1), Evaluation of course content (P2), Learning process (P3), Knowledge assessment (P4), Analysis of system performance (P5).

Next, it’s required to determine the use of services in processes, and requests of services to entities to read data from them and change their data. For convenience, we will summarize this information in Table 3. The rows will contain services, in the columns the use of their processes, reading and writing data in entities, and in the cells, there will be 1 if there is a use of the service.

3 Table - Using services in processes, reading and writing entity data

Service	Processes	Reading entities	Altering entities

	P1	P2	P3	P4	P5	S1	S2	S3	S4	S5	S1	S2	S3	S4	S5
F1			1	1	1	1			1					1	
F2			1	1		1	1	1	1	1					
F3	1	1	1				1	1							
F4					1	1	1	1	1	1					
F5			1	1	1	1	1		1	1					
F6				1		1			1					1	
F7	1							1					1		
F8			1			1									1
F9			1			1	1	1					1		
F10	1			1		1	1	1	1	1				1	1
F11			1		1		1			1					
F12			1		1	1				1					
F13	1					1	1	1							
F14	1	1					1	1							
F15	1	1					1	1							
F16		1			1			1							
F17			1	1		1			1						
F18	1					1	1						1		
F19	1					1							1		
F20			1	1		1	1	1	1	1			1	1	1
F21			1	1		1	1	1	1	1			1	1	1
F22			1			1	1				1	1			
F23	1	1						1	1	1			1	1	1
F24				1	1	1	1	1	1	1					
F25				1		1			1						
F26				1		1			1						
F27				1		1			1						
F28	1		1			1	1								1
F29			1			1	1								1

Based on the data given in Table 3 and according to Formula 1, the adjacency of functions was calculated and a matrix of services adjacency was compiled (Table 4).

Based on the obtained adjacency matrix, FOREL clustering is created with radii of 0.76 and 0.5, since the number of possible clusters is not known in advance.

4 Table - Service adjacency matrix

Part 1															
	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	F14	F15
F1	1.00	0.73	0.40	0.56	0.93	0.44	0.00	0.30	0.26	0.33	0.70	0.83	0.32	0.23	0.23
F2	0.67	1.00	0.50	0.50	0.78	0.36	0.05	0.30	0.41	0.52	0.59	0.59	0.39	0.34	0.34

F3	0.40	0.50	1.00	0.34	0.46	0.00	0.30	0.17	0.35	0.27	0.53	0.40	0.58	0.83	0.83
…															
F28	0.30	0.36	0.47	0.11	0.30	0.14	0.25	0.62	0.43	0.47	0.39	0.39	0.43	0.39	0.39
F29	0.30	0.36	0.30	0.11	0.30	0.14	0.00	0.87	0.68	0.22	0.39	0.39	0.18	0.14	0.14

Part 2

	F16	F17	F18	F19	F20	F21	F22	F23	F24	F25	F26	F27	F28	F29	
F1	0.40	0.83	0.14	0.14	0.50	0.50	0.30	0.18	0.73	0.50	0.67	0.67	0.30	0.30	
F2	0.28	0.84	0.11	0.05	0.77	0.77	0.36	0.16	0.75	0.34	0.59	0.59	0.36	0.36	
F3	0.53	0.40	0.30	0.17	0.27	0.27	0.30	0.42	0.34	0.23	0.23	0.23	0.47	0.30	
…															
F28	0.00	0.39	0.52	0.39	0.43	0.43	0.52	0.33	0.11	0.14	0.14	0.14	1.00	0.75	
F29	0.00	0.39	0.27	0.14	0.43	0.43	0.77	0.08	0.11	0.14	0.14	0.14	0.75	1.00	

As a result of clustering for a search radius of 0.62, the following result is obtained:

Cluster 1: {F1, F2, F5, F6, F8, F9, F10, F17, F20, F21, F23, F28, F29}. This cluster includes 13 services - 10 user-level services and 5 analytical-level services. This cluster of services, as can be seen from the distribution, is focused on the user level of the reference model, since this group includes services related to the registration and analysis of user activity.

Cluster 2: {F3, F4, F11, F12, F16, F22, F24}. This cluster includes 7 services - 6 user-level services, 3 content-level services, 3 analytical-level services and 1 administrative-level service. This group of services is mainly aimed at analyzing the operation of the LMS and corresponds to the analytical level of the reference model.

Cluster 3: {F7, F13, F14, F15, F18, F19}. This cluster includes 6 services - 2 user-level services, 5 content-level services and 3 analytical-level services. This group of services is mainly focused on the assessment of the LMS content and corresponds to the content level of the reference model.

Cluster 4: {F25, F26, F27}. This cluster includes 3 services from the administrative level. Based on the distribution, this group corresponds to the administrative level of the reference model.

As can be seen from the analysis based on clustering, the resulting distribution of services corresponds to the proposed reference model of LMS monitoring and control services. In addition, the proposed clustering model can be used to analyze the existing services of LMS systems to determine service groups in accordance with the proposed reference model.

Conclusion

In this article, the monitoring and control services that are used in LMS learning management systems were considered.

The article provides an analytical overview of the existing LMS, what opportunities they provide for monitoring and control. The authors proposed a classification of monitoring and control services based on the criterion of the coverage of users and elements. Based on the proposed classification, services are subdivided into services for user control, content control, and operational management and administration. A reference model is also proposed, which includes 6 levels of services, which are grouped into 3

groups: firmware services (software and hardware levels), basic services (user level and content level), and management and analysis services (administrative and analytical levels). To check the effectiveness of the LMS VKTU, the reference model was correlated with the existing and planned services. The result of this correlation showed that the above services are fully consistent with the reference model, which indicates the effectiveness of the LMS VKTU.

The authors also proposed an approach for clustering using the semantic similarity of services on the example of LMS VKTU. An algorithm was used to calculate the semantic similarity of services based on the processes in which they participate and the entities with which they interact. Based on the obtained estimates of semantic similarity, the clustering of services was performed using the FOREL algorithm with different radii. The resulting clusters make it possible to assess the similarity of services within the clusters, and correspond to the distribution of services according to the reference model, and also make it possible to implement the missing services within the existing ones.

References:

1. *T.Y. Wang, C.H. Wang.* «E-Learning Platform of STEAM Aesthetic Course Materials Based on User Experience» In Proc. Of the 1st International Cognitive Cities Conference (IC3), IEEE, August 2018, P. 123-128.

2. *P. Zaharias, C. Pappas.* Quality management of learning management systems: A user experience perspective // Current Issues in Emerging eLearning, vol. 3(1), 2016, P. 5.

3. *R. Kraleva.* Designing an Interface for a Mobile Application Based on Children's Opinion // International Journal of Interactive Mobile Technologies, vol. 11(1), 2017, P. 53-70.

4. *J.W. Lin, H.C.K. Lin.* User acceptance in a computersupported collaborative learning (CSCL) environment with social network awareness (SNA) support // Australasian Journal of Educational Technology, vol. 35(1), 2019, P. 100-115.

5. *V. Narayan, J. Herrington, T. Cochrane.* Design principles for heutagogical learning: Implementing student-determined learning with mobile and social media tools // Australasian Journal of Educational Technology, vol. 35(3), 2019, P. 86-101.

6. *I. Valova, M. Marinov.* Facebook as a Tool Aiding University Education-Whether it is Possible and Useful // TEM Journal, vol.8(2), 2019, P. 670-676.

7 *V. Mokerov.* Razrabotka metodov i modeley proyektirovaniya servisov protsessno-oriyentirovannykh informatsionnykh sistem: dissertatsiya na soiskaniye uchenoy stepeni doktora filosofii (PhD): 6D070300 – Ust'-Kamenogorsk, 2014. – 116 s.

8 *B.W. Kernighan, S. Lin* An efficient heuristic procedure for partitioning graphs. // Bell Syst. Tech. J., – 1970 – vol. 49. – P. 291–307.

9 *S. Kumargazhanova , A. Baklanov, Gy. Györök et al.* Development of the Information and Analytical System in the Control of Management of University Scientific and Educational Activities, Acta Polytechnica Hungarica, Vol. 15, No. 4, 2018, pp. 27-44, DOI: 10.12700/APH.15.4.2018.4.2

10 *A. Baklanov, O. Baklanova, S. Grigoryeva, S. Kumargazhanova, G. Györök et al*. The Development of Hybrid IP Architecture for Solving the Problems of Heating Networks // Acta Polytechnica Hungarica, №1 (17), 2020. pp. 123-140, DOI: 10.12700/APH.17.1.2020.1.7.

11 *M. Bazarova, W. Wójcik, G. Zhomartkyzy, S. Kumargazhanova, G. Popova.* Knowledge transfer as one of the factors of increasing university competitiveness// Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 9(3), 4-9. https://doi.org/10.35784/iapgos.229 ISSN 2083-0157, e-ISSN 2391-6761, DOI: https://doi.org/10.35784/iapgos.229

12 *S. Kumargazhanova, G. Zhomartkyzy, G.Soltan, L. Suleymenova.* Analytical monitoring model of educational system //Proceedings of the 5th International Conference on Engineering and MIS 2019 (ICEMIS ’19), ACM. - Nur-Sultan, Kazakhstan. 2019. – pp. 1-6. DOI: 10.1145/3330431.3330445

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАРДЫ ДЕНСАУЛЫҚ САЛАСЫНДА ПАЙДАЛАНУ

Хакимова Т.Х., Абдиахметова З.М.
e-mail: zukhra.abdiakhmetova@gmail.com
Казахский национальный университет имени аль-Фараби, Казахстан

Аннотация. *Заманауи ақпараттық телекоммуникациялық технологиялар денсаулық саласында қашықтықтан медициналық көмек көрсетуге мүмкіндік береді. Телемедицина – коммуникациялық технологиялар саласындағы жаңа құбылыс. Ол телемедицинаның негізінде қалыптасқан медициналық көмекті қашықтықта көрсетуге мүмкіндік береді. Олар рентген суреттері, УДЗ мәліметтері сияқты медициналық ақпаратпен алмасады. "Телемедицина-бұл аурулардың сапасы мен қанағаттануын арттыратын диагностика мен емдеудің қуатты құралы". Телемедицинаның негізгі және бірінші кезектегі міндеті қашықтықтан диагностика жасау.*

Дәстүрлі түрде телемедицинаның екі негізгі бағыты бар: алыстан кеңес беру және дәрігерлік қабылдау сеанстары, және медицина қызметкерлерінің біліктілігін арттыру және оқыту. Алыстағы консультациялар қатарына белгілі медициналық орталықтардың арнайы мамандары — сарапшылардың консультацияларын да жатқызуға болады, олардың мақсаты қандай да бір себептермен емдеуші дәрігерге қол жетпейтін пациенттің технологияларды, әдістемелер мен препараттарды пайдалану есебінен емдеу процесінің сапасын арттыру болып табылады.

Телемедицина 2 жүйе бойынша жұмыс істейді:

"дәрігер-дәрігер". Ол дәрігерлердің дәрістерін, консилиумдарын өткізуді білдіреді. Сондай-ақ осы жүйе бойынша басқа мамандардан қашықтықтағы қосымша кеңес беруді көздейтін операциялар жүргізіледі.

"дәрігер-пациент". Бұл жүйе үйдегі науқастар мен медик арасындағы қашықтықтан қарым-қатынасты көздейді. Соңғысы алыстан кеңес, диагностика, емдеу және науқасқа бақылау жасай алады.

Осы тұрақты әрекеттерден басқа, телемедицинаның бірнеше бағыты бар:

Онлайн-режимде хирургиялық операцияларды жүргізу және көрсету. Сонымен, тәжірибелі дәрігерлер өздерінің тәжірибелі әріптестерінің операция барысын бақылай алады: операция жасау, Құрал-саймандарды, дәрі-дәрмектерді пайдалану бойынша кеңестер беру.

Дәрігерлерді онлайн оқыту. Әр түрлі қашықтықтан өткізілетін семинарлар мен дәрістер ой-өрісін кеңейтіп, медицина және фармакология саласындағы жаңа әзірлемелермен таныстыруға, теориялық және практикалық білімнің багажын толықтыруға қабілетті.

Онлайн-кеңес беру. Нақты уақыт режимінде дәрігер мен пациенттің өзара әрекеттесуі орын алады. Олар мәтіндік, аудио және графикалық мәліметтермен алмасуы мүмкін.

Басты телемедицина және биомониторинг. Осы бағыттың арқасында үйде емделіп жатқан науқастарға кеңес беруге және бақылауға болады. Пациентте

орнатылған арнайы құрылғылар оның пульсі, АҚ, сондай-ақ басқа да параметрлері туралы ақпаратты емдеуші дәрігердің компьютеріне бере алады.

Мобильді медициналық кешендер. Олар әртүрлі медициналық құрылғылар мен сымсыз байланыс құралдарымен байланыс орнатуға қабілетті қуатты компьютерден тұрады. Мұндай кешендер ТЖ кезінде жиі қолданылады.

Телемедицинаны дамыту

Телемедицина мамандарының ұсынысы бойынша, бірінші кезекте, дистанциялық диагностика болып қала береді, бірақ оның әлеуетті мүмкіндіктері айтарлықтай кең. Желілік технологиялар науқастарды клиникадан клиникаға ауыстыру кезінде ауру тарихын құжаттық түрде беру, сақтандыру және төлеу мәселелерін жедел шешу, дәрігерлердің біліктілігін арттырудың жаңа мүмкіндіктері, жаңа медициналық технологиялар мен әдістерді кеңінен енгізу, дистанциялық медициналық консультациялар, консилиумдар, телеконференциялар және телеманипуляциялар (аппаратураны қашықтықтан басқару және тіпті қашықтықтағы хирургиялық араласу) мүмкіндігін береді.

Әр түрлі бағалаулар бойынша, қазіргі уақытта әлемде шамамен 200 ауқымды телемедициналық жоба жүзеге асырылуда. Жыл сайын миллиондаған алыстағы консультациялар өткізіледі. Көптеген жобалар белгілі бір тақырыпқа арналған және бірқатар медициналық орталықтарды біріктіретін телемедициналық желілер болып табылады. Телемедициналық желілерді іске асыру деңгейі бойынша халықаралық, өңірлік және Ұлттық желілерге бөлу орынды. Халықаралық желілер медициналық орталықтарды, ауруханаларды, әртүрлі елдердің (іс жүзінде - континенттердің) зерттеу институттарын, бір өңір шеңберінде әртүрлі елдердің өңірлік — Медициналық және зерттеу мекемелерін біріктіреді, Ұлттық жобалар жеке алынған ел деңгейінде, көбінесе – денсаулық сақтауды дамытудың ұлттық бағдарламалары шеңберінде іске асырылады.

Телемедициналық жүйелерді құру және пайдалану, биотелеметриялық жүйелерді әзірлеу және қолдануда үлкен тәжірибесі бар ғарыштық медицинамен тығыз байланысты болды. Ю. А. Гагарина мен Г. С. Титова ұшулар кезінде телеметрикалық ЭКГ бір және екі кеуде бұрылыстарында және пневмограммаларда тіркелді. Бұдан әрі сейсмокардиограмманы тіркеу енгізілді, ғарыштық ұшу жағдайында адам ағзасының негізгі физиологиялық және биохимиялық параметрлерін қашықтықтан тіркеу үшін арнайы әдістер мен аппаратура әзірленді, бұл ақпаратты жерге беру және туындаған бұзушылықтарды түзету бойынша шаралар қабылдау үшін, тәжірибелік қызметке ғарыштық ұшуларды медициналық қамтамасыз етуді пайдаланылатын технологияларды енгізу туралы мәселе тұрды. Спутниктік технологиялар өз уақытында телемедициналарды дамытуда үлкен серпіліс жасады.

Интерактивті теле оқыту

Өңірлік телемедициналық желілер мен жүйелерді құрудың мысалы, мысалы, Еуропалық Одақ елдерінің бірлескен жобалары болып табылады. Мұндай жобалардың қатарына eHealth for Safety бастамасы жатады, оның мақсаты дәрігерлік қателерді редукциялау және ауыр ауруларды емдеу процесімен байланысты басқа да келеңсіз оқиғаларды жою, сондай-ақ денсаулық сақтаудағы тәуекел-менеджмент тұжырымдамасын дамыту болып табылады. eHealth for Safety ЕО елдерінің көпшілігін қамтитын 7 басқа бағдарламалармен қатар іске асырылады және 10 жылға есептелген.

Олардың арасында қызығушылық ILS — ЕО елдеріндегі демографиялық көрсеткіштерді бақылау жүйесі, телекоммуникацияны дамытуға және үй

медицинасының ұтқырлығын арттыруға арналған semanticHEALTH бағдарламасы, Q-REC — телемедицина үшін бағдарламалық қамтамасыз етудің сапасын бағалау және сертификаттау бағдарламасы, Share — зерттеу жобаларын қолдау және Еуропа елдеріндегі медицинаның құқықтық және экономикалық аспектілерін дамыту бастамасы болып табылатын басқа да еуропалық жобаларды да атап өткен жөн.

Ұлттық деңгейде телемедициналық жобалар қарқынды дамып келеді,алайда әр түрлі елдердегі даму динамикасы өзгеше. Жалпы, елдің экономикалық даму деңгейі мен ауқымды телемедициналық жобалар саны арасында параллель өткізуге болады. АҚШ немесе Батыс Еуропа елдері сияқты экономикалық дамыған елдерде ұлттық бағдарламалардан басқа зерттеу орталықтарының немесе ірі медициналық орталықтардың қаражаты есебінен іске асырылған Ұлттық медициналық желілер мен жүйелердің айтарлықтай саны бар. Әлсіз мемлекеттер телемедицина саласында, негізінен жалпыұлттық бағдарламалар шеңберінде жобаларды іске асырады.

Көптеген елдерде телемедицина жобаларын үйлестіру үшін қоғамдық және үкіметтік ұйымдар құрылды. Мысалы, Канадада телемедициналық бағдарламаны дамыту үшін медиктерді, ЖОО оқытушыларын, ат-компанияларын біріктіретін телемедицина қоғамы құрылды; АҚШ-та телемедицина қауымдастығы белсенді жұмыс істейді; Жапонияда телемедицина бойынша жұмыстарды үйлестіру үшін денсаулық сақтау министрлігінің жанында директорат құрылды. Қытай ChinaSatCom байланыс операторының белсенді қатысуымен Өз елінде және Оңтүстік-Шығыс Азия елдерінде телемедициналық қызметтерді ұсыну үшін спутниктік желі құруды жоспарлап отыр.

Телемедицина саласында медициналық мекемелер шеңберінде "ресми" консультациялық бағыт қана емес, белсенді дамып келе жатқанын атап өткен жөн. Соңғы 5-6 жылда үй медицинасы жедел қарқынмен дамып келеді, бұл ең алдымен демографиялық үрдістердің теріс дамуымен: халықтың қартаюымен, сырқаттанушылықтың өсуімен, жатқан науқастар санының өсуімен байланысты. Үйдегі телемедицина интернет бойынша кеңес беруден бастап үздіксіз мониторингке дейін және пациенттің жағдайын қашықтан бақылауға дейін технологиялардың кең спектрін пайдалануды білдіреді. Үй телемедицинасына арналған мобильді құрылғылар қосылған қысымды немесе пульсті өлшеуіш — медициналық аспаптармен бейне байланыстың шағын құрылғысы болып табылады, жатқан науқастар жағдайында емдеуші дәрігерге пациенттің жағдайы туралы қажетті ақпаратты жедел алуға мүмкіндік беретін арнайы медициналық пульттер болуы мүмкін. Үй телемедицина саласындағы ең ірі еуропалық жоба "үйде" карт адамдарға қызмет көрсетуге, жатқан науқастардың физиологиялық көрсеткіштерін бақылауға, сондай-ақ босанғанға дейінгі кезеңде жүкті әйелдерді үй бақылауы мен кеңес беруге бағытталған EPIC (European Prototype for Integrated Care) болып табылады.

Телемедицина және Интернет

Телемедицина ғаламдық Интернет желісін дамытумен байланысты, ол арқылы телемедицинаның алдына қойылатын барлық міндеттерді жүзеге асыруға болады. Алайда, телеконсультацияға қатысушылар арасында кепілдік берілген өткізу жолағының болмауы көрнекі ақпараттың берілуін баяулатуға және аудиоақпаратты берудің шектелуіне (олардың үлкен көлеміне байланысты қарым-қатынас жасау мен бейнефрагменттерді берудің практикалық мүмкін еместігіне дейін) әкеп соғады.

Сонымен қатар, Интернет ашық желі болып табылады, ал пациенттердің медициналық деректерін беру және оларды барлық режимде ашық талқылау құқықтық тұрғыдан жарамсыз болып табылады. Ақпаратты қатаң қорғауды енгізу медициналық (жеке, пациент туралы) ақпараттың құпиялылығын сақтау қажеттілігімен байланысты.

Сондықтан телекоммуникацияларды медицинада пайдалану (және мамандар мен денсаулық сақтау мекемелерінің әртүрлі ақпараттық қажеттіліктерін қанағаттандыру) екі негізгі бағыт бойынша дамиды: ашық Интернет желісі арқылы және жабық корпоративтік желілер арқылы телемедицинаның өзі немесе телеконсультация уақытына бөлінген режимде "нүкте-нүкте" немесе "нүкте-көп нүкте"режимінде бар желілердің фрагменттері. Бұл ақпаратты, әсіресе рентгенограммаларға, томограммаларға, микробағдарламаларға және т. б. беруге қойылатын жоғары талаптарға сәйкес келеді. Медициналық бейнелерді (рентген-радиологиялық, микроскопиялық, тері белгілерінің түстерін беру және т.б.) алу және ұсыну стандарттарын әзірлеу, енгізу және сақтау қажетті шарт болып табылады. Белгіленген шектеулерге қарамастан, белгілі бір шектеулермен телемедициналық консультациялар Интернет арқылы да (IP-қосылысты пайдалана отырып) жүзеге асырылады. Бұл жағдайларда, әдетте, науқастарды, емдеуші дәрігерді, консультантты талқылау барысында басқа бейнематериалдар, тек NetMeeting режимінде ортақ "АҚ тақтаны" пайдалана отырып жұмыс істеуге болатын статикалық графикалық материалдар (олардың үстінен сурет салу, күмән тудыратын учаскелерді белгілеу) берілмейді. Кеңес интерактивті дауыстық нұсқада қолдау көрсетеді. Дәл осылай шешен Республикасындағы далалық педиатриялық госпиталінде науқас және зардап шеккен балаларға телеконсультативтік көмек ұйымдастырылды. Интернет және телекоммуникациялық технологияларды пайдалану медицина ғылымы мен практикасының ажырамас бөлігі. Интернеттен ақпарат белгілі бір дәрежеде дәрігерлер қоятын диагноздарға және олар өз пациенттеріне жазып отырған дәрілерді таңдауға әсер етеді.

Қорытынды

Телемедицина өзіне бірнеше саланы біріктіреді, яғни, медицина, телекоммуникация, ақпараттық технологиялар. Ең басты жетістіктерінің бірі – жетекші медициналық орталықтардың жоғары мамандандырылған жәрдемін жеке аудандарға беру, пациенттердің шығындарын айтарлықтай үнемдеу мүмкіндігі. Телемедициналық кеңестер байланыстың электрондық каналдары арқылы медициналық ақпараттық хабарлар беру көмегімен жүзеге асырылады. Кеңестер деректерді беру және сақтау режимінде де және сол нақты уақытта online режимінде де орындалады. Жоспарлы және шұғыл, жоспардан тыс видеокеңестер, видеоконсилиумдар кеңесші дәрігер мен емдеуші дәрігердің, қажет болған жағдайда науқасты қатыстыра отырып, тікелей қатынасуға болады. Сонымен қатар, видеоконференциялық байланыстар сеансы екі абонент арасында да және көпнүктелі режим деп аталатын бірнеше абоненттер арасында да өткізуге болады, яғни аса күрделі жағдайларда түрлі медициналық орталықтардың дәрігерлері арасындағы консилиумымен талқылануы мүмкін. Телемедициналық жүйелер дәрігер сарапшымен диалогты ұйымдстыруға, кез-келген аралықта мамандандырылған қорытынды шығару үшін барлық медициналық ақпараттарды (ауру тарихынан үзінді, УДЗ суреттері) беруге мүмкіндік береді. Телемедицина жобасының түпкі мақсаты – төрт интеграциялық деңгейлермен телемедицинаның ұлттық желісін құру болып табылады.

Әдебиеттер

1. Т.Х.Хакимова, Инновационные методы обучения информатике (учебное пособие). ISBN9965-830-45-2. Издательство"NURPRESS", Алматы, 2013. – 270стр.
2. Т.Х.Хакимова, Қашықтықтан оқыту технологиясы (Оқу әдістемелік құрал). ISBN-978-601-04-1031-2. Қазақ университеті, Алматы: 2015– 200 бет.
3. Т. Хакимова, М.Ж. Сакыпбекова, Ж.Х. Спабекова. Қашықтықтан оқытуды ұйымдастырудың желілік технологиясы. Материалы 51-ой научно-методической конференции «Оценка ожидаемых результатов обучения по образовательным программам и учебным дисциплинам в контексте компетентностно-ориентированного подхода» 17-19 марта 2021 года, Книга 2,стр.335-340.Алматы «Қазақ университеті», 2021.
4. Т.Х.Хакимова. «Ақпараттық технологияларды оқытудың логикалық бағдарламалау негіздері.»(Оқу құралы.)ISBN 978-601-04-0205-8, Издательство"Қазақ университеті", 2013 - 102бет.
5. https://crbpanfilov.kz/index.php/kz/zha-aly-tar/85-telemeditsina
6. https://telemedicina.one/telemedicina/telemeditsina.html
7. https://ppt-online.org/207407
8. Истрофилова О. И. Инновационные процессы в образовании: Учебно-методическое пособие. – Нижевартовск: Изд-во Нижеварт.гост.ун-та, 2014. -133 стр.

СЕКЦИЯ 3

Жасанды интеллект технологиялары. Интеллектуалды басқару жүйелері. Компьютерлік лингвистика және сөйлеу технологиялары. Бейнелерді танып білу және кескіндерді өңдеу. Биоинформатика және биометрикалық жүйелер. Адам-машиналық өзара әрекеттесуі. Машиналық оқыту. Интеллектуалды робототехникалық жүйелер

Технологии искусственного интеллекта. Интеллектуальные системы управления. Речевые технологии и компьютерная лингвистика. Распознавание образов и обработка изображений. Биоинформатика и биометрические системы. Человеко-машинное взаимодействие. Машинное обучение. Интеллектуальные робототехнические системы

Technologies of artificial intelligence. Intelligent control systems. Speech technologies and computer linguistics. Image recognition and image processing. Bioinformatics and biometric systems. Human-machine interaction. Machine learning. Intelligent Robotic Systems

СТУДЕНТТЕРДІҢ ДЕНСАУЛЫҚ ЖАҒДАЙЫН БАҒАЛАУҒА АРНАЛҒАН ДЕРЕКТЕРДІ ТАЛДАУДА ҚОЛДАНЫЛАТЫН ӘДІС – ТӘСІЛДЕР

Г.А.Тюлепбердинова[1], М. Е. Мансурова[2], А.Шілмағамбетова[3]
e-mail: tyulepberdinova@mail.ru
[123]әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Қазақстан

Аңдатпа. *Бұл мақалада студенттердің денсаулық жағдайын бағалаудың зияткерлік ақпараттық жүйесінің тұжырымдамасы мен архитектурасын әзірлеу тұжырымдалды. Соңғы он жылдықта Қазақстан Республикасының Үкіметі денсаулық сақтау жүйесін цифрландырудың маңыздылығын алға тартып келеді, оның құрамына мәліметтер базасын интеграциялау, үйде емделіп жатқан науқастарға бақылау жүйесін және тұлғалардың денсаулық жағдайын бағалауға арналған интеллектуалды ақпараттық – аналитикалық жүйелерді құру және оны бағалау сынды жобалар кіреді. Мемлекет тарапынан құрылып отырған «Денсаулық» жобасының мақсаттарының бірі – балалар мен жастар денсаулығын қадағалау, орын алған жағымсыз жағдайларды алдын алып оңтайлы басқару болып табылады. Бұл мақсатқа қол жеткізу тиісті бағдарламалық қамтамасыздандырусыз, атап айтқанда, дәрігердің шешім қабылдауына интеллектуалды қолдау көрсететін бағдарламалық өнімдердің құрылуынсыз мүмкін емес.*

Жастардың денсаулық жағдайына әртүрлі факторлардың күрделі кешені әсер ететіні белгілі, олардың арасында қарқынды ақыл-ой белсенділігімен, жұмыс және демалыс режимінің бұзылуымен, физикалық белсенділікпен, тамақтану әдеттерімен, денсаулыққа қауіп төндіретін зиянды әдеттермен шиеленісетін стресстік жағдайлармен байланысты оқу жүктемесі ерекше орын алады. Бұл студенттердің физикалық жағдайын ғана емес, сонымен бірге оның психологиялық денсаулығын және дененің бейімделу қабілетінің даму дәрежесін бағалауға мүмкіндік беретін әдістер негізінде қалыптастырылған ақпаратты автоматтандырылған өңдеу жүйелерін дәрігерлердің тәжірибесіне кеңінен енгізу қажеттілігіне әкеледі [1]. Бұл денсаулық жағдайына мониторинг жүргізуге және мүмкін болатын жағымсыз жағдайларды алдын – алуға мүмкіндік береді. Интеллектуалды – ақпараттық жүйе әр – түрлі деректер көзінен қажетті деректерді жинақтайды. Біздің жағдайымызда деректер көзі болып зерттеу объектісі ретінде алынған жасөспірім жастағы 1 курс студенттерінен алынған HBSC сауалнама нәтижелері болып табылады. Алынған HBSC сауалнама нәтижелері онда кездесетін қателіктерден, қажеті мен маңызы жоқ деректерден немесе дұрыс жауап берілмеген деректерден тазаланып, одан әрі деректер қорына көшіріледі. Деректер қоры ретінде бұлтты технологияны қолдайтын деректер қоры алынды. Себебі, жинақталған деректер уақыт өткен сайын толықтанады, және интеллектуалды ақпараттық – аналитикалық жүйе соңғы талдау жұмыстары жүргізілген деректерді нақты уақыт режимінде визуализациялап, соңғы толықсыған HBSC сауалнама деректеріне талдау жұмысын көрсетеді. Бұл динамикалық түрде жүзеге асырылады, яғни деректерге уақыт өткен сайын жаңа деректер қосылса, талдау автоматты түрде өзгерілуі керек. Одан әрі деректерді өңдеу процесі орын алады, бұл жерде сауалнама сұрақтарының арасындағы байланыстар мен индикаторлардың өлшемі анықталып,

деректер моделінде пайда болған кестелер арасындағы байланыстар табылып, қажетті сұраулар орындалады. Сауалнама нәтижесіне корреляциялық, факторлық талдаулар және сонымен қатар, медицина саласында қолданылатын статистикалық талдаулар жасалынып өңделеді. Талдау жұмыстары кестелер, диаграммалар және карталар түрінде көрсетіледі.

Деректерді талдауда қолданылатын әдіс – тәсілдерге тоқталайық. Жинақталып және өңделген деректерді талдау жұмыстарын жасау үшін медициналық деректерді талдауда қолданылатын статистикалық әдістер, оның ішінде корреляциялық талдау мен мүмкіндік қатынасы қолданылды.Сонымен қатар, қосымша талдау жұмыстарына, Power BI қосымшасы ұсынатын компоненттер арқылы жасалынды.

Мүмкіндік қатынасы (Odds Ratio) - бұл статистикалық көрсеткіш, белгілі бір нәтиженің болмауы немесе болуы белгілі бір статистикалық топта белгілі бір фактордың болуымен немесе болмауымен байланысты екенін сандық түрде сипаттаудың негізгі тәсілдерінің бірі. Мүмкіндік қатынасы белгілі бір нәтиже мен қауіп факторы арасындағы байланысты бағалауға мүмкіндік береді. Мүмкіндік қатынасы белгілі бір нәтижені анықтау жиілігі бойынша зерттелетін топтарды салыстыруға мүмкіндік береді. Мүмкіндік қатынасын қолдану нәтижесі фактор мен нәтиже арасындағы байланыстың статистикалық маңыздылығын анықтау ғана емес, сонымен бірге оны сандық бағалау болып табылады. Екі топты салыстыру кезіндегі мүмкіндіктің қатынасы негізгі топтағы нәтиженің даму мүмкіндігін бақылау тобындағы нәтиженің даму мүмкіндігіне бөлудің көрсеткіші ретінде есептеледі. Өз кезегінде, мүмкіншіліктер-нәтиженің болуымен зерттелетін санның нәтиженің болмауымен зерттелетін санның санына қатынасы. Сондай-ақ есептелген үшін 95% сенімді интервалы есептеледі (95% CI). Мүмкіндік - белгілі бір белгісі (нәтижесі немесе факторы) бар зерттелгендер санының осы белгісі жоқ зерттелгендер санына қатынасы. Ыңғайлы әдіс конъюгация кестесін қолданып есептеу болып табылады. Конъюгация кестесі - бұл үйлесімділік принципі бойынша екі немесе одан да көп белгілерді топтастыру негізінде зерттеу объектілері туралы мәліметтерді ұсыну нысаны. Егер бірінші айнымалы m мәндерін, ал екінші айнымалы n мәндерін қабылдай алатын болса, онда алынған белгілердің жұптасу кестесі $m * n$ матрицасы болады, оның әр ұяшығына кездесетін белгілер комбинациясының жиілігі енгізіледі. 1- кестеде конъюгация кестесінің үлгісі көрсетілген.

Кесте 1 – Конъюгация кестесінің жалпы түрі

	Нәтижесі бар (1)	Нәтижесі жоқ (0)	Барлығы
Тәуекел факторы бар (1)	A	B	A+B
Тәуекел факторы жоқ (0)	C	D	C+D
	A+C	B+D	A+B+C+D

Берілген кесте үшін мүмкіндік қатынасы келесі формула бойынша есептеледі:

$$OR = \frac{A * D}{B * C} \quad (1)$$

Нәтиже мен қауіп факторы арасындағы анықталған байланыстың статистикалық маңыздылығын бағалау өте маңызды. Бұл бірлікке жақын мүмкіндік

қатынастарының төмен мәндерімен де байланыс маңызды болуы мүмкін және статистикалық тұжырымдарда ескерілуі керек. Керісінше, мүмкіндік қатынасының үлкен мәндерімен, көрсеткіш статистикалық тұрғыдан маңызды емес, сондықтан анықталған байланысты елемеуге болады.

Мүмкіндік қатынасының маңыздылығын бағалау үшін сенімділік интервалының 95% шекаралары есептеледі («confidence interval» ағылшын тілінен 95% CI аббревиатурасы қолданылады). 95% CI жоғарғы шекарасының мәнін табу формуласы:

$$e^{\ln(OR)+1,96*\sqrt{\frac{1}{A}+\frac{1}{B}+\frac{1}{C}+\frac{1}{D}}} \quad (2)$$

95% CI төменгі шекарасының мәнін табу формуласы:

$$e^{\ln(OR)-1,96*\sqrt{\frac{1}{A}+\frac{1}{B}+\frac{1}{C}+\frac{1}{D}}} \quad (3)$$

Мүмкіндік қатынасы мәнінің интерпретациясы:

✓ Егер мүмкіндіктің қатынасы 1-ден көп болса, онда бұл нәтиже бар топта тәуекел факторын анықтау мүмкіндігі көбірек екенін білдіреді. Яғни фактор нәтиженің пайда болу ықтималдығымен тікелей байланысты. Мүмкіндік қатынасы мәні негізгі топтағы нәтиженің мүмкіндігі бақылауға қарағанда қанша есе жоғары екенін көрсетеді. Мысалы, егер OR = 3 болса, негізгі топта зерттелетін нәтиженің даму мүмкіндігі бақылау тобына қарағанда 3 есе көп деген қорытынды жасалады.

✓ Мәні 1-ден аз мүмкіндіктің қатынасы екінші топта қауіп факторын анықтау мүмкіндігі көбірек екенін көрсетеді. Яғни фактордың шығу ықтималдығымен кері байланысы бар. Мысалы, егер OR=0,5 болса, онда біз негізгі топтағы нәтиженің мүмкіндігі бақылау тобына қарағанда 2 есе төмен деген қорытынды жасау керек.

✓ Мүмкіндік қатынасы 1–ге тең болған жағдайда, салыстырылатын топтарда қауіп факторын анықтау мүмкіндігі бірдей. Тиісінше, фактор нәтиже ықтималдығына әсер етпейді.

Сонымен қатар, әр жағдайда сенім интервалының 95% мәндеріне сүйене отырып, мүмкіндік қатынастарының статистикалық маңыздылығы міндетті түрде бағаланады.

✓ Егер сенімді интервал 1-ді қамтымаса, яғни шекаралардың екі мәні де 1-ден жоғары немесе төмен болса, $p<0,05$ маңыздылық деңгейінде фактор мен нәтиже арасындағы анықталған байланыстың статистикалық маңыздылығы туралы қорытынды жасалады. Мысалы, 95% CI: 1,5-3,7. Статистикалық маңызды айырмашылықтардың болуы туралы қорытынды жасалады, өйткені төменгі шекара 1,5>1, ал жоғарғы - 3,7>1. Сенімділік интервалы 1-ді қамтымайды.

✓ Егер сенімділік интервалы 1 - ді қамтыса, яғни оның жоғарғы шегі 1-ден жоғары, ал төменгі шегі 1-ден аз болса, $p>0,05$ маңыздылық деңгейінде фактор мен нәтиже арасындағы байланыстың статистикалық маңыздылығының болмауы туралы қорытынды жасалады. Мысалы, 95% CI: 0,7-2,3. Статистикалық маңызды айырмашылықтардың жоқтығы туралы қорытынды жасалады, өйткені төменгі шекара 0,7<1, ал жоғарғы шегі - 2,3>1.

✓ Сенімділік интервалының мәні фактор мен нәтиженің байланысы маңыздылығының деңгейіне кері пропорционал, яғни 95% CI- дан аз болса, анықталған тәуелділік соғұрлым маңызды болады [2].

Корреляциялық талдау. Корреляция - екі немесе одан да көп айнымалылар арасындағы байланыс. Корреляциялық талдаудың мақсаты - бұл қарым-қатынастың болуын немесе болмауын анықтау. Егер екі айнымалы болса, олардың мәні қатынастар шкаласында өлшенеді, Пирсонның R сызықтық корреляция коэффициенті қолданылады, ол -1-ден +1-ге дейінгі мәндерді алады. Сауалнама нәтижелерін талдаудағы денсаулыққа қатысты шағымдардың бір – біріне қалай әсер ететіндігін Пирсонның корреляциялық критерийі бойынша есептеуге болады. Мысалы, бас ауруы, бас айналу сезімі, іштің ауруы, жүйке сезімі, тітіркену мен жаман көңіл күй арасындағы корреляциялық байланысты табуға болады. Сонымен қатар, Пирсонның корреляция критерийін қолдана отырып, студенттің ӘЭС мен оның пайдалы және зиянды тамақтану, дене салмағы, университеттен тыс белсенді салауатты өмір қағидаты арасындағы байланыс бар ма деген сұраққа жауап беруге болады.

Мысалы, баланың өсуі оның жасына байланысты, яғни бала неғұрлым үлкен болса, соғұрлым жоғары болады. Егер біз әр түрлі жастағы екі баланы алсақ, онда үлкен баланың өсуі кішіге қарағанда жоғары болады. Бұл құбылыс тәуелділік деп аталады, бұл индикаторлар арасындағы себептік байланысты білдіреді. Әрине, олардың арасында корреляциялық байланыс бар, яғни бір көрсеткіштің өзгеруі басқа көрсеткіштің өзгеруімен бірге жүреді.

Пирсонның корреляция коэффициентін есептеу келесі формула бойынша жүзеге асырылады:

$$r_{xy} = \frac{\sum (d_x * d_y)}{\sqrt{(\sum d_x^2 * \sum d_y^2)}} \qquad (4)$$

Пирсон корреляция коэффициентінің интерпретациясы:

Пирсонның корреляция коэффициентінің мәні оның абсолютті мәндеріне байланысты түсіндіріледі. Корреляция коэффициентінің мүмкін мәндері 0-ден ±1-ге дейін өзгереді. R_{xy} абсолютті мәні неғұрлым үлкен болса, екі шаманың арасындағы байланыс тығыздығы соғұрлым жоғары болады. $r_{xy} = 0$ байланыстың толық жоқтығын білдіреді. $r_{xy} = 1$- абсолютті (функционалды) байланыстың болуын көрсетеді. Егер Пирсонның корреляция критерийінің мәні 1-ден көп болса немесе -1 – ден аз болса-есептеулерде қате жіберіледі.

Кесте 2 – да көрсетілгендей, Чеддок кестесін қолданып, корреляциялық байланыстың беріктігін дәлірек бағалауға болады [3].

Кесте 2 – Корреляциялық байланыстың кестесі

Абсолютті мәні r_{xy}	Корреляциялық байланыстың беріктігі
r_{xy} <0,3	әлсіз

$0,3 \le r_{xy} < 0,5$	орташа
$0,5 \le r_{xy} < 0,7$	елеулі
$0,7 \le r_{xy} < 0,9$	жоғары
$r_{xy} \ge 0,9$	өте жоғары

Сонымен, 2 кестеге қарай отырып, HBSC сауалнамасының нәтижесін талдау барысында жасалған корреляциялық талдау арқылы талданып отырған көрсеткіштер қаншалықты деңгейде байланысқанын анықтауға болады. Мысалы, студенттің дене салмағы мен оның университеттен тыс уақытта белсенді салауатты өмір салтын ұстану арасындағы корреляциялық байланыс 0,8 болатын болса, онда бұл екі көрсеткіш арасында тығыз, яғни өте жоғары байланыс бар екенін көрсетеді.

Әдебиеттер

1. Alanjary, M., Cano-Prieto, C., Gross, H. & Medema, M. H. Computer-aided re-engineering of nonribosomal peptide and polyketide biosynthetic assembly lines. Nat. Prod. Rep. 36, 1249–1261 (2019).
2. Montalbán-López, M. et al. New developments in RiPP discovery, enzymology and engineering. Nat. Prod. Rep. 38, 130–239 (2020).
3. Hannigan, G. D. et al. A deep learning genome-mining strategy for biosynthetic gene cluster prediction. Nucleic Acids Res. 47, e110 (2019).

ҚАЗАҚ ТІЛІНДЕГІ МӘТІНДЕРДЕ КОЛЛОКАЦИЯЛАРДЫ АНЫҚТАУДЫҢ СТАТИСТИКАЛЫҚ ӘДІСТЕРІН ТАЛДАУ

Г.С. Ыбытаева[1], О.Ж. Мамырбаев[2], Н.Ф. Хайрова[3], Б.Ж. Жумажанов[4]
*e-mail: ybytayeva.galiya@gmail.com
[1]Satbayev University, Қазақстан, Алматы
[2,4] Ақпараттық және есептеуіш технологиялар институты, Қазақстан, Алматы
[3]«Харьков политехникалық институты» ұлттық техникалық университеті, Украина, Харьков

Аңдатпа. *Мақалада қазақ тіліндегі тұрақты тіркестерді анықтау бойынша зерттеу нәтижелері сипатталады. Эксперимент қазақ тілінің жиіліктік етістіктері мен зат есімдері бар биграммаларды табу және талдау болды.*

Корпустық материалға статистикалық әдісті қолдану зерттеушілерге алынған деректерді сандық түрде бағалауға мүмкіндік береді. Мақалада сөз тіркестер шеңберіндегі байланыс күшін есептеу үшін MI, t-score өлшемдеріне шолу жасалады, оның ішінде олардың негізгі сипаттамалары талқыланады.

1 Кіріспе

Қазіргі заманғы ақпараттық-коммуникациялық технологиялардың ғылымның барлық салаларына, атап айтқанда, филология ғылымына ену процесінде тілдің әртүрлі аспектілерін зерттеуде мәтіндердің лингвистикалық корпустарын қолданудың танымалдығы артып келеді. Соңғы бірнеше жылда әдістемелік әдебиеттерде әр түрлі лингвистикалық корпустар арқылы шет тілінің лексикалық және грамматикалық жақтарына оқушылар мен студенттерді оқытуға арналған әдістемелік зерттеулердің тұтас топтамасы пайда болды [1-4]. Осы және басқа зерттеулерді талдау авторлардың «лингвистикалық корпус» терминінің тұжырымдамалық мазмұнына қатысты белгілі бір келісімге келгенін көрсетеді. Бұл белгілі бір әдістеме бойынша таңдалған және белгіленген және электронды түрде ұсынылған мәтіндердің ұйымдастырылған жиынтығын білдіреді.

Біздің зерттеудің негізгі бағыты параллель мәтіндердің корпусына арналған. Біздің зерттеуімізде параллель мәтіндер корпусы деп бір тілдегі бастапқы мәтіннен және оның басқа тілге немесе басқа тілдерге аударылуынан тұратын лингвистикалық корпустың түрін түсінеміз.

Бұл лексикалық үйлесімділікті немесе контекстегі коллокация құбылысын зерттеуге мүмкіндік беретін мәтіндердің лингвистикалық корпусы.

Жақында автоматтандырылған жүйелерге қажеттіліктің артуына байланысты мәтіндердегі тіркесімдердің сөз тіркестерін автоматты түрде бөлуге байланысты мәселеге көп көңіл бөлінді. Сөздердің үйлесімділігін бағалау үшін әртүрлі статистикалық көрсеткіштер бар. Бірқатар өлшемдер ассоциация өлшемдері немесе ассоциативті өлшемдер деп аталады. Олар сөз тіркестерінің элементтері арасындағы байланыс күшін есептеуге мүмкіндік береді және осы сөз тіркестерінің жиілігіне және олардың құрамына кіретін жеке сөздерге негізделеді. Осылайша, лексикалық бірліктерге тән кейбір тұрақтылықты есептеуге болады, бұл оларды шартты шкала бойынша орналастыруға мүмкіндік береді: еркін комбинациялардан

фразеологиялық бірліктерге дейін. Жалпы, 80-нен астам өлшем бар, олар фразалардың байланыс күшін бағалауға мүмкіндік береді [5].

Мақала келесідей ұйымдастырылған. 2-бөлім әдебиеттерді шолуға арналған. 3-бөлімде статистикалық әдіске шолу беріледі, 4-бөлімде зерттеу әдістемесі келтіріледі және соңғы бөлімде зерттеу нәтижелері талқыланып, болашаққа арналған жоспарлар ұсынылады.

2 Байланысты жұмыстар

«Коллокация» термині жақында тұрақты қолданысқа енгенімен, қазіргі тіл білімінде маңызды орындардың бірін алады. Кең мағынада, бұл бірлескен кездесуге бейім екі немесе одан да көп сөздердің тіркесімі. Қазіргі уақытта коллокациялар лексикографиялық тәжірибеде жетекші рөл атқарады [6, 7]. Соңғы уақытта шетелде және Қазақстанда арнайы коллокациялар сөздіктері құрылуда [8, 9, 10].

Алайда, қолданыстағы тұрақты сөз тіркестерінің сөздіктері, біріншіден, олардың толық тізімін қамтымайды, екіншіден, олар көбінесе жеткіліксіз дәйекті түрде жасайды. Бұл әсіресе қазақ тіліне қатысты. Сондықтан мәтіндерден коллокацияларды автоматты түрде анықтау бойынша жұмыстардың өзектілігі сөзсіз.

Қазіргі уақытта біз мәтіндердің үлкен корпустарынан коллокацияларды алудың автоматтандырылған әдістерін қажет ететін бірнеше маңызды қолданбалы міндеттерді көріп отырмыз. Атап айтқанда, бұл сөздіктер мен басқа лексикографиялық құралдарды құрастыру, онтологияларды құрастыру, тілді оқыту, лингвистикалық процессорларды жөндеу, ақпараттық іздеу міндеттері.

Коллокация ұғымына қысқаша тоқталайық. Бұл тұжырымдаманың әртүрлі анықтамалары бар. Жалпы, коллокацияның көптеген анықтамалары фразалық элементтердің семантикалық-грамматикалық өзара тәуелділігі құбылысына негізделген [11].

Орыс тілді ғылыми әдебиеттегі «коллокация» термині алғаш рет О.С. Ахмановаңың лингвистикалық терминдер сөздігінде пайда болды [12]. Орыс лингвистикасындағы орыс тілі материалындағы коллокация ұғымын зерттеуге арналған алғашқы жұмыс - Е.Г. Борисованың монографиясы [13].

Қазақ тілінен шет тіліне тұрақты тіркестің мағынасын, ұлттық-мәдени келбетін жоғалтпай аудару мәселесімен айналысқан Қожахметова Х., Жайсақова Р.Е., Қожахметова Ш.О. сынды ғалымдар 2300-ге жуық тұрақты тіркестерден тұратын сөздікті жарыққа шығарды. Сөздік аударма ісінде қолдануға тиімді, алайда, егер тұрақты тіркестер мағыналық категориялар бойынша бөлінсе қолданыста тиімділігі арта түседі деп санаймыз.

3 Статистикалық әдіс

Қазіргі уақытта «коллокация» термині корпус лингвистикасында кеңінен қолданылады, оның аясында коллокация ұғымы дәстүрлі лингвистикамен салыстырғанда қайта түсіндіріледі немесе жеңілдетіледі. Бұл тәсілді статистикалық деп атауға болады. Бірлескен кездесу жиілігі бірінші орынға қойылады, сондықтан корпус лингвистикасындағы коллокацияларды статистикалық тұрақты тіркестер ретінде анықтауға болады. Сонымен қатар, статистикалық тұрақты комбинация фразеологиялық және еркін болуы мүмкін. Соңғы жылдары осы тұжырымдамаға статистикалық тәсілдің теориялық аспектілеріне де, коллокацияны анықтаудың практикалық әдістеріне де әсер ететін коллокацияларға арналған көптеген зерттеулер мен әзірлемелер пайда болды.

Бұл мәтіннің үлкен өкілдік корпусының пайда болуы, бұл тұтастай алғанда тілдегі бір немесе басқа комбинацияның жиілігі туралы сенімді мәліметтер алуға мүмкіндік береді. Бірлескен кездесу жиілігінің жоғары мәні осы комбинацияның тұрақтылығын көрсететін сияқты. Алайда, бұл сипаттама белгілі бір сөздердің таңдаулы үйлесімділігі туралы айту үшін жеткіліксіз. Сондықтан коллокация құрамындағы элементтер арасындағы байланыс күшін есептейтін бірқатар статистикалық өлшемдер (олар «ассоциация өлшемдері» немесе ассоциативті байланыс өлшемдері, ағылшын. association measures деп аталады) жасалды. Жалпы жағдайда, бұл өлшемдер бірлескен кездесу жиілігін де, басқа да параметрлерді де, ең алдымен әрбір жеке элементтің берілген корпусындағы жиілікті ескереді.

Алайда статистикалық мәліметтер жеткіліксіз. Мұндай статистикалық тұрақты тіркестер тағы қандай талаптарға сәйкес келуі керек деген сұраққа жауап беру керек.

Корпус менеджерлерінің көпшілігінде сөздердің немесе сөз формаларының жиілігін және бірлескен кездесу жиілігін есептеу мүмкіндігі бар. Осы мәліметтерге негізделген көптеген ассоциация өлшемдері бар.

Бұл өлшемдердің жалпы саны ондаған деп есептеледі. Ассоциация өлшемдерінің мағыналарын фразалық элементтер арасындағы синтагматикалық байланыс күшінің көрсеткіштері деп санауға болады. Ең көп таралған өлшемдердің сипаттамасын [14] қараңыз. MI, t-score басқаларға қарағанда жиі қолданылады. Кейбір корпус менеджерлері бұл өлшемдерді есептеуге мүмкіндік береді.

[15] жұмысқа енгізілген MI (mutual information) өлшемі мәтінде кездейсоқ пайда болған сөздер сияқты контекстке байланысты тәуелді жиіліктерді тәуелсіз жиіліктермен салыстырады:

$$MI(n,c) = \log_2 \frac{f(n,c)\times N}{f(n)\times f(c)}, \text{ мұндағы} \qquad (1)$$

n – түйінді сөз (node); c – коллокат (collocate); f(n,c) – n кілт сөзінің c коллокатымен жұпта кездесу жиілігі; f(n), f(c) – n кілт сөзінің және корпустағы (мәтіндегі) c сөзінің абсолютті (тәуелсіз) жиілігі; N – корпустағы (мәтіндегі) сөз қолданыстарының жалпы саны.

Егер MI (n,c) мәні белгілі бір мәннен үлкен болса, онда бұл сөз тіркесін статистикалық маңызды деп санауға болады. MI (n, c) нөлден аз болса, n және c бір-бірін толықтыратын қатынаста болады деп айтылады.

T-score өлшемі сонымен қатар коллокаттар арасындағы ассоциацияның (байланыстың) күші қаншалықты кездейсоқ емес деген сұраққа жауап бере отырып, кілт сөз бен оның коллокатының бірлескен кездесу жиілігін ескереді:

$$t - score = \frac{f(n,c) - \frac{f(n)\times f(c)}{N}}{\sqrt{f(n,c)}} \qquad (2)$$

4 Статистикалық әдіс негізінде коллокацияларды анықтау

Жұмыстың мақсаты – қазақ тілі корпусына негізделген әр түрлі ассоциациялық өлшемдерге салыстырмалы талдау. Сонымен қатар, нәтижелердің (бірдей өлшем негізінде алынған коллокациялар тізімі) мәтіндік материалға (мәтін түрі) тәуелділігі зерттеледі.

Біздің зерттеу 645 мәтінді қамтитын «nur.kz», «zakon.kz», «patrul.kz», «caravan.kz», «inform.kz» жаңалықтар мәтіндері корпусының материалы негізінде жүргізілді.

Төмендегі 1-кестеде MI өлшемінің мәні бойынша сұрыпталған *полиция* тірек сөзі бар 15 коллокацияға арналған мәліметтер келтірілген.

Кесте 1. «Полиция» сөзіне ассоциациялық өлшемдерінің мәндері

№	Collocation	Joint	Freq1	MI	t-score
1	Полиция департаменті	86	255	9,86	4,14
2	Полиция басқармасы	34	186	9,41	3,17
3	Полиция қызметкері	56	302	9,23	6,2
4	Полицияға хабарласу	67	227	8,95	5,07
5	Полиция қызметі	63	304	8,87	5,31
6	Полиция бөлімі	51	86	8,36	2,03
7	Полиция көлігі	15	520	8,1	5,52
8	Полиция басшысы	46	113	7,81	4
9	Полиция шақыру	45	123	7,73	3,12
10	Полицияға жүгіну	50	109	7,45	6,47
11	Әскери полиция	11	13	6,55	4,41
12	Қаржы полициясы	26	96	6,38	3,31
13	Тұрғылықты полиция	26	32	6,11	3,86
14	Полиция жасағы	35	43	6,07	5,39
15	Патрульдік полиция	25	42	5,21	3,74

Кестенің бағандарында, коллокацияның өзінен басқа, келесі сипаттамалар көрсетілген: Joint – бірлескен кездесу жиілігі, Freq1 – коллокат жиілігі, MI score – MI өлшемінің мәні, T-score – t-score мәні.

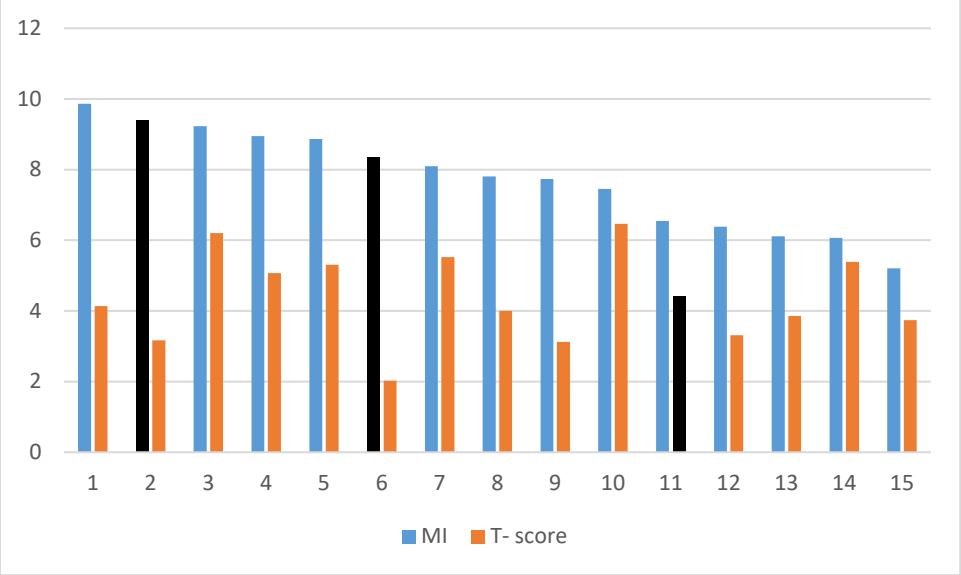
Кесте 1 деректерін талдау (барлығы 15 коллокация) әртүрлі өлшемдер негізінде алынған коллокациялардың рангтері сәйкес келмейтінін көрсетеді.

Сондай-ақ, әр түрлі өлшемдер коллокацияны құрайтын сөздердің жиілігіне және бірлескен кездесу жиілігіне әсер ететінін ескеру қажет. Осылайша, MI төмен жиілікті сөздерге сезімтал, ал t-score жоғары жиілікті коллокацияларды табу үшін пайдалы деп айтылады.

Біз ассоциацияның әртүрлі өлшемдері негізінде автоматты түрде алынған коллокацияларды әртүрлі сөздіктердің деректерімен салыстырдық. Материал омонимсіз 2 зат есім (sozdik.kz) және 1 сын есімнің (Қазақ-орыс, орыс-қазақ терминологиялық сөздігі. Құқықтану) жинақтары болды.

Жоғарыда келтірілген коллокацияларды «дұрыс» деп атаймыз.

Төменде ординат осі бойынша MI, t-score өлшемдерінің мәндері және абсцисса осі бойынша биграмм дәрежелері көрсетілген график келтірілген. Қара түс «sozdik.kz» (3, 6 рангтары) сөздігінен «дұрыс» коллокацияларды және «Қазақ-орыс, орыс-қазақ терминологиялық сөздік. Құқықтану» (11 рангы) сөздігінде табылған қосымша коллокацияны көрсетеді



Сур. 1 – Полиция сөзімен коллокациялар үшін өлшемдердің мәндері

Алынған барлық тіркестер үшін бірдей тенденция байқалады: өлшемнің мәні неғұрлым аз болса, соғұрлым бұл сөз тіркестерінің қазақ тілінің сөздіктерінде тұрақты тіркестер ретінде тіркелмеуі ықтимал. Осылайша, сөздіктерде келтірілген үйлесімділік деректері ассоциациялық өлшемдері негізінде алынған мәліметтерге сәйкес келеді деп айтуға болады.

Эксперимент нәтижесінде сөздіктердің ешқайсысында тіркелмеген тіркестер анықталғандығы маңызды болып көрінеді. Мұндай тіркестерді талдау көрсеткендей, ықтималдық дәрежесі бойынша тізімнің жоғарғы жағында орналасқан (өлшемдердің бірінен кему ретімен сұрыпталған) биграммалар тұрақты болып шығады, демек, оларды тізімге енгізуге болады.

Жоғарыда айтылғандай, лингвистикалық модельдерге негізделген статистикалық критерийлер бойынша басқа әдістер де жұмыс істеуі керек. Бұл идея әйгілі Sketch Engine [16] жүйесіне бекітілген және енгізілген. Ол берілген кілт сөз үшін, бір жағынан, берілген тілдегі сөздердің үйлесімділігіне шектеу қоятын синтаксиске, екінші жағынан, семантика мен тілдік узуска байланысты ықтималды заңдылықтарға байланысты типтік сөз тіркестерін береді.

Анықталғандай, «дұрыс» коллокациялар аз екендігі белгілі болды, бірақ бұл біз сүйенген сөздік қордың тым аз болуымен түсіндіріледі, яғни оны кеңейту керек. Жаңа коллокациялық сөздік қажет деп айтуға болады, онда әр түрлі тұрақты тіркестер болуы тиіс.

Осы түрдегі коллокацияларды іздеу және анықтау нәтижелері сөздіктер үшін әртүрлі мысалдарды таңдай алатын лексикографтар үшін және белгілі бір аспект бойынша лексика мен синтаксисті зерттейтін лингвистер үшін ыңғайлы.

5 Қорытынды

Статистикалық әдістерді қолдана отырып алынған тіркестерді сөздіктермен салыстыру кезінде бірдей тенденция байқалады: өлшемнің мәні неғұрлым аз болса, соғұрлым бұл тіркестер қазақ тілінің сөздіктерінде тұрақты болып бекітілмейді және керісінше. Сөздіктерде жазылған коллокациялардың көпшілігі ассоциациялық

өлшемдердің біріне негізделген тізімнің жоғарғы жағында орналасқан. Осылайша, сөздіктерде келтірілген тұрақты үйлесімділік туралы мәліметтер ассоциациялық өлшемдері негізінде алынған мәліметтермен сәйкес келеді немесе басқаша айтқанда, ассоциацияның статистикалық өлшемдері нақты семантикалық-синтагматикалық байланыстарды жақсы анықтайды деп айтуға болады.

Сөздің әртүрлі таптары үшін алынған барлық мәліметтердің жиынтығы бойынша жүргізілген ассоциацияның әртүрлі өлшемдерін салыстырмалы талдау мыналарды көрсетеді.

MI өлшемі ең жақсы орташа нәтиже беруі мүмкін. Бұл тұрақты фразеологиялық сөзтіркестерді, сондай-ақ тиісті атаулар коллокат ретінде әрекет ететін тіркестерді, сондай-ақ төмен жиілікті арнайы терминдерді ажыратуға мүмкіндік береді. T-score өлшемін қолданудың кемшіліктері, ең алдымен, жиілікті коллокат-сөздермен, атап айтқанда, көмекші сөздермен анықтап көрсететіндігімен байланысты. Сондықтан, t-score үшін ең жиі кездесетін сөздерді «жою» үшін тоқтатым-сөздерінің тізімін орнату керек, олардың тіркесімдері әрдайым кестенің жоғарғы жағында болады: көмекші сөздер, есімдіктер немесе жалғаулықтар. Алайда, бұл басқа өлшемдерге де қатысты.

Лемма немесе сөзтұлғасын іздеу кезінде статистикалық өлшемдерде ескеру керек пе деген сұрақ ашық күйінде қалады. Сондай-ақ, коллокациялардың негізін құрайтын құрылымдық синтаксистік формулалар мен семантикалық шектеулерді ескеру қажет.

Болашақта үлкен корпуста әдістің тиімділігін тексеру жоспарлануда.

Алғыс

Жұмыс Қазақстан Республикасы Білім және ғылым министрлігі Ғылым комитетінің қаржылық қолдауымен орындалды (№AP09259309).

Әдебиет

[1] Сысоев П.В. Лингвистический корпус, корпусная лингвистика и методика обучения иностранным языкам // Иностранные языки в школе. 2010. № 5. С. 12-21.

[2] Сысоев П.В. Лингвистический корпус в методике обучения иностранным языкам // Язык и культура. 2010. № 1 (9). С. 99-111.

[3] Чернякова Т.А. Методика формирования лексических навыков студентов на основе лингвистического корпуса: автореф. дис. ... канд. пед. наук. М., 2012.

[4] Рязанова Е.А. Методика формирования грамматических навыков речи студентов на основе лингвистического корпуса: автореф. дис. ... канд. пед. наук. М., 2012.

[5] Pecina P. Lexical Association Measures. Collocation Extraction. Prague: Institute of Formal and Applied Linguistics, 2009.

[6] Atkins S. and Rundell M. The Oxford Guide to Practical Lexicography. Oxford University Press, 2008.

[7] Kilgarriff A. Collocationality (and how to measure it) // Proceedings of the Euralex International Congress. Torino, 2006.

[8] Krishnamurthy R. & Keith B. 2006. Collocations Encyclopedia of Language & Linguistics. Oxford: Elsevier. P. 596–600.

[9] Смағұлова Г. С 52 Мағыналас фразеологизмдер сөздігі /Гүлдархан Смағұлова. - Алматы: «Елтаным баспасы», 2010 жыл. – 252 бет.

[10] Қазақ әдеби тілінің сөздігі. Он бес томдық. 1-том / Құраст. Т.Жанұзақ, С.Омарбеков, Ә.Жүнісбек және т.б. – Алматы, 2011.

[11] Иорданская Л. Н., Мельчук И. А. Смысл и сочетаемость в словаре. М.: 2007.

[12] Ахманова О. С. Словарь лингвистических терминов, М.: 1966.

[13] Борисова Е. Г. Коллокации. Что это такое и как их изучать. М.: 1995. (Борисова 1995a).

[14] Evert S. The Statistics of Word Cooccurences Word Pairs and Collocations. PhD thesis. Institut für Maschinelle Sprachverarbeitung (IMS), Universität Stuttgart: 2004.

[15] Church K., Hanks P. Word association norms, mutual information, and lexicography // Computational Linguistics, 1996, № 16(1), P. 22–29.

[16] Kilgarriff A., Rychly P., Smrz P., Tugwell D. The Sketch Engine // Proceedings of the Eleventh EURALEX International Congress. Lorient, 2004. P. 105–116.

ANALYZING AND CLASSIFYING MEMES BY CONTENT

Azamat Moldabek[1], Muratbay Almurzayev[1], Pavel Lerman[1], Iskander Akhmetov[1,2], Rustam Mussabayev[2], Alexander Krassovitskiy[2]
[1] *Faculty of Information Technology, Kazakh-British Technical University, Almaty, Kazakhstan p_lerman@kbtu.kz https://kbtu.edu.kz/kz*
[2] *Institute of Information and Computational Technologies, Pushkin str. 125, Almaty, Kazakhstan i.akhmetov@ipic.kz http://iict.kz*

Abstract *In this work we present a new way to solve challenging task for not only artificial intelligence but also for average human being. The challenge is to detect hate speech in multimodal memes. The problem is challenging because data is constructed such that unimodal models do not perform well, and only multimodal models can achieve good results. "Benign confounders" are also in the dataset to make it hard for unimodal models. The task requires subtle reasoning yet is straightforward to evaluate as a binary classification problem. Since the challenge has been published, many people tried to solve it and the results are satisfying, but best remedies of tech problem remain difficult to understand. We purpose a new more simple way to solve the problem and yet our model do not fall far behind the best solutions. We find that state-of-the-art methods perform poorly compared to humans, illustrating the difficulty of the task and highlighting the challenge that this important problem poses to the community.*

I.Introduction. To solve the problem, we have explored some papers about hate speech detection, image captioning since we will be extracting information from the images we have and then put the descriptions and text from the image together, you may explore more about data in the next section.

The field of computer vision has made remarkable progress in object detection, image classification and image captioning over the last few decades, with rigid deep learning algorithms now capable of classifying thousands of images using large-scale photo collections. Since 2010 when first ImageNet competition [1] was held computer vision technologies have been dramatically evolved. One of the huge features of a use machine learning in computer vision is transfer learning which is now used in almost any computer vision problem. Kornblith, Simon Shlens, Jonathon Le, Quoc V in their work [2] they gave several answers to relevant question in computer vision technologies, especially transfer learning methods were discussed, as a conclusion they have written that computer vision models that use ImageNet pre-trained models are not overfit to ImageNet dataset, and models that perform better in ImageNet dataset may not bring performance improvement for models that are used in other problems when transfer learning method is used. Alex Krizhevsky, Ilya Sutskever, Geoffrey Hinton in [3] propose a model based on deep convolutional neural networks which is trained on ImageNet dataset. In their work they justified every step of the process, starting with dataset, neural networks' architecture, nonlinear ReLU as a activation function and ending with data augmentation and dropout methods. ImageNet models are often used for transfer learning, one of the examples of TL can be [4], in the paper they study realization of various methods for classification of paintings into art eras. They also provide evaluation of the effect of training set sizes on convolutional neural networks that are trained with and without additional data. As a result, pre-trained models' outperformance is highlighted. When deep neural networks are in use for computer vision problem, there are several methods come along to improve the model's

performance [5], [6]. First work discusses a novel data augmentation path where small shifting may increase misclassification rate, as a remedy they use iterative trust-region approximations which shows better performance than other model which is trained on a raw data only, without data augmentation. In the second work improving convolutional neural networks via combined unsupervised and supervised methods is discussed. Difference between these two is that while in supervised learning the model is not provided with the answer output, in unsupervised learning we assume that there is a difference between classes in our dataset and we do not provide our model with the output and let it classify the data by clusters. The paper uses both methods above, it employs unsupervised learning to improve the performance of supervised learning. In papers [7], [8] depth of neural networks and problems that it brings are discussed. One agrees on that the deeper gets neural networks the better its performance becomes; however, the accuracy can get worse rapidly if the depth is exceeded some unknown level. As a solution they suggest a framework called deep residual learning and gets results on ImageNet dataset. Overall, the results show that deep residual neural networks are easy to optimize and may boost accuracy by the depth gets deeper. Other work proves that very deep models can show great performance on small dataset using as long as the image has good quality so that it will not get ruined as the model goes deeper. The main idea is to train deep model to small dataset through Batch Normalization and using robust dropout layers.

II.Literature review. Nowadays, entertaining pictures with captions called "memes" are very common on social networks. Memes are information (links, texts, pictures, even colloquial constructs), usually transmitted by users to each other through the network. This is usually done for entertainment purposes, but other information, including of a provocative or hateful nature, can be disseminated in the same way. In our work, we will classify memes into positive and hateful. To do this, we need to define some things: define the text (positive or hateful), recognize the picture (what or who is on it and in what interpretation) and compare the picture with the text.

Figure 1. Memes example

In Figure 1, we see 3 memes in the first row. Consider them:

1. Positive inscription, but when combined with a picture of a skunk, this text becomes not entirely pleasant.

2. This text combined with a rose makes this meme positive.

3. If you slightly change the text in the picture with a skunk, then the meme becomes positive and funny.

At the stage of defining hate speech detection, we must define the text. We studied some of the methods that were used in the articles and stopped our own on the BERT model. In many articles, the BERT model showed better results compared to the others (fast text [9], logistics regression [10], SVM[10], etc.)

Bidirectional Encoder Representations from Transformers (BERT), is a language model that is pre-trained with a very large corpus to learn deep bidirectional representations developed by Google. BERT is the first fine-tuning based representation model that achieves state-of-the-art performance on a large suite of sentence-level and token-level tasks, outperforming many task-specific architectures [11].

We introduce BERT and its detailed implementation in this section. There are two steps in our framework: pre-training and fine-tuning. During pre-training, the model is trained on unlabeled data over different pre-training tasks. For fine-tuning, the BERT model is first initialized with the pre-trained parameters, and all the parameters are fine-tuned using labeled data from the downstream tasks. Each downstream task has separate fine-tuned models, even though they are initialized with the same pre-trained parameters. A distinctive feature of BERT is its unified architecture across different tasks. There is minimal difference between the pre-trained architecture and the final downstream architecture.

BERT's Architecture

The BERT architecture builds on top of Transformer. We currently have two variants available:

BERT Base: 12 layers (transformer blocks), 12 attention heads, and 110 million parameters

BERT Large: 24 layers (transformer blocks), 16 attention heads and, 340 million parameters

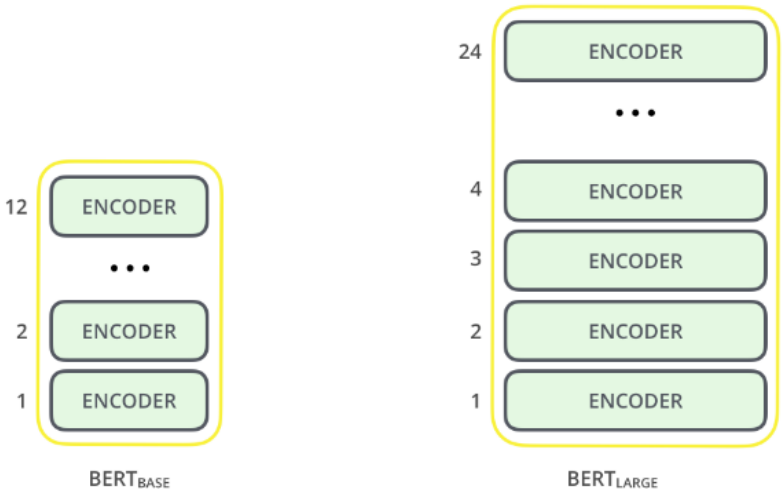


Figure 2. BERT's Architecture

Text Preprocessing

The developers behind BERT have added a specific set of rules to represent the input text for the model. Many of these are creative design choices that make the model even better [11].

For starters, every input embedding is a combination of 3 embeddings:

Position Embeddings: BERT learns and uses positional embeddings to express the position of words in a sentence. These are added to overcome the limitation of Transformer which, unlike an RNN, is not able to capture “sequence” or “order” information.

Segment Embeddings: BERT can also take sentence pairs as inputs for tasks (Question-Answering). That’s why it learns a unique embedding for the first and the second sentences to help the model distinguish between them. In the above example, all the tokens marked as EA belong to sentence A (and similarly for EB).

Token Embeddings: These are the embeddings learned for the specific token from the WordPiece token vocabulary.

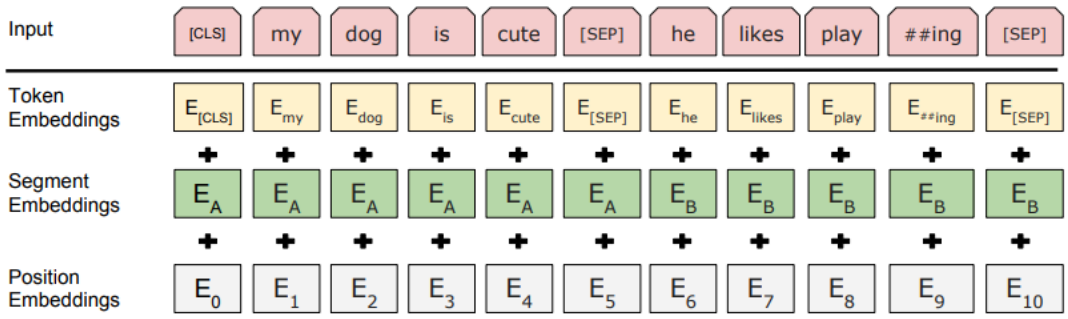


Figure 3. BERT embedding

Moreover, most existing works based on multimedia contents use a pre-trained deep CNN like VGG19 [12] to obtain general visual representations and fuse them with text information.

Deep learning based methods use deep artificial neural networks to learn abstract feature representations from input data through its multiple stacked layers for the classification of hate speech. The input can be simply the raw text data, or take various forms of feature encoding, including any of those used in the classic methods. However, the key difference is that in such a model the input features may not be directly used for classification. Instead, the multi-layer structure can be used to learn from the input, new abstract feature representations that prove to be more effective for learning. For this reason, deep learning based methods typically shift its focus from manual feature engineering to the network structure, which is carefully designed to automatically extract useful features from a simple input feature representation. Indeed, we notice a clear trend in the literature that shifts towards the adoption of deep learning based methods and studies have also shown them to perform better than classic methods on this task [13].

Note that this categorisation excludes those methods [14], [15] that used Deep Neural Network to learn word or text and subsequently apply another classical classifier (e.g., SVM, logistic regression) to use such embeddings as features for classification.

III. Data and Methodologies. The problem is to detect hate speech in memes with texts, data was gathered and labeled by Facebook AI team containing 10,000 images with

two classes, here is an example of memes that have similar texts but different images making them differ in classes they are in, this is one of the examples what makes the task challenging:

Figure 4. Different classified memes with the same text

To solve the problem, we propose two staged model, in first we caption the image extracting information out of it, after we combine extracted description of an image with the text that is written in the image, so we get something like this: "In the picture a skunk is smelling the grass. And the text says: love the way you stink today". After we have combined the generated captions with the text, we pass it to the classifier that decides if the meme is hateful or not. The scheme is below:

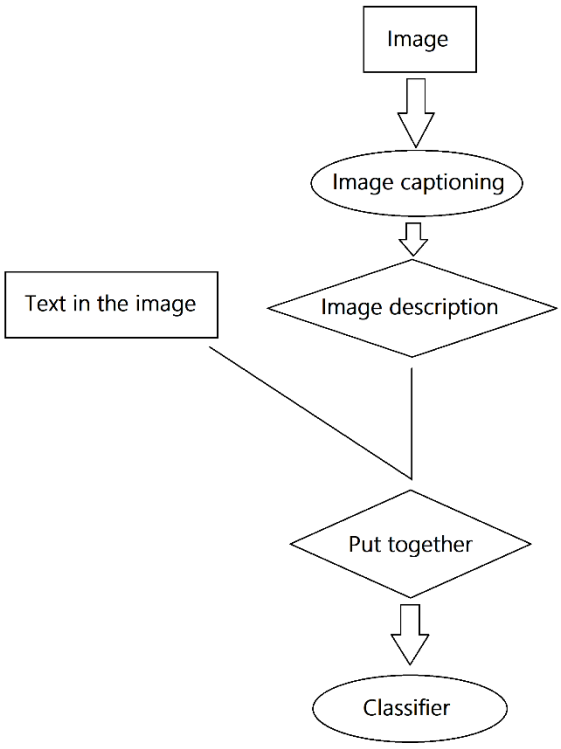


Figure 5. Model scheme

IV. Metrics and results. The data is split into 2 classes, corresponding to hateful and not hateful, overall there are 10000 images and 38 per cent of them are hateful. To measure performance we used balanced accuracy and AUC metrics since our data is not balanced.

These metrics are calculated as follows:

$$Balanced\ accuracy = \frac{TPR + TNR}{2}$$

$AUC = \int TPR(T)FPR^{-1}(T)dT$ - where T is classification threshold.

As a loss function for optimization cross-entropy loss function is used. Cross-entropy loss function is commonly used for classification tasks in machine learning. The implementation looks as following:

$$H_p(q) = -\frac{1}{N}\sum y_i * logp(y_i) + (1 - y_i) * log1 - p(y_i)$$

This is the loss function that our model is trying to minimize in order to shrink the difference between true distribution of output and the distribution that is predicted by the model. The true and predicted distribution are defined by $y_i$and $p(y_i)$ respectively. As long as we have only 2 classes it is obvious that the true distribution is binary, therefore the model that minimized loss function as possible to 0 must give in output 100 per cent certainty about the prediction.

The results we got are not the best, although high performance of the models were not expected since we were using simplified multimodal model. In figures 6, 7 and 8 loss function, accuracy and AUC values by number of epochs are shown. The model seems to get overfitted as long as loss function values of training and validating is decreasing and increasing respectively as number of epochs passes over 20.

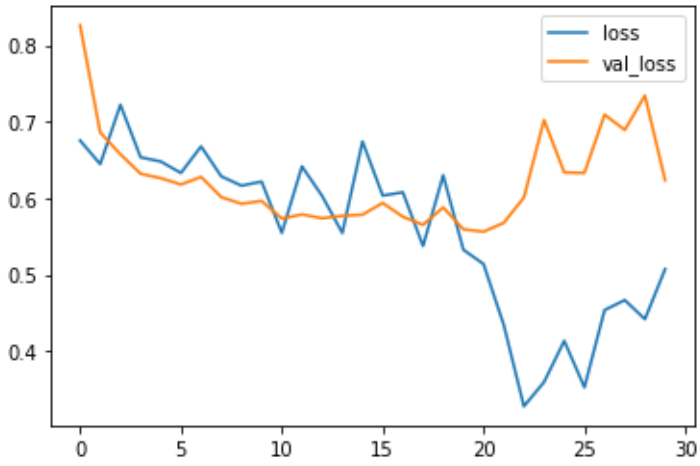


Figure 6. Cross-entropy loss function on training and validation sets

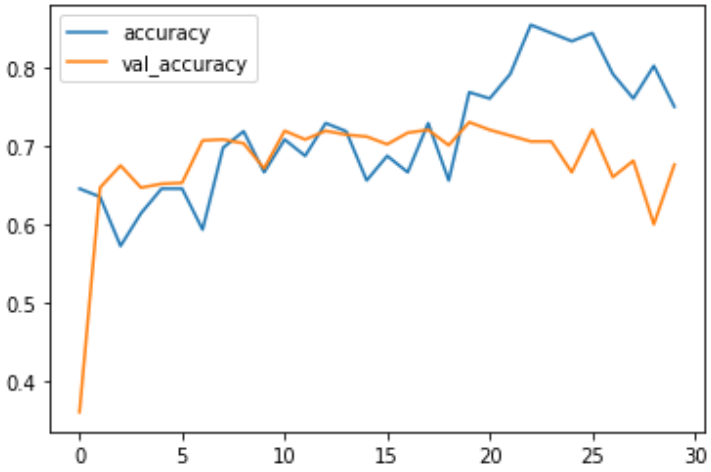


Figure 7. Accuracy on training and validation sets

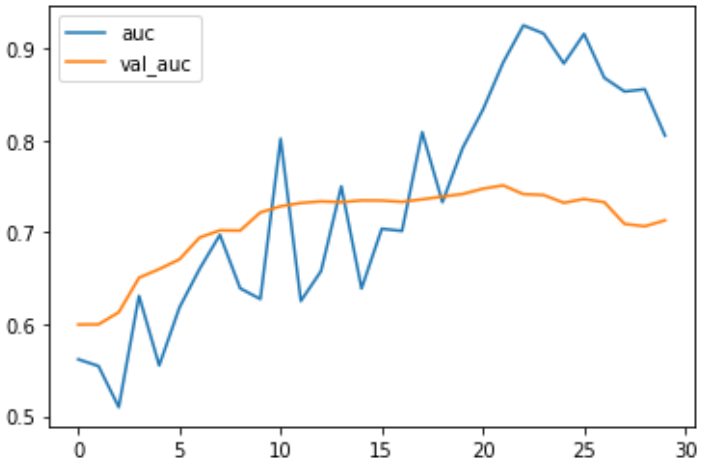


Figure 8. AUC value on training and validation sets

We also have been holding test set for final evaluation, accuracy on test set is 0.71 and AUC value is 0.77, these results are not bad, since the best model that have been developed so far shows 0.80 AUC value.

V. Conclusion. In this work, we tried solve a challenge centered around detecting hate speech in multimodal memes. Hate speech is an important societal problem, and addressing it requires improvements in the capabilities of modern machine learning systems. Still, our current state-of-the-art multimodal models perform relatively poorly on this dataset, with a large gap to human performance, highlighting the challenge's promise as a benchmark to the community. We hope that this work can drive progress in multimodal reasoning and understanding, as well as help solve an important real-world problem.

VI. Acknowledgment. This research is conducted within the framework of the grant num. AP09058174 ``Development of language-independent unsupervised methods of semantic analysis of large amounts of text data".

References

[1] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. ImageNet: A large-scale hierarchical image database. 2010.

[2] Simon Kornblith, Jonathon Shlens, and Quoc V. Le. Do better imagenet models

transfer better? In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2019.

[3] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E. Hinton. Im- ageNet classification with deep convolutional neural networks. In Advances in Neural Information Processing Systems, 2012.

[4] Christian Hentschel, Timur Pratama Wiradarma, and Harald Sack. Fine tuning CNNS with scarce training data - Adapting imagenet to art epoch classification. In Proceedings - Interna- tional Conference on Image Processing, ICIP, 2016.

[5] Alhussein Fawzi, Horst Samulowitz, Deepak Turaga, and Pascal Frossard. Adaptive data augmentation for image classification. In Proceedings - International Conference on Image Processing, ICIP, 2016.

[6] Kien Nguyen, Clinton Fookes, and Sridha Sridharan. Improving deep convolutional neural networks with unsupervised feature learning. In Proceedings - International Conference on Image Processing, ICIP, 2015.

[7] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2016.

[8] Shuying Liu and Weihong Deng. Very deep convolutional neural network based image classification using small training sample size. In Proceedings - 3rd IAPR Asian Conference on Pattern Recognition, ACPR 2015, 2016.

[9] Ashwin Geet D'Sa, Irina Illina, and Dominique Fohr. BERT and fastText Embeddings for Automatic Detection of Toxic Speech. Proceedings of 2020 International Multi-Conference on: Organization of Knowledge and Advanced Technologies, OCTA 2020, 2020.

[10] N. D.T. Ruwandika and A. R. Weerasinghe. Identification of hate speech in social media. 18th International Conference on Advances in ICT for Emerging Regions, ICTer 2018 - Proceedings, pages 273–278, 2019.

[11] Jacob Devlin, Ming Wei Chang, Kenton Lee, and Kristina Toutanova. BERT: Pre-training of deep bidirectional trans- formers for language understanding. NAACL HLT 2019 - 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies

- Proceedings of the Conference, 1(Mlm):4171–4186, 2019.

[12] Karen Simonyan and Andrew Zisserman. Very deep con- volutional networks for large-scale image recognition. 3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings, pages 1–14, 2015.

[13] Bj¨orn Gamb¨ack and Utpal Kumar Sikdar. Using Convolutional Neural Networks to Classify Hate-Speech. (January):85–90, 2017.

[14] Quoc Le and Tomas Mikolov. Distributed representations of sentences and documents. 31st International Conference on Machine Learning, ICML 2014, 4:2931–2939, 2014.

[15] Yashar Mehdad and Joel Tetreault. Do Characters Abuse More Than Words? (September):299–303, 2016.

EXPERIMENTS WITH FUZZY CLUSTERING ON TOPIC MODELING

Gulmira Tolegen, Alymzhan Toleu, Rustam Mussabayev
gulmira.tolegen.cs@gmail.com, alymzhan.toleu@gmail.com, rmusab@gmail.com
Institute of Information and Computational Technologies
Almaty, Kazakhstan

Abstract. *This paper presents a fuzzy clustering method for topic modeling. The main idea of this is to divide the searching space into small sub-searching spaces. The results show that the method performs well in coherence score and the space-reduction strategy leads the model takes less running time than the exiting approach.*

1. Introduction

Topic modeling is the task of identifying hidden structures (topics) in a large collection of documents automatically. This is an efficient way of a corpus analysis when you want to know what topics the targeted large corpus is about, or you try to filter out or search some of the specified topic-related documents. Also, in social media analysis, instead of looking for each tweet/post, topic model can provide the population level statistics: What proportion of facebook/twitter users have ever talked healthcare event, etc.

After running a topic model on data, the topic model provides you clusters of words (topic), each of which is a ranking of all unique words in the documents by relevance to topic. Take top N most relevant words to describe the topic then get the relevant document by these topics. Early work on topic modeling is Latent semantic analysis (LSA)[1], which is an approach of using singular value decomposition (SVD) that tries to find the best low rank approximation of an occurrence matrix. While these approaches are have seen a resurgence adding probabilistic feature renamed probabilistic latent semantic analysis (pLSA) [2] in recent years. Instead of using SVD, the core idea of PLSA is to find a probabilistic model that can generate concurrence matrix we observed. LDA[4] is another more advanced approach which is a Baysian version of PLSA, in particular, it uses dirichlet priors for document-topic and topic-word distribution. Basically, these approaches are trying to find two document-topic and topic-word matrices in a large space: $D(\#documets) \times N(\#words) \times T(\#topics)$, which can better describe the co-occurrence matrix.

In this paper, we present an experimental work of topic modeling by reducing aforementioned space with fuzzy clustering algorithm. The core idea is to divide the large search space into two sub-spaces: $W(\#words) \times T(\#topics)$ and $D(\#document) \times T(\#topics)$. First of all, we find the possible topics of documents with fuzzy clustering algorithm in a sub-space $W \times T$, then calculate the correlations between document and topic in another sub-space $D \times T$. These reduction scale is notable, especially in big data scenario. Fuzzy clustering algorithms is applied to calculate the topics and the Jaccard index is used for calculating document-topic matrix. We compare these approach with LDA, which consider as the strong baseline. Evaluation results show that fuzzy clustering approach produces higher performance with the number of most relevant words of topic get larger, while LDA performs well when take less number relevant words for each topic.

The rest of the paper is organized as follows: Section 1 presents introduction and Section 2 give related work about topic modeling; Section 3 describe the method based on fuzzy clustering and follows with experimental Section 4 and we conclude the work in Section 5.

2. Related Work

Existing approaches to topic modeling are mixture of unigram [3], probabilistic latent semantic analysis (PLSA) [2], Latent Dirichlet allocation (LDA)[4] and Additive regularization of topic model (BigARTM) [5] and among them, the last two approaches can be considered the state-of-the-art in this field.

LDA is a two-level Bayesian generative model: i) the first one is to model topics distribution over words and ii) another one is to model documents distribution over topics. The one assumption of LDA is to apply a prior from Dirichlet distribution to generate the above mention distributions, which overcomplicate the model when applying the Bayesian inference [6, 7]. There are many other variations of LDA [8,9,10,11] have been proposed, most of them tried to solve the limitation of the original LDA under the LDA's framework, but these overcomplicate the algorithms.

BigARTM [5] is a non-Bayesian model that attempts to solve the problems that appeared in the LDA model. It considers the topic modeling as problem-oriented matrix factorization and the parameters are trained through expectation–maximization (EM) algorithm adding several task-specific regularization terms and the model parameters start with random initialization. In the point of BigARTM, the parameters of LDA more likely to be initialized with Dirichlet distribution and trained with the single objective function.

3. Method

3.1. Fuzzy Clustering

Clustering is a process of grouping tokens into clusters and keep the intra-distances as

small as possible, while keep inter-distances as large as possible. In other words, tokens in the same cluster should be similar to each other and the tokens belong to different clusters should be dissimilar. Fuzzy clustering, aka soft clustering, in contrast to hard clustering, it can assign one token into more than one cluster. Algorithm 1 describe the fuzzy k-means used in this work.

Algorithm 1. Fuzzy K-means clustering.

Input: $\boldsymbol{X} = (x_1, x_2, \dots, x_N)$ is a finite collection of words and K is the number of cluster.

Output: a list of centroids $C = (c_1, \dots, c_K)$ and the partition matrix W.

Random initialize the partition matrix $W = w_{ij} \in [0,1], i = 1, \dots, N \; and \; j = 1, \dots, K$

Until there are no changes in any mean:

Calculate cluster centroids as

$$c_j = \frac{\sum_{i=1}^{N} W_{ij} x_i}{\sum_{i=1}^{N} wij}$$

Update the membership function:

$$W_{ik} = \frac{1}{\sum_{j=1}^{K} \frac{\|x_i - c_k\|}{\|x_i - c_j\|}^{\frac{2}{m-1}}}$$

Minimize following objective function:

$$argmin \sum_{i=1}^{N} \sum_{k=1}^{K} w_{ik} \|x_i - c_k\|$$

3.2. Fuzzy Clustering-based Topic Modeling

We treat topic modeling as word and document clustering task, indeed, the output of the existing approaches (LDA) are the clustered bag-of-words and the clustered documents relevant to word-clusters (topics).

Clustering-based topic models consists of three steps: 1) tokens representation; 2) topic identification and 3) document-topic correlations.

In the first step, we extract all the distinct words from documents, and represent each word with a distributional vector from co-occurrence matrix. The vocabulary size of a collection of document is large normally, in order to have better topics, the simple frequency-filtering is used. In the second step, we clustering these words and the final clusters considered as topics.

Then, we calculate the correlation between documents and topics with Jaccard metric:

$$J(D,T) = \frac{|D \cap T|}{|D \cup T|}$$

4. Experiments

4.1. Data Set

We crawled Russian web text from the media[1], in which the titles, content, publish-date, #view, #comment and etc. information are collected. We pre-process the content before the experiments, namely stopwords removing, punctuations cleaning and stemming.

Table 1: Statistics of the original corpus.

#documents	#unique tokens	#filtered words
186,183	695,581	19,628

Table 1 presents statistics of the corpus, as shown, the number of the unique tokens is large, clustering these number of tokens into a small number of topics leads low purity of topics. Thus, we filtering the unique tokens with simple strategy only keep tokens > 100 frequency.

4.2. Evaluation Metrics

Topic coherence [12] is a widely used measurement for topic modeling, which is an average score of pairwise word similarity of M-most relevant words of topic. There are several versions of topic coherence: Umass and Cv coherence score.

Umass coherence defines word pairs with point-wise mutual information (PMI):

$$Umass(x_i, x_j) = \log \frac{Count(x_i, x_j) + \varepsilon}{Count(x_j)}$$

Cv coherence calculated via normalized point-wise mutual information(NPMIs).

4.3. Results

We conducted several experiments to evaluate the fuzzy clustering, the first one is to compare the coherence score of these methods and the second is to check the optimal topic number. Unless stated, the topic number of the following results is set to 30.

Table 2 and Table 3 shows the experimental results of the Umass and Cv coherence scores. *M* defines how many relevant words used in topics.

Table 2: Umass coherence.

Method	**M=10**	**M=30**	**M=50**	**M=70**	**M=100**
LDA	-2.27	-3.01	-3.42	-3.67	-3.87
k-means	-13.17	-13.41	-13.3	-13.5	-13.5
fuzzy k-means	-15.46	-15.94	-16.01	-16.08	-15.98

Table 3: Cv coherence.

Method	**M=10**	**M=30**	**M=50**	**M=70**	**M=100**
LDA	0.64	0.59	0.57	0.55	0.53
k-means	0.38	0.56	0.61	0.63	0.65
fuzzy k-means	0.47	**0.68**	**0.74**	**0.76**	**0.77**

As shown in Table 2, LDA outperforms all other methods regardless of what *M* values it takes and surprisingly standard k-means is better than the fuzzy one in Umass coherence. It is easy to observe from Table 3 that the performance more different than previous. When using the 10 most relevant words to describe topics the LDA performs best, second is fuzzy k-means and follows by k-means. In the case of M > 10, the fuzzy k-means becomes the well performing model, the possible reason behind on this is that, the Cv coherence score is based on normalized point-wise mutual information. Fuzzy k-means also outperforms k-means in Cv coherence.

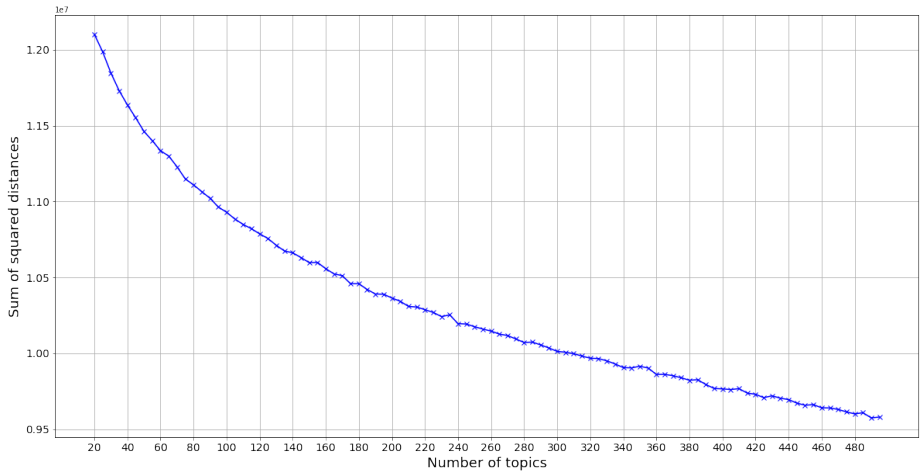


Figure 1. Sum of squared distances.

In order to identify the optimal number of topics, we conducted 500 times experiments with k-means, and the topic number is set from 1 to 500. The purpose is to use elbow method to identify the optimal topic numbers. Figure 1 plots how the curve

behaves with different topic numbers. It is clearly seen that the sum of squared distances (SSD) is decreasing as the number of topics growing. We expected that in some degree of topic number the SSD should grow, unfortunately, this not happened in this experiment. In order to further analyze these, we used average silhouette scores and conducted the same experiments. The results plotted in Figure 2.

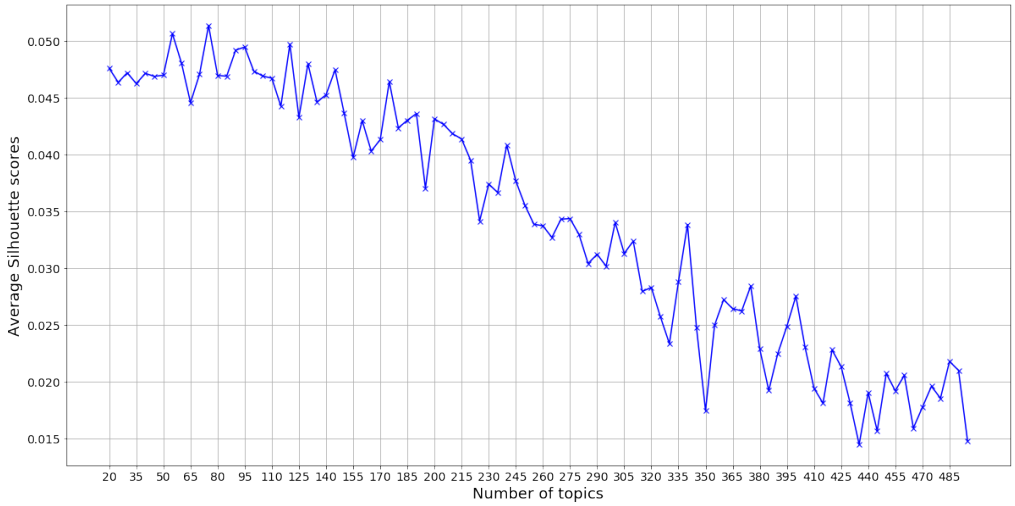


Figure 2. Average Silhouette scores.

It shown that in globally the curve is decreasing during these process, but in local region, there are some fluctuation like 335(up) and 350(down) position, which may can provided little information for choosing the optimal topics. As we know, identifying the optimal topic number is still an open task in topic modeling, and the strategy of identifying fine/coarse topics is also different.

Table 4: Comparisons of running time.

Method	**Time,m**
LDA	33.15m
k-means	3.11m
fuzzy k-means	4.29m

Table 4 presents the running time of different methods, it can be clearly seen that the running of clustering-based model takes less time than LDA due to the decomposed sub-searching space.

5. Conclusion

In this paper, we present experimental research work of doing topic modeling with fuzzy clustering. Unlike existing approaches that try to produce documents-topics and topics-words matrix with matrix decomposition method or with EM algorithm in large search space: D(#documets) × N(#words) × T(#topics). We used the fuzzy clustering algorithm for topic modeling and tried to solve the task in two sub-space: W(#words) × T(#topics) and D(#document) × T(#topics). The result shows that fuzzy k-means

outperforms k-means in cv coherence and the sub-space reduction effect is significant that enables the model to take less running-time than others.

Acknowledgement

This research has been conducted within the framework of the grant num. AP09259324 “Advanced topic modeling via clustering by variable neighborhood search”.

References

1. Scott Deerwester, Susan Dumais, Thomas Landauer, George Furnas, and Richard Harshman. Indexing by latent semantic analysis. Journal of the American Society of Information Science, 41(6):391–407, 1990.

2. T. Hofmann. Probabilistic latent semantic indexing. Proceedings of the Twenty Second Annual International SIGIR Conference, 1999.

3.K. Nigam, J. Lafferty, and A. McCallum. Using maximum entropy for text classification. IJCAI- 99 Workshop on Machine Learning for Information Filtering, pages 61–67, 1999.

4. David M. Blei, Andrew Y. Ng, and Michael I. Jordan. 2003. Latent Dirichlet allocation. Journal of Machine Learning Research, 3(Jan):993–1022.

5.Vorontsov, K.V.: Additive regularization for topic models of text collections. Doklady Mathematics 88(3) (2014).

6. Shashanka, M., Raj, B., Smaragdis, P.: Sparse overcomplete latent variable decomposition of counts data. In Platt, J.C., Koller, D., Singer, Y., Roweis, S., eds.: Advances in Neural Information Processing Systems, NIPS-2007. MIT Press, Cambridge, MA (2008) 1313–1320.

7. Wang, C., Blei, D.M.: Decoupling sparsity and smoothness in the discrete hierarchical dirichlet process. In: NIPS, Curran Associates, Inc. (2009) 1982–1989.

8. Ke Zhai, Jordan Boyd-Graber. Online Latent Dirichlet Allocation with Infinite Vocabulary Proceedings of the 30th International Conference on Machine Learning, PMLR 28(1):561-569, 2013.

9. Jagarlamudi, Jagadeesh et al. “Incorporating Lexical Priors into Topic Models.” EACL (2012).

10. Yuan Zuo, Jichang Zhao, Jichang Zhao, Ke Xu. Word network topic model: a simple but general solution for short and imbalanced texts. Knowledge and Information SystemsAugust 2016 https://doi.org/10.1007/s10115-015-0882-z.

11. Blei D., M,Lafferty JD (2006). Dynamic topic models. In:ICML, pp113–120 .

12. D. Newman, J.H. Lau, K. Grieser, and T. Baldwin. Automatic evaluation of topic coherence. In Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the Association for Computational Linguistics, HLT 2010, pages 100–108.

13. D. Mimno, H.M. Wallach, E. Talley, M. Leenders, and A. McCallum. Optimizing semantic coherence in topic models. In Proceedings of the Conference on Empirical Methods in Natural Language Processing, EMNLP 2011, pages 262–272.

SENTIMENT ANALYSIS OF KASPI PRODUCT REVIEWS

Jaxylykova Assel, Akhmetov Iskander, Yerassyl Kelsingazin
Email: aselya17.89@mail.ru, iskander.akhmetov@gmail.com,
e_kelsingazin@kbtu.kz
Institute of Information and Computational Technologies
CS MES RK, Kazakhstan,
Kazakh-British Technical University, Kazakhstan

Abstract

Customer reviews are the key to the success functionality for the companies. A producer will gain the true result of his products from the customer feedback. He can make necessary changes to his product according to the feedback. However, it is common to see when most client may inadequately overestimate or underestimate the mark. To avoid the confusion it is better to analyze the text. This paper focus on the sentiment feedback analysis and finding the relationship between reviews and ratings on the basis of data collected from "Kaspi.kz" marketplace. These data streams are cleaned and analyzed and reviews is got through opinion mining. We used several algorithms to find the best one. The experiments have shown 92% accuracy in the sentimental analysis.

I. INTRODUCTION

Nowadays, the quality of the product starts to become more important than the price of the product. In order for the business to live for a long time and so that the flow of customers does not decrease and their number and their gratitude only increase, you need to improve the quality of your product every time. In order to achieve this quality, not only the opinion of the seller is important, but also of the buyers. In many cases, the buyer's opinion should weigh more than the seller's. What should the seller do to achieve good quality for his product? Just by looking at the stars and reading the usual text, the seller will not be able to improve their product well enough, because different people can understand the same text in different ways. That's why, the seller can improve the wrong part of their product and make their product worse. Sentimental analysis can be applied here. The likelihood of correctly understanding the text that went through the sentimental analysis is higher than the usual text from buyers. Since we are in the market of Kazakhstan. The "Kaspi.kz" is a big player here. We decided to introduce sentiment analysis for him. The paperwork is done by Rajkumar S. Jagdale, et al. [1] the idea of classifying Amazon product reviews into positive and negative categories. The algorithm is based on Na¨ıve Bayes Classifier outperforms with an accuracy of 98.17% while Support Vector machine got accuracy 93.54 A paper published by Anto, Minara P et al. [2] focused on the technique of providing automatic feedback based on data collected from Twitter. These data streams are filtered and analyzed and feedback is obtained through opinion mining. Here they mainly analyze the data for mobile phones. The experiments have shown 80% accuracy in the sentimental analysis. A study was done by Vidisha M. Pradhan, et al. [3] on how a survey on sentiment analysis algorithms for opinion mining could enable extracting opinions from the internet and predict customer's preferences. From the preprocessed reviews opinion words and objects on which opinion is generated are extracted and any opinion mining technique is applied to find the polarity of the review. They classified opinion mining into three levels of granularities: Document level, Sentence level, and Aspect level. From the survey done in this paperwork, it can be concluded that

supervised techniques provide better accuracy compared to the dictionary-based approach. According to paperwork by M. Munir Ahmad [4] they are applied three approaches: Lexicon based techniques, Machine Learning based techniques and hybrid techniques (which combines lexicon based and machine learning based approach). Different training and datasets were used for the evaluation of these tool by the researchers i.e., movie reviews and product reviews, while some tools were tested on generic datasets and average accuracy of the tools were considered. Originality of our work is to analyze local marketplace reviews by using sentiment analysis. We analyzed related works and there was no such approach for this marketplace. Also, many of the text processing methods are adapted to the English language. That's why we will improve the method by focusing on the Russian language.

II. METHODS

In order to implement our approach, we need a voluminous data set from the "Kaspi.kz" marketplace. However, "Kaspi" prevents the traditional way of website parsing. For that reason a parser based on Json response was written using JavaScript programming languages. At all we collected more than ten thousand review units.

	Name	Rating	Positive	Negative	Comment
11636	Браслет Xiaomi Mi Band 3 черный	3	Качество хорошее, непромокаемый	Неудобный	В остальном всё хорошо
11637	Браслет Xiaomi Mi Band 3 черный	3	Уведомления мессенджеров не выходят. Ватсап, т...		
11638	Браслет Xiaomi Mi Band 3 черный	2	Не понравился то, что невозможно подключить к ...		

Fig. 1. Initial data set

We got unbalanced data set. Kaspi.kz allows customers to split their comments to the three different sections: positive, negative and comment. It makes it impossible to work with data, because many clients does not fully fill reviews. People are tend only to fill one of section that passionate about them. That is why we had to combine all three sections to one and call it "Review".

11634	Браслет Xiaomi Mi Band 3 черный	2	Капсула хорошо зафиксирована в ремешке Сыроват...
11635	Браслет Xiaomi Mi Band 3 черный	1	Я очень расстроен.
11636	Браслет Xiaomi Mi Band 3 черный	3	Качество хорошее, непромокаемый Неудобный В ос...
11637	Браслет Xiaomi Mi Band 3 черный	3	Уведомления мессенджеров не выходят. Ватсап, ...
11638	Браслет Xiaomi Mi Band 3 черный	2	Не понравился то, что невозможно подключить к...

11639 rows × 3 columns

Fig. 2. Combined data set

For algorithms implementation we should prepare our data set. We should remove all symbols except base Latin alphabet and Cyrillic. Delete functional parts of speech and stop-words. Next we should bring the words to their normal form and vectorize texts. It is significant, because we cannot perform classification algorithms over text: we have to make numeric representations. The scikit-learn library provides 2 different schemes that we can use. The CountVectorizer provides a simple way to both tokenize a collection of

text documents and build a vocabulary of known words, but also to encode new documents using that vocabulary. However, it is basic. For instance, the word “the” will appears many times and its large counts will be meaningless in the encoded vectors. An alternative is to calculate word frequencies, which we can achieve using TfidfVectorizer. Then based on rating value we added a new column ”sentiment”. If rating more than 3, sentiment is equal to 1, otherwise it equals to 0. It is important feature, because it is output value of our algorithms. After that using train test split function from sklearn library we divide our data set to train and test models. It automatically splits the data in 75/25 proportion: 75% for the training and 25% for the testing. It this work we are going to use 2 methods: SVC (SVM) and logistic regression. A. Baseline: Logistic Regression For first approach we use logistic regression, It is a statistical model used to predict the likelihood of an event occurring by comparing it to a logistic curve. This regression gives the answer in the form of the probability of a binary event (1 or 0). Using abstract concept pipeline we pass two values, and it will automatically complete them one after another before applying the final score. After we gave this algorithm a sample for training and test, at Figure 3 we got confusion matrix with four values. B. GridSearchCV: Logistic Regression The GridSearchCV creates a grid over the search space and evaluates the model for all of the possible hyper parameters in the space. This method is simpple Good in the sense that it is simple and makes it possible to see the results when using all possible parameters. However, it has a major disadvantage, it may be prohibitively expensive in computation time if model has many hyper parameters. C. Randomized Search CV: Logistic Regression In contrast with the GridSearchCV, Randomized Search CV uses

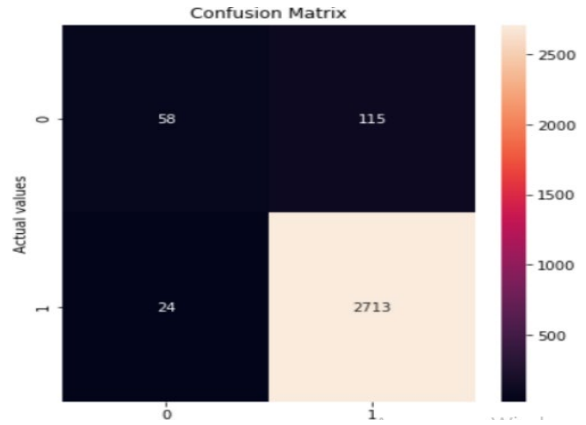


Fig. 3. Confusion matrix of Baseline Logistic regression

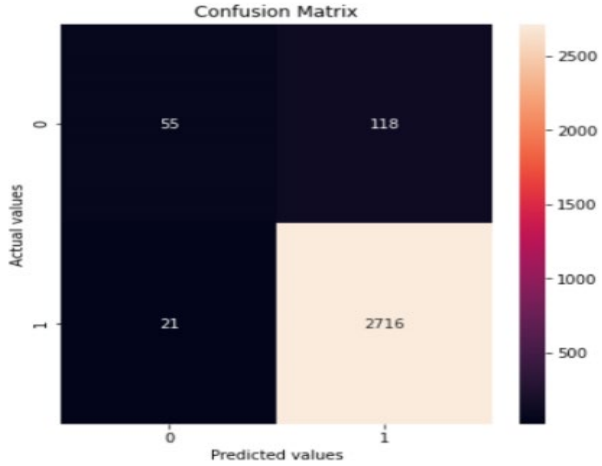


Fig. 4. Confusion matrix of Logistic regression with GridSearchCV

a random set of hyper parameters. It is mainly useful and solves GridSearchCV's problem, when there are many hyper parameters. In this method not all parameter values are tried out, but rather a fixed number of parameters from the specified distributions are used. The number of parameter settings that are used is specified by $n_iterparameter$.

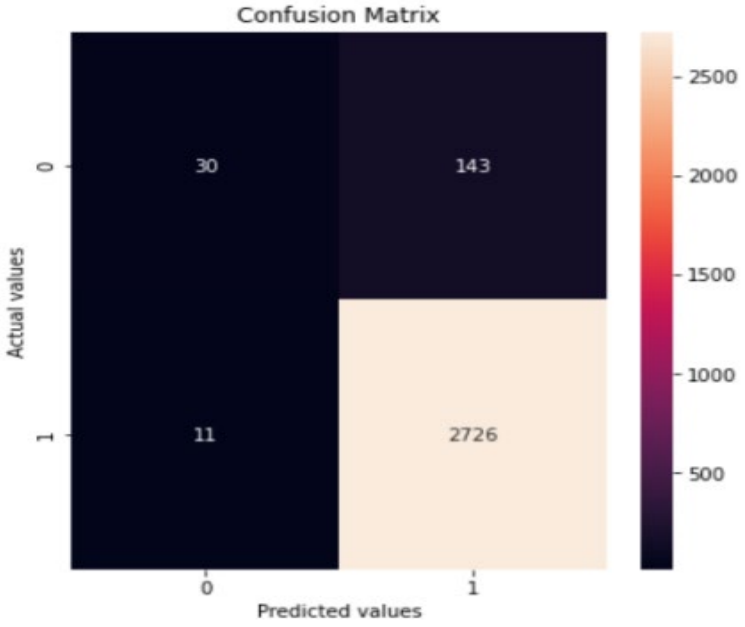


Fig. 5. Confusion matrix of Logistic regression with GridSearchCV

Support Vector Classifier [5] The implementation is based on libsvm. The fit time scales at least quadratically with the number of samples and may be impractical beyond tens of thousands of samples. For large datasets consider using LinearSVC or SGDClassifier instead, possibly after a Nystroem transformer.

III. RESULTS

The precision, recall and F-score metrics are used to find out the algorithm performance. Next formulas are used to determine accuracy

$$\text{precision} = \frac{TP}{TP+FP} \quad (1)$$

Precision shows how much we can trust classifier if it works correctly.

$$\text{recall} = \frac{TP}{TP+FN} \quad (2)$$

Recall shows how many true objects of the first class the algorithm selects, how many of them it works on

$$\text{F score} = 2 * = \frac{\text{precision} * \text{recall}}{\text{precision} + \text{recall}} \quad (3)$$

	Precision	Recall	Fscore
Baseline LR	0.96	0.99	0.98

GridSearch LR	0.96	0.99	0.98
RandomizedSearchCV LR	0.95	1.00	0.97
Baseline SVC	0.94	1.00	0.97
GridSearch SVC	0.94	1.00	0.97
RandomizedSearchCV SVC	0.94	1.00	0.97

Based on the results, it can be understood that at the moment the best algorithm is baseline logistic regression.

IV. CONCLUSION

Sentiment analysis is a highly effective tool for a business to not only take a look at the overall brand perception, but also evaluate customer attitudes and emotions towards a specific product line or service. This data-driven approach can help the business better understand the customers and detect subtle shifts in their opinions in order to meet changing demand. We parsed the data from the ”Kaspi.kz” marketplace. Then we preprocess it by using lemmatization, stemming techniques and eliminating the stop words. Then the data from the dataset are 11639 classified using logistic regression approach. In a further researches we will use larger data and other classification methods.

ACKNOWLEDGMENT

We gratefully acknowledge financial support of Institute of Information and Computational Technologies. (Grant AP09260670, Kazakhstan).

REFERENCES

1. Jagdale R. S., Shirsat V. S., Deshmukh S. N. Sentiment analysis on product reviews using machine learning techniques //Cognitive Informatics and Soft Computing. – Springer, Singapore, 2019. – С. 639-647.
2. Anto M. P. et al. Product rating using sentiment analysis //2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT). – IEEE, 2016. – С. 3458-3462.
3. Pradhan V. M., Vala J., Balani P. A survey on sentiment analysis algorithms for opinion mining //International Journal of Computer Applications. – 2016. – Т. 133. – №. 9. – С. 7-11.
4. Ahmad M. et al. Machine learning techniques for sentiment analysis: A review //Int. J. Multidiscip. Sci. Eng. – 2017. – Т. 8. – №. 3. – С. 27.
5. https://scikit-learn.org/stable/modules/generated/sklearn.svm.SVC.html sklearn documentation, 2021.

DESIGN OF ADAPTIVE SYSTEMS

Sabitov A.
aman_93s@list.ru
L.N. Gumilyov Eurasian National University, Kazakhstan, Nur-Sultan
Kintonova A. Zh.
aliya_kint@mail.ru
L.N. Gumilyov Eurasian National University, Kazakhstan, Nur-Sultan

Annotation. *Adaptive hypermedia (AG) systems form an individual user model and apply it to adapt to this user, adapting the content of the hypermedia page to the user's level of knowledge and goals, or offering the most appropriate hyperlinks for further navigation. This article presents the principles and approaches to the design of adaptive information systems. A method of implementation and criteria for adapting the system are proposed. Methods for adapting the interface and content of resources to the user level are proposed.*

Keywords: adaptive systems, a*daptation methods*, user model, adaptive learning, distance learning, educational platforms.

Adaptive systems

Recently, hypermedia systems have gained great popularity as a convenient means of accessing information, controlled by the user. Adaptive hypermedia is one of the lines of research in the field of adaptive user systems. The aim of these studies is to increase the functionality of hypermedia through its individualization. Adaptive hypermedia (AG) systems form a model of goals, preferences and knowledge of a particular user and use this in the process of interacting with the user to adapt to his needs.

We will call adaptive hypermedia systems (or adaptive hypermedia systems) all hypertext and hypermedia systems that reflect some user characteristics in the user model and apply this model to adapt various visual and content aspects of the system to the needs of the user[1].

Adaptive Hypermedia Methods and Techniques

Adaptation techniques use methods to ensure adaptation in existing AG systems. These techniques are part of the implementation level of AG systems. Each technique is characterized by a certain type of knowledge representation and a certain adaptation algorithm.

Adaptation methods are defined as generalizations of existing adaptation technologies. Each method is based on the idea of “pure” adaptation that can be conceptualized.

Here is a list of the main techniques for adapting the visual range and content of information resources

1. Changing the order of information resources in the current topic (in the current subject area)

2. Changing the navigation scheme of the theme and system based on user preferences or his adaptive model.

3. Formation of relevant ("interesting" to the user) sets of links to other information resources based on various adaptation schemes

a) Displaying a list of links to relevant resources, determining relevance based on a set of keywords in the user's model, the history of his visits, the semantic space of the current topic.

b) Listing of links to resources by keywords of the current resource

4. Highlighting links of the current educational level or the current level of complexity of the resource or links of the current subject area. Highlighting in a different color links of a higher level and lower level (within the offset). Highlighting links of the current level, but leading to other concepts (by keywords).

5. Hiding links falling out for or above the current level of the user or the complexity of the resource.

6. Hiding information fragments and highlighting them according to the same criteria

7. Adaptation of the interface. User choice of style. User customization of the interface for himself - the choice of modules and interface solutions of interest. Dynamic interface adaptation

8. Pop-up tips on keywords (defined by the author of the resource) - the basic concepts (concepts) of the resource[2].

The architecture of the adaptive system for managing information and educational resources Xite

Let's describe the structural logical model of the system. The proposed system model uses a multi-level data organization: at the highest logical level, an information system (adaptive hypermedia environment) is a set of sites - each site is a directed multigraph of content modules, or topics in terms of the Xite system (you can call them chapters, lectures or page groups) - content nodes of hypermedia space, subject areas of knowledge or information; at the middle level, each topic is described by a weighted directed multigraph of resources (pages, elementary units of the information system). At a lower level, each resource is an XML document, a composition of elementary information fragments, media resources (text, graphics, clips, data access points, etc.).

Resources are described by XML documents stored in the repository. They are a composition of media resources, with given characteristics of displaying media resources on a page, with a given order of appearance of these media resources, and are themselves subjects of the hypermedia space (that is, they have a name, description, and other characteristics).

Topics represent larger units of information space. In a sense, topics can be described as chapters or lectures, consisting of separate pages (resources). The topic includes at least one resource. *The topic* is set by a graph, the edges of which represent the relationship between resources - order, subordination, or some kind of navigation presets, for example, in the case of an educational module, this is a sequence of studying elementary resources to get an idea of the topic as a whole (that is, a set of elementary knowledge for obtaining a complex knowledge of the topic)[3].

User model

The User Model describes user characteristics, preferences, browsing history, forms abstract stereotyped user profiles. The user model is a key element in the process of adapting the information content and navigation space of the terminal; based on the user model, the system, using the specified rules, changes the content of resources and the screen interface.

The intelligent training course will be based on the ***adaptive model*** shown in Figure 1:

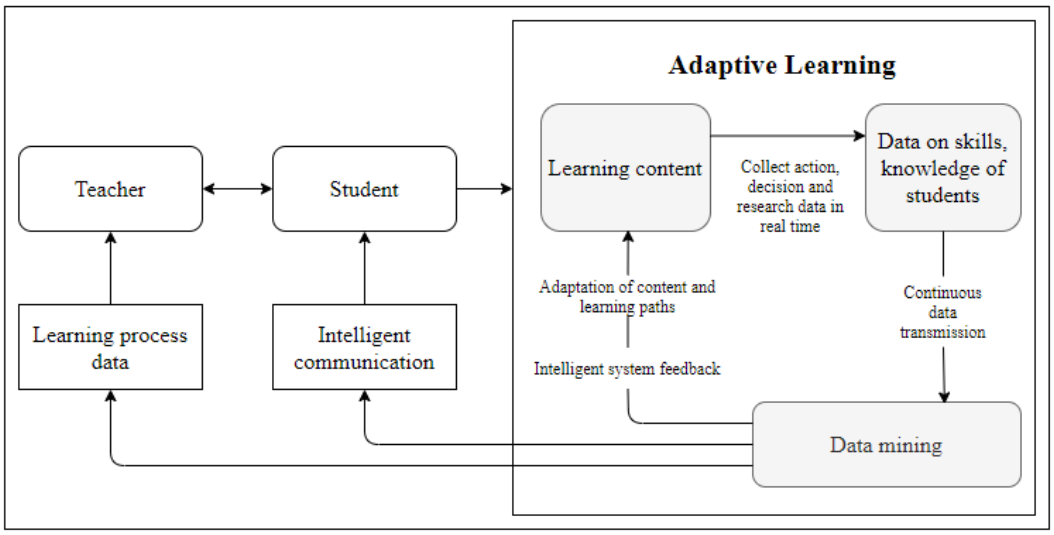


Fig.1 Model of adaptive learning

–**Data collection system:** collects and processes huge amounts of information about the student's knowledge.

– **Calculation block:** processes data in real time and analyzes in parallel for further use.

– **Personalization System:** Harnesses the power of data from the entire system to find the optimal strategy for each learner at each level.

– **Block of recommendations:** communicates the next steps, corrects goals, evaluates the strengths and weaknesses of the learner, etc.

– **Block of analytical forecasts:** predicts the speed and likelihood of achieving goals, the expected grade or score, the level of knowledge, etc.

– **Unified learning history:** personal statistics of the student.

– **Inference system:** expands the dataset and draws conclusions from it.

– **Psychometric unit:** evaluates the knowledge and skills of students, adjusts content parameters. With each new level, the information about the student becomes more accurate.

– **Learning strategy block:** evaluates learners' sensitivity to changes in teaching, pace, grading, etc.

– **Feedback block:** combines all this data and transfers it to the data collection system

–**Block of recommendations:** communicates the next steps, corrects goals, evaluates the strengths and weaknesses of the learner, etc.

–**Block of analytical forecasts:** predicts the speed and likelihood of achieving goals, the expected grade or score, the level of knowledge, etc.

–**Unified learning history:** personal statistics of the student.

–**Inference system:** expands the dataset and draws conclusions from it.

–**Psychometric unit:** evaluates the knowledge and skills of students, adjusts content parameters. With each new level, the information about the student becomes more accurate.

–**Learning strategy block:** assesses learners' sensitivity to changes in teaching,

pace, grading, etc.

–**Feedback block:** combines all this data and transfers it to the data collection system.

What user characteristics can be taken into account to ensure adaptation? Let us briefly describe some of the parameters of the user model that are derived from the above initial data.

Knowledge. *The user's level of knowledge* of a topic implemented in hyperspace is the most important characteristic. The level of knowledge is variable for each specific user. This means that the system using the user's knowledge must record changes in the level of this knowledge and accordingly modify the user's model. User knowledge in any area is most often represented by an *overlay model,* which is based on a structural model of the domain (software).

Goals. The user's goal or user task is a parameter that depends, to a greater extent, on the very nature of the user's work in hypermedia, rather than on the user as such. Depending on the type of system, this can be a work goal (in application systems), a search goal (in information retrieval systems), and a learning or solution goal (in training systems).

Level of training and experience. The following two characteristics of the user have something in common with the level of knowledge of the user, but functionally differ from it. This is the level of training of the user and the existing experience of the user with this hypermedia.

Preferences. The last, but not least, user characteristic considered by adaptive hypermedia systems is a set (system) of user preferences.

System operation model

The goal of an adaptive hypermedia system is to adapt content and visual presentation based on user knowledge. Some of this knowledge can be derived from user behavior in the system, taking into account the fact that some of this knowledge about the user may be hidden or implicit, and some - generally accepted. For example, the use of user data mining technologies (clustering, classification, etc.) can help reveal hidden knowledge, while monitoring user connections allows for more fine tuning of the system response time.

This article proposes to build a Model System along three orthogonal coordinates or adaptation dimensions:

1. *technology* (that is, technical conditions for access to the application, for example, the available bandwidth of communication channels, the characteristics of the user terminal or the type of browser, etc.);

2. *user behavior* (that is, a set of user actions, user preferences, etc.);

3. *external conditions* (user location, including time zone, user language, provider requirements, author settings, etc.)

The adaptive hypermedia system tracks various possible variations in the data lying on these coordinates, collecting sets of values into datasets for each dimension. The choice of specific variables and values for each specific case of adaptation depends on the subject area and the current profile of the application[4].

Conclusion

The proposed approach to the design of adaptive systems, it seems to us, makes it possible to build rather complex and effective information systems, oriented towards application in various fields of knowledge and fields of activity. The described design methods and approaches to the implementation of adaptive systems allow you to build a

subset of sites in one resource space, which ensures the unity of information flows of organizations, allows you to keep a single account of users, and standardizes information and educational resources.

In addition to the standard model of adaptive systems, we proposed expanding it by adding a dynamic interface model. The mechanism of the adaptive system operation, providing its flexibility and extensibility, is proposed.

List of sources used:

1. Dikarev SB, Sakharov VL, Designing adaptive hypermedia systems, Proceedings of the IEEE AIS'03 and CAD-2003 conferences, Divnomorskoe, 2003.

2. VV Gura, VV Vasilovsky, SB Dikarev, Electronic educational resources as a pedagogical environment of open education, Proceedings of the X All-Russian scientific and methodological conference "Telematics'2003", 2003

3. Chernyak, L. Adaptability and adaptability [Text] / L. Chernyak // Open systems. - 2004. - No. 9. - S. 30-35.

4. Masciadri, L. Frameworks for the Development of Adaptive Systems: Evaluation of Their Adaptability Feature Software Metrics [Text] / L. Masciadri, C. Raibulet // Proceedings of the 4th International Conference on Software Engineering Advances, Porto, Portugal, 20 -25 Sept., 2009. - P. 41-50.

PARALLELIZING THE FACE RECOGNITION PROCESS FROM A BIG DATABASE

Sadykova A.
e-mail: sadykova.akmanat@gmail.com
Al-Farabi Kazakh National University, Almaty, Kazakhstan

Abstract. *This article proposes a fresh system for identifying persons, which has the ability to identify a person in a timely manner, if his uniformity has already been saved in the system. The development works by protecting and comparing the investments of the object's faces, and then recognizing them later in the video stream. This development is quite accurate, it has the ability to identify people and brand them with personal numbers in real time. It is capable of this, including if variant.*

Keywords*: face recognation, GoogLeNet, DNN, OpenCV.*

Introduction

When we visually see an object or a scene, we mechanically identify the objects as different instances and associate them with separate definitions. However, visual identification is a rather difficult task for machines. The definition of images using artificial intelligence is a longstanding research problem in the field of computer vision. But over the period, various methods have developed, the joint goal of determining images is considered to be the classification of identified objects into various categories. As a consequence, it is also called the definition of objects.

Current implementations of video surveillance systems are provided for these purposes, such as detection of movement and objects. [1] These systems urge human awareness in order to actually apply the large amounts of data generated by video surveillance. Due to the exponential volume of data data and the superiority of using data data to support an early warning system, or it can be used as part of some other output system. Apart from this, a person does not have the ability to scroll through hours of video data without missing the main details that the computer vision system can easily identify [2]. This system has the ability to perform the same tasks that have every chance of being provided to a person, rather and more gracefully. One of the leading parts of the research system is the face identification system. The primary reason for using such a system will primarily be to identify persons who had the opportunity to be involved in some kind of illegal work. Other uses can be biometric testing [3], tracking the movements of specific individuals, terrorism prevention systems [4], etc.

In the field of computer vision, these definitions, such as segmentation, classification, definition and detection, are often used interchangeably, and all kinds of problems are somewhat the same. But in most cases this does not cause problems, everything becomes confusing, if your proletarian process insists that you do a certain task on purpose.

Definitions of image definition and computer vision are often used interchangeably, but in reality they are different. In practice, image detection is a computer vision application that bundles a suite of tasks encompassing object detection and image organizing.

Object localization is another type of computer vision, which is often confused with the definition of images. Object localization refers to determining the location of 1 or more objects in the image and drawing a bounding box around their perimeter. However, the localization of the object does not include the systematization of the identified objects.

Definitions of image detection and image detection are often used in lieu of buddy. However, there are significant technical differences.

Image detection is the task of arresting an image at the entrance and finding all sorts of objects in it. The case has the ability to work with face detection, in which methods wish to find patterns of faces in images. When we are strictly addicted to detection, we are not concerned about whether the detected objects have any meaning. The task of detecting the image is made only in order to distinguish one object from another, in order to qualify how many various objects are present in the image. This way, bounding boxes are drawn around every single object.

On the other hand, the definition of images is the task of identifying objects of interest in the image and determining which category or class they belong to. The usual layout of computer vision for image recognition is the ordering of image filtering, segmentation, symptom extraction, and rule-based systematization.

However, the usual layout of computer vision insists on the highest value of knowledge, a large amount of engineering time and has a large number of characteristics that must be predetermined manually, while portability for other tasks is rather limited.

There are a number of steps that go into the operation of image detection systems.

Study data dataset

Image definition models will require teaching data (video, image, photo, etc.). Neural grids need teaching images from a purchased dataset to get an idea of how specific classes look.

For example, an image definition model that defines different poses (a pose estimation model) will require multiple instances of different human poses in order to understand what makes the poses unique to buddy from buddy.

Learning neural grids

Images from the generated dataset are fed into the neural network method. This is a nuance of solid or machine learning when developing an image definition model. Learning the imaging technique allows convolutional neural networks to recognize and identify specific classes. Now for these purposes, a number of existing and well-tested frameworks are used.

Testing the model

The trained model should be tested with images that are not considered part of the training dataset. This is used to determine the usability, performance and accuracy of the model. In this way, within 80-90% of a perfect set of image data is used to study the model, and other data is reserved for testing the model. The performance of the model is measured based on a set of characteristics that show the percentage of confidence in the accuracy for the test image, incorrect identifications and much more. Read our post on how to evaluate the performance of machine learning models.

We are using Python 3.6 with OpenCV 4.1 to merit our goals [5]. We will apply the improved OpenCV deep neural networks (dnn) module [6] for extracting faces from images and the original GoogLeNet [7] architecture for calculating face embeddings.

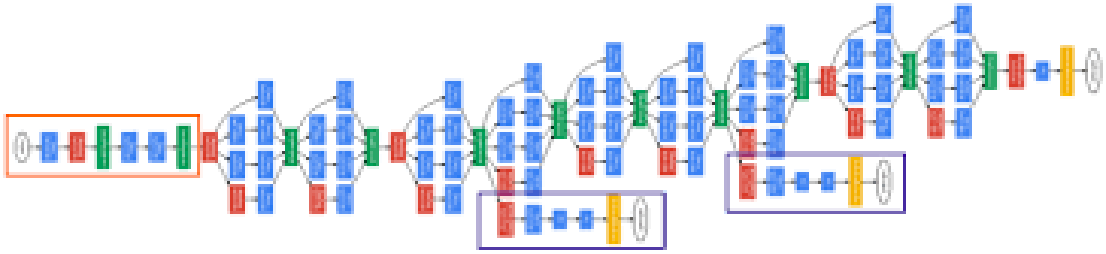


Figure – 1. Architecture of GoogLeNet Inception Model

This investment will be saved to create a database of faces that the face recognition system will later want to compare and foreshadow a person's face. In real time, for each faces that are recognized from the video stream, the investments of faces will be calculated, which will be compared with all embedded faces in the data set. This is a problem of tracing, when the components are not ordered. Means, it is necessary to find linearly. This will take quite a long time. First algorithm: Database Creation Algorithm

Input: Face pictures and ID

FIND all pictures in the DB
foreach picture in DB do
FIND localization and dimensions of face in picture
foreach face in picture do
CALCULATE face attachments
ADD ID and face attachments in a list as a result
SAVE result

Output: Database with faces

We use this probability to parallelize the search process. Algorithm 2: Parallel Algorithm for Face Recognition

Input: Face attachments Database and video

foreach frame in video do
  FIND location and dimensions of faces in pictures
  foreach face in picture do
    CALCULATE face attachments
    DISTRIBUTE a list as output of found faces
    foreach input list of found faces do
      CALCULATE a distance from face
      ADD a calculated value to a list of results
    FIND the smallest distance from calculation
PRINT a found person

Output: face identification on video

Database creation

We can apply the previously mentioned methods to determine the location of faces and calculate the investment of faces to create a database of faces. Images of people can be used to calculate the investment of persons who have every chance of being saved in a file or data base together with their names or personal numbers. Fresh records can be added to the file or data base later, or past records can be simply deleted.

The method is sold in the Python 3.8 programming language and uses the open source computer vision library OpenCV. For our experimental evaluation, we used an Intel Core i9 microprocessor system with 4 cores and 8 jets. The experiments were carried out with the QDF dataset [8]. The dataset has facial images of over 100 subjects in various orientations. The analysis was carried out with different volumes of the investment persons database, and the totals were plotted. The processing time of each frame is importantly reduced with a larger data base.

The acceleration can be monitored in Figure 2.

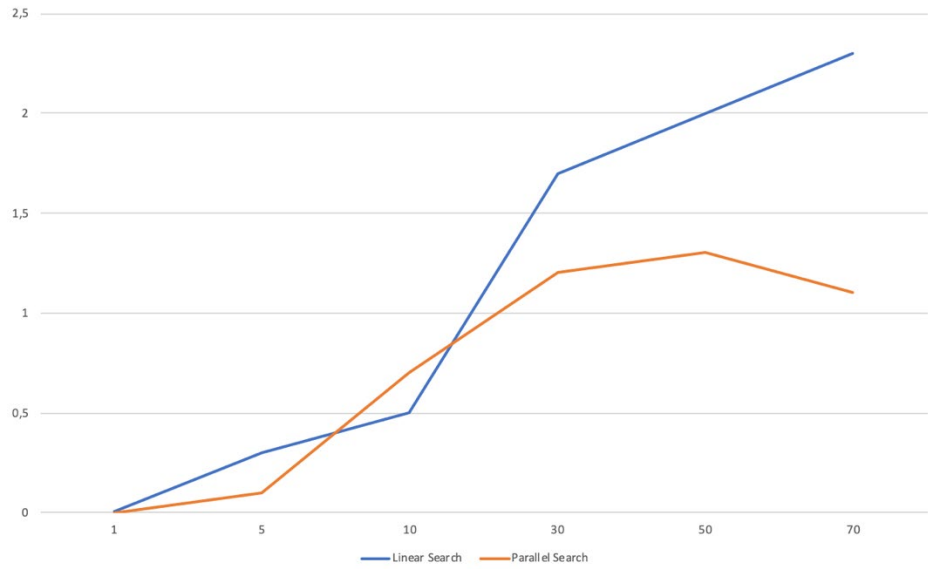


Figure – 2. Speedup of parallel version

Conclusion

Based on the test results, it reads that a fairly reliable solution has been created for this problem. A solution that could first be extracted, then compare the attachments of faces for recognition purposes, and then stored simulated. Figure 4 shows that due to the parallelization of processes, the above algorithm works more efficiently. More importantly, without sacrificing accuracy. The proposed model can be used for both specific and multipurpose. This model can be used to establish identity when entering or leaving social space. Another use can be a system for predicting a person's energy, which analyzes where a person spends time in a building and at what time of the day. It has the

ability to be much more than these applications that use this layout as their own soil, and then use it for something else.

References

1. Lin K., Lam K., Xie X., Siu W. An Efficient Human Face Indexing Scheme Using Eigenfaces. Proceedings of the 2003 IEEE International Conference on Neural Networks and Signal Processing. 2003, 920-923.

2. Jafri R., Arabnia R. A Survey of Face Recognition Techniques. Journal of Information Processing Systems. 2013, 5(2), 41-68.

3. Bengio Y. Representation learning: A review and new perspectives. Pattern Analysis and Machine Intelligence. 2013, 35(8), 1798–1828.

4. Grauman K., Leibe B. Visual object recognition. Morgan & Claypool Publishers, 2010, 165-186.

5. Huang G.B. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. Technical Report 07-49, University of Massachusetts. 2007, 1(2), 3–37.

6. Reuters. 2020. Blacklisted Chinese firm Megvii cleared for $500 million Hong Kong IPO. Retrieved from: https://www.reuters.com/article/us-megvii-ipo/blacklisted-chinese-firm-megvii-cleared-for-500-million-hong-kong-ipo-idUSKBN1Z511E (Accessed December 2020).

7. VisionLabs. 2017. Visionlabs-003. Retrieved from: https://visionlabs.ai/ru/products/luna-sdk (Accessed December 2020).

REVIEW OF EXISTING RESOURCES AND PRODUCTION OF NATURAL URANIUM IN THE WORLD

Yunicheva N.R., Kuchin Y., Mukhamedieva E.L.
Institute of Information and Computational Technologies KN MES RK, Almaty
e-mails: naduni@mail.ru , ykuchin@mail.ru, muhamedijeva@gmail.com

All over the world, uranium is the main resource for the operation of nuclear power plants. Deposits of uranium ores are not evenly distributed around the globe. Today, only 28 countries of the world extract valuable raw materials in their bowels. The main world reserves of uranium in the world are located in 8 countries. We will tell you a little more about the countries with the largest uranium reserves.

Figure 1 shows the countries with the largest uranium reserves according to [1,2].

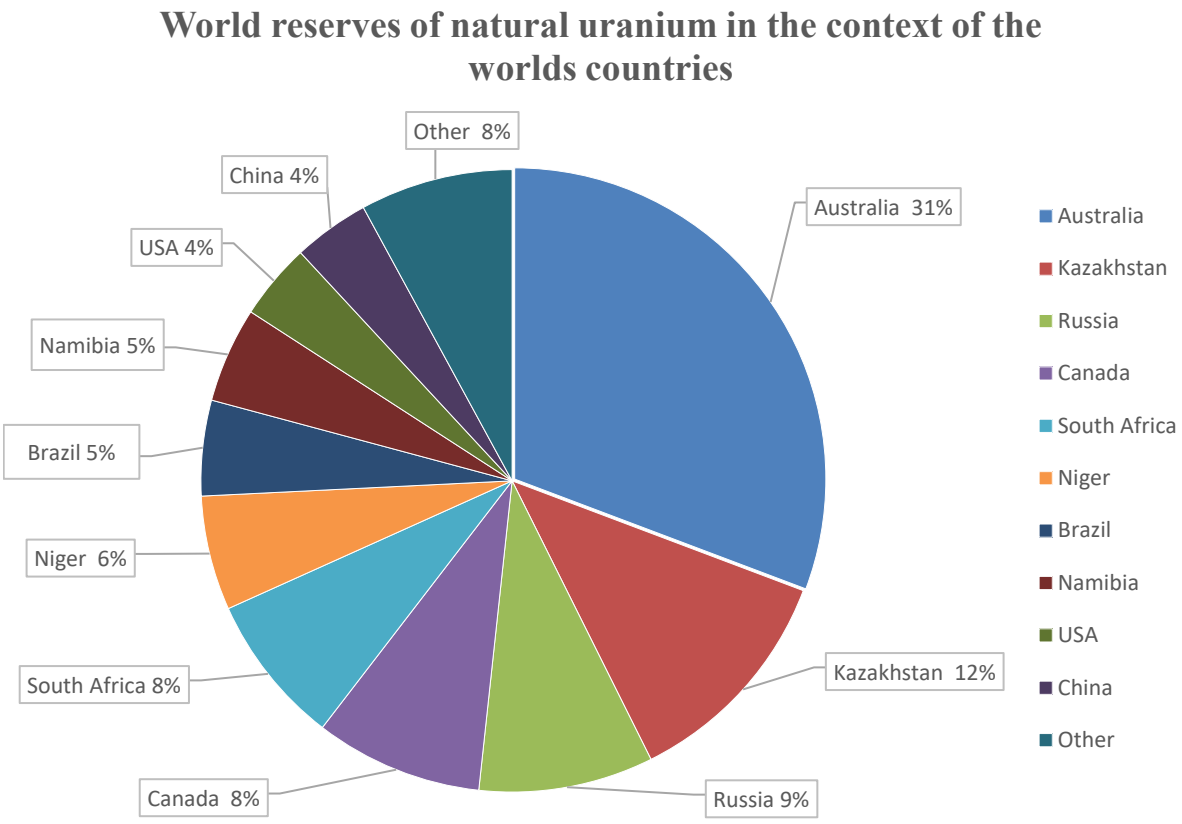


Figure 1 - World reserves of natural uranium in the context of the worlds countries

Table 1 below contains a summary of the uranium reserves, the number and names of deposits in the leading countries in terms of uranium reserves.

Table 1 - Leading countries in terms of natural uranium reserves in the world

№	Country	Information about uranium reserves, the number of deposits, etc.
1.	Australia	Australia is the undisputed leader in the world's uranium reserves. According to the World Nuclear Association, about 31.18% of all world uranium reserves are located in this country, which in numerical terms means 661 thousand tons of uranium. There are 19 uranium deposits in Australia. The largest and most famous are Olympic Dam, where about 3 thousand tons of uranium is mined per year, Beaverley (production of 1 thousand tons) and Honemun (900 tons per year). The cost of uranium mining in the country is $ 40 per 1 kg.
2.	Kazakhstan	The second place in uranium reserves belongs to Kazakhstan. The Asian country contains 11.81% of the world's fuel reserves, which equals 629 thousand tons of uranium. There are 16 developed deposits in Kazakhstan, where a valuable resource is extracted. The Chusaray and Syrdarya uranium provinces are home to the largest Korsan, South Inkai, Irkol, Kharasan, West Mynkuduk and Budenovskoe deposits.
3.	Russia	Russia ranks third in uranium reserves. According to experts, there are 487,200 tons of uranium in its depths, which is 9.15% of the world's uranium resources. Despite the size of the country and large reserves of uranium, there are only 7 deposits in Russia, and almost all of them are located in Transbaikalia. More than 90% of the uranium mined in the country comes from the Chita region. This is the Streltsovskoe ore field, which includes more than ten uranium ore deposits. The largest center is the city of Krasnokamensk. The remaining 5-8% of uranium in the country is located in Buryatia and the Kurgan region.
4.	Canada	He leading place in the reserves of uranium ore in North America, and the fourth in the world belongs to Canada. The total uranium reserves in the country are 468,700 tons of uranium, which is 8.80% of the world's reserves. Canada owns unique deposits of the "unconformity" type, the ores of which are rich and compact, the largest of which are MacArthur River and Cigar Lake. The country is developing the Waterbury Project uranium deposit, which consists of several deposits, the area of which is 12,417 hectares. Canada has enjoyed tremendous advantages throughout its history due to its proximity to the United States. The main uranium mining company in Canada is Cameco.
5.	South Africa	South Africa, uranium is mined along the way from gold deposits. The Dominion deposit is the largest in the country with open-pit and underground mining. Large mines include Western Ariez, Palabora, Randfontein and Vaal River, where gold tailings are mainly mined. The average cost of uranium mining in an African country is $ 40 per kg. In uranium production, South Africa lags far behind the leading countries in this industry, producing 540 tons of uranium a year, which is the twelfth figure in the world. According to some estimates, South Africa has 6% of the world's total uranium reserves. However, other sources claim that South Africa has less reserves than Niger and Namibia. The main problems in the country's economy are unemployment, high levels of poverty and inequality. The country is better known for mining gold, platinum and chromium, rather than uranium. There are I nuclear power plants in South Africa, but there are plans to build several more nuclear power plants. Thus, South Africa could become a potentially large market for the use of uranium.
6.	Niger	Uranium reserves account for 5% of the world's total. The largest deposits in the country are Imuraren, Madauela, Arlit and Azelit, there

		are 12 of them in total in the country. The prime cost of uranium mined in Niger is $ 34-50 per 1 kg. The main player in the uranium market of the country is the French company Areva SA, which is mining at the Arlit deposit, one of the 10 largest uranium deposits in the world. In addition, uranium is Niger's largest export. According to Areva, uranium accounts for about 5% of the country's GDP. At the same time, Niger is a rather poor country and depends on foreign investment in the extraction of natural resources.
7.	Brazil	The country's indicator is equal to 276,700 tons of uranium ore. Production of U per year is 198 tons per year.
8.	Namibia	Uranium reserves in the country are 261 thousand tons. There are four major uranium deposits in Namibia. Namibia's reserves are believed to account for 5% of the world's total. The economy of Namibia, as in the case of Niger, is rather poor, but it is more diversified than in Niger. The country exports diamonds, copper, gold, zinc as well as uranium. In general, mining accounts for 11.5% of GDP.
9.	USA	The total reserves of U in the USA are 207,000 tons.
10.	China	China possesses approximately 5% of the world's uranium reserves. At the same time, various sources estimate the reserves in different I: some indicate that China's reserves are slightly higher than in Namibia and Niger, some put China only in eighth place in terms of reserves. The country has about 20 nuclear power plants under construction.

Analysis of information related to the leadership of countries in uranium reserves does not allow us to conclude that these same countries are leaders in uranium mining.

In 2018, the world's largest uranium miners produced 86% of the world's uranium mined, according to the World Nuclear Association. The main uranium mining companies are mining corporations from Kazakhstan, Canada, Australia: they account for two-thirds of the world's production.

Table 2 shows the top ten uranium mines based on 2018 production results. At least three of these top ten mines (Rössing, Arlit (SOMAÏR) and Ranger), representing 10% of 2018 production, are scheduled/expected to close before the end of the 2020s and will need to be replaced by new mine capacity by then, in order not to cause further reduction of primary uranium production [3].

Table 2 - Ten largest world uranium mines, ranked by 2018 production, tU

Main	**Country**	**Main owner**	**Type**	**tU**	**% of world**
Cigar Lake	Canada	Cameco/Orano	Underground	6,924	12.9
Olympic Dam	Australia	BHP Billiton	By-product	3,159	5.9
Husab	Namibia	Swakop Uranium (CGN)	Open-pit	3,028	5.7
Inkai 1-3	Kazakhstan	Kazatomprom/ Cameco	ISR	2,643	4.9
Rössing	Namibia	Rio Tinto	Open-pit	2,102	3.9

Budenovskoye 2	Kazakhstan	Uranium One/ Kazatomprom	ISR	2,081	3.9
Tortkuduk	Kazakhstan	Orano/Kazatomprom	ISR	1,900	3.6
Arlit (SOMAÏR)	Niger	Orano	Open-pit	1,783	3.3
Ranger	Australia	Rio Tinto/ERA	Open-pit	1,695	3.2
Kharasan 2	Kazakhstan	Kazatomprom	ISR	1,631	3,0
Others				26,553	49.6
Total				**53,498**	**100**

During the development of the uranium market, the technology of mining processing itself has changed more than once. Basically, uranium ore is mined in two ways - mine or open pit, depending on the depth of the layers with uranium ore.

The career path means less radiation and higher safety. Underground (mine) allows you to extract higher quality uranium ore, but it is also more dangerous because of radon - a radioactive gas that accumulates in mines.

Underground leaching of uranium ores is the most advanced uranium mining technology, first used since 1957. The method is the injection of a special chemical solvent underground into the layer of uranium ores, which reacts to uranium compounds. Then this solution is brought to the surface and processed already. The disadvantage of this method is the ability to use it only in sandstone and below the groundwater level. The method has gained particular popularity in Kazakhstan, Uzbekistan and the United States, although this method of production is used in Canada, Australia and China.

The geography of the in situ leaching method is steadily increasing its share of the total volume, mainly due to Kazakhstan (this method covers more than half of the production). Since 2015, global production has proceeded as follows:

Conventional mines had a mill where the ore was crushed, crushed, and then leached with sulfuric acid to dissolve uranium oxides. In a conventional mine mill or sewage treatment plant with ISL operation, the uranium is then separated by ion exchange before drying and packaging, usually as uranium oxide (U3O8). Some mills and ISL operations (especially in the US) use carbonate leaching instead of sulfuric acid, depending on the orebody.

Today, the approximate distribution of uranium mining methods is as follows [4]:

Table 3-Evaluation of uranium mining methods

№	Uranium mining methods	t, U	Specific weight, %
1	Underground leaching (ISL)	29,197	48,3%
2	Underground and quarrying (except Olympic Dam) *	27,791	45,9%

3	By-product	3,509	5,8%
	Total:	**60,497**	**100%**

According to the table, the method of underground leaching of uranium ores is used approximately equally along with two methods – mine or quarry. The extraction of uranium using underground leaching causes significantly less damage to the environment than the methods described above. Over time, reclamation processes occur on the developed land plot. The use of this method can reduce economic costs. But it has its limitations. It is not used only in sandstone and below the water table. Almost all the uranium mining companies listed above have all the existing mining technologies, depending on the characteristics of specific deposits and mines.

This research has been funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP09562260 "Development of a method for calculating the filtration characteristics of wells of uranium deposits based on machine learning algorithms working with inaccurately marked interval data".)

References

[1] URL: https://eenergy.media/2018/11/06/zapasy-urana-u-kakih-stran-oni-samye-bolshie
[2] URL: https://vivareit.ru/strany-lidery-po-zapasam-urana (дата обращения: 13.08.2021).
[3] Recent uranium production. The Nuclear Fuel Report 2019 https://world-nuclear.org/getmedia/b488c502-baf9-4142-8d12-42bab97593c3/nuclear-fuel-report-2019-expanded-summary-final.pdf.aspx
[4] Амирова У.К., Урузбаева Н.А. Обзор развития мирового рынка урана // Universum: экономика и юриспруденция: электрон. научн. журн. 2017. № 6 (39). URL: https://7universum.com/ru/economy/archive/item/4802 (дата обращения: 16.08.2021).

РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ СИСТЕМ КОНТРОЛЯ ВОДИТЕЛЯ

Б.С.Амирханов[1], Т.Ж. Мазаков[2]
e-mail:[1]amirkhanov.b@gmail.com, [2]tmazakov@mail.ru
[1]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан
[2]Институт информационных и вычислительных технологий, Алматы, Казахстан

Аннотация. *В данной работе описывается улучшение существующих систем контроля/помощника водителя, а также рассматривается разработка собственного прибора для анализа состояния водителей. Улучшение планируется за счет анализа видеопотока с камеры перед водителем, с помощью предыдущих наработок авторов считывается с видеопотока частота сердечных сокращений(ЧСС) с лица водителя. Анализируя данные ЧСС мы можем отслеживать аритмию сердца в течении времени поездки.*

Ключевые слова: *BioPython, биоинформатика, OpenCV, контроль водителя, частота сердечный сокращений, сердечная аритмия.*

Введение. На текущий момент много разработок посвящены контролю усталости здоровья водителей. Все разработки призваны решить одну из распространенных причин аварий на дорогах усталость — до 25% водителей попадают в ДТП во время длительной поездки. Чем дольше человек находится в дороге, тем ниже падает бдительность. Согласно проведенным исследованиям, всего 4 часа вождения снижают реакцию в два раза, а после восьми часов — в 6 раз. Хотя проблема кроется в человеческом факторе, производители автомобилей стремятся обезопасить езду и пассажиров. Специально для этих целей разрабатывается система контроля усталости водителя.

Первая разработка появилась на рынке от японской компании Nissan, которая запатентовала революционную технологию для автомобилей в 1977 году. Но сложность технической реализации в то время заставила производителя сосредоточиться на более простых решениях для повышения безопасности транспорта. Первые рабочие решения появились спустя 30 лет, но их продолжают совершенствовать и улучшать способы распознавания усталости водителя.

Суть решения заключается в том, чтобы анализировать состояние водителя и качество вождения. Изначально система определяет параметры при старте поездки, что позволяет оценить полноту реакции человека, а после этого начинает отслеживать дальнейшую скорость принятия решений. Если обнаружено, что водитель сильно устал, появляется уведомление с рекомендацией отдыха. Отключить звуковые и визуальные сигналы нельзя, но они автоматически появляются через заданные промежутки времени.

Особая потребность в решении наблюдается у водителей одиночек. Когда человек едет с пассажирами, они могут поддерживать его бодрое состояние разговорами и отслеживать усталость. Самостоятельная езда способствует сонливости и замедлению реакции на дороге.

Главное предназначение системы контроля усталости заключается в предотвращении аварийных ситуаций. Это осуществляется с помощью наблюдения за водителем, определения замедленной реакции и постоянной рекомендации отдыха, если человек не останавливает движение. Основные функции:

1. Контроль движения автомобиля — решение самостоятельно отслеживает дорогу, траекторию движения, допустимые скорости. Если водитель нарушает правила скоростного режима или покидает полосу, система подает звуковые сигналы, чтобы повысить внимание человека. После этого появятся уведомления о необходимости отдыха.
2. Контроль водителя — изначально отслеживается нормальное состояние водителя, а затем отклонения. Реализация с помощью камер позволяет наблюдать за человеком, а в случае закрытия глаз или падения головы (признаки сна) подаются предупреждающие сигналы.

Элементы конструкции системы зависят от способа реализации и контроля движения. Решения для слежения за водителем сконцентрированы на человеке и происходящем в салоне транспорта, а остальные варианты — на показателях авто и обстановке на дороге. Рассмотрим несколько вариантов конструктивных особенностей.

Австралийская разработка DAS, которая находится на стадии тестирования, предназначена для слежения за дорожными знаками и соблюдения транспортом требований скоростного режима и норм движения. Чтобы анализировать ситуацию на дороге, используют:

- три видеокамеры — одна фиксируется на дороге, две остальные отслеживают состояние водителя;
- блок управления — обрабатывает информацию о дорожных знаках и анализирует поведение человека.

Другие системы оснащаются датчиком руля, видеокамерами, а также электроникой, которая может отслеживать параметры тормозной системы, устойчивости при движении, показателях двигателя и многое другое. В случае усталости подается звуковой сигнал. Принцип работы всех систем сводится к тому, чтобы определить уставшего водителя и предотвратить ДТП. Для этого производители используют различные конструкции и логику работы. Если говорить о решении Attention Assist от Mercedes-Benz, то выделяются следующие особенности:

- контроль движения транспортного средства;
- оценка поведения водителя;
- фиксация взгляда и отслеживание состояния глаз (Рис. 1).

Рис. 1 Отслеживание движение глаз у водителя

После начала движения система анализирует и считывает нормальные параметры управления автомобилем в течение 30 минут. Затем происходит слежение за водителем, включая силу воздействия на рулевое колесо, использование переключателей в салоне автомобиля, траектория поездки. Полноценный контроль усталости осуществляется при скорости от 80 км/час. Дополнительный контроль применяется к движению автомобиля и качеству управления рулевым колесом. Система считывает такие параметры, как:

- манера вождения, которая определяется при изначальном движении;
- время суток, продолжительность и скорость движения;
- эффективность использования подрулевых переключателей, тормозов, дополнительных устройств управления, силы вращения руля;
- соответствие скорости максимально допустимой на участке;
- состояние дорожного покрытия, траектории движения.

Если алгоритм находит отклонения от нормальных параметров, система задействует звуковое уведомление для повышения бдительности водителя и рекомендует временно остановить поездку с целью отдыха. Существует ряд особенностей у систем, которые в качестве основного или дополнительного фактора анализируют состояние водителя. Логика реализации основана на использовании видеокамер, которые запоминают параметры бодрого человека, а затем выполняют мониторинг при длительных поездках. С помощью камер, направленных на водителя, получают следующую информацию:

- закрытие глаз, причем система различает моргание и сонливость;
- частота и глубина дыхания;
- напряжение лицевых мышц;
- уровень открытости глаз;
- наклон и сильные отклонения в положении головы;
- наличие и частота зевания.

Учитывая дорожные условия, изменения в управлении транспортом и параметры водителя, появляется возможность предотвращать аварии. Система автоматически информирует человека о необходимости отдыха и подает экстренные сигналы для увеличения бдительности.

Методы исследования. Авторы данной статьи хотят улучшить существующие системы контроля/помощника водителя или даже разработать собственный прибор для анализа состояния водителей, при наличии соответсвующего финансирования. Улучшение планируется за счет анализа видеопотока с камеры перед водителем, с помощью наших наработок [16] мы можем считывать с видеопотока частоту сердечных сокращений (ЧСС) с лица водителя. Имея на руках данные ЧСС мы можем отслеживать аритмию сердца в течении времени поездки. Аритмией называется нарушение сердечного ритма. Основными причинами, вызывающими сбой, являются:

- интоксикация организма в результате употребления спиртного, наркотиков и табакокурения;
- стресс;
- сужение сосудов;
- недостаток гемоглобина в крови;
- сильный выброс адреналина;
- нарушение электролитного баланса;

- заболевания сердца (сердечная недостаточность, инфаркт, порок сердечной мышцы);
- гормональный дисбаланс;
- физическое и психическое истощение.

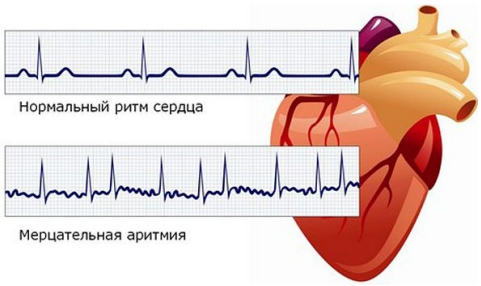


Рис. 2 Нормальный ритм сердца и мерцательная аритмия

Основными симптомами аритмии являются:

1. Тахикардия. Это учащенное сердцебиение (выше 90 ударов в минуту).
2. Брадикардия. Снижение частоты сердцебиений (менее 50 ударов).
3. Экстрасистолия. Неритмичное биение сердца (несвоевременное сокращение сердечных камер).
4. Мерцательная аритмия. Разновидность тахикардии, проявляющаяся фибрилляцией предсердий. (Рис. 2)
5. АВ-блокада. Разновидность брадикардии, характеризующаяся нарушением проведения импульса из предсердий в желудочки.

Профилактика аритмии сердца должна проводиться только после консультации с врачом, который точно определит, имеется ли сбой в ритме сердечной мышцы и чем он вызван. При аритмии у человека изменяется частота сердечных сокращений. Нарушение ритма довольно редко является самостоятельным заболеванием. В большинстве случаев аритмия сигнализирует о наличии у человека различных болезней сердца.

Авторы в рамках этой работы не преследуют цель постановки диагноза при использовании своего оборудования для определения сердечной аритмии. Цель данной работы создание технологии предупреждения водителя, медицинских работников предприятий организующих пассажирские перевозки, ответственных сотрудников за безопастность движения о том , что у водителя присутсвуют признаки аритмии частоты сердечных сокращений, которые могут повлечь за собой внештатные ситуации на дороге вплоть до ДТП.

Например если рассмотреть последний случай ДТП с участием общественного транспорта произошедшего 21.08.2021 в г.Алматы. Almaty Electrotrans организация осуществляющая пассажирские перевозки в г.Алматы, сообщает: "Водитель троллейбуса БН 1240, почувствовав кратковременное недомогание, не справился с управлением и ударился о край стены подземного перехода. Данный факт зарегистрирован в ДП, ведётся разбирательство". Мы, как авторы проекта контроля/помощника водителя, понимаем что наша разработка жизненно необходима как минимум в пассажирских перевозках. Своевременная диагностика с помощью определения частоты сердечных сокращений, позволит определить стрессовые ситуации у водителей пассажирского транспорта, отследить

артимию сердца, что позволит на ранних этапах принять решение ответственных сотрудников за безопастность на дорогах о допуске водителей на маршрут, что позволит уменьшить количество таких ДТП.

В своей работе [16] «Дистанционный метод мониторинга жизненных показателей человека» авторы описывают концепцию измерения частоты сердечных сокращений (пульса) человека, снятого на простую видео или веб-камеру, при помощи визуализации потока крови на лице. Представлены несколько возможных методов постобработки для улучшения извлечения фактического импульсного сигнала:

- независимый компонентный анализ позволяет обнаруживать независимые сигналы из набора наблюдений, которые состоят из линейных смесей основных источников;
- Эйлерово усиление видео подчеркивает цветовые вариации, и позволяет анализировать изменения значения каждого пикселя с течением времени;
- детрендинг удаляет небольшие тренды из входного сигнала без искажения его амплитуды.
- Приведены алгоритмы получения частоты сердечных сокращений по видеосигналу:
- спектр мощности, набор уравнений, позволяющий определить частоту сигнала с помощью преобразования Фурье;
- обнаружение импульсной волны, алгоритм обнаружения и проверки нарастающих фронтов импульсного сигнала.

В работе используются [16] фотоплетизмография. Одним из методов неинвазивного снятия показателей является фотоплетизмография (ФПГ) - это концепция оптического измерения объемных изменений органа. Его наиболее широко используют в пульсоксиметрах. ФПГ основан на принципе, что кровь поглощает больше света, чем окружающие ткани, таким образом, изменения объема крови влияют на светоотражение [6]. Использование специальных источников света и инфракрасных длин волн, а также контактных зондов было нормой [4,5,7]. Однако в последнее время была изучена дистанционная бесконтактная PPG-визуализация [8,9]. Метод, используемый в статье [9], захватывает значения пикселей (красный, зеленый и синий каналы) лицевой области ранее записанного видео, где добровольцев просили минимизировать движения. Затем значения пикселей в пределах интересующей области (ROI) усреднялись для каждого кадра. Было обнаружено, что это пространственное усреднение значительно увеличивает отношение сигнал/шум. Далее оценка частоты сердечных сокращений вычислялась с помощью быстрого преобразования Фурье и спектра мощности. Авторы работы [6] демонстрируют, что зеленый канал имеет более сильный сердечный сигнал по сравнению с красным и синим каналами. Это убедительное доказательство того, что сигнал обусловлен колебаниями объема крови, поскольку гемоглобин поглощает зеленый свет лучше, чем красный и синий.

В работе [16] авторами разработано приложение (Рис. 3) для мониторинга жизненно важных показателей на основе метода Эйлерова видеоусиления, которое включает в себя следующие функции:

- определение и оценка частоты сердечных сокращений на основе метода Эйлерова видеоусиления;
- отображение изменений в реальном времени, таких как увеличенный кровоток, полученный с помощью метода Эйлерова видеоусиления;

- решение проблемы с движением артефактов, вызванным движением человека и/или смартфона.

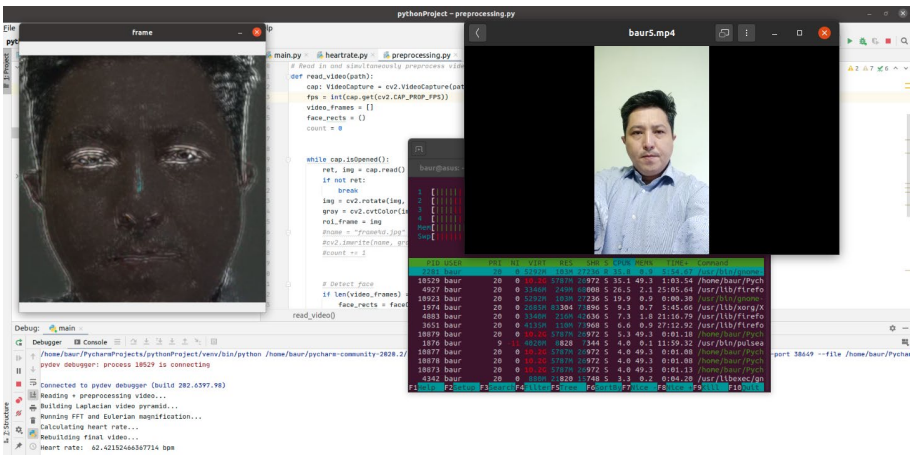


Рис. 3 Определение ЧСС из видеопотока

Заключение. На основе своей работы [16] авторы создали прототип прибора для определения частоты сердечных сокращений водителя транспортного средства. На текущий момент идет тестирование данного прототипа. Авторы надеются довести прототип до полнофункциональной системы, с распознованием водителей, для допуска на машрут и ведением базы состояний водителя, с интеграцией с системами HR, с GPS контролем маршрута и скорости и т.д.

Работа выполнена за счет средств программы целевого финансирования на основе договора по оказании услуг субподряда «Разработка национального электронного банка данных по научной зоологической коллекции Республики Казахстан, обеспечивающего их эффективное использование в науке и образовании».

Литература

1. Hao-Yu Wu, Michael Rubinstein, Eugene Shih, John Guttag, Frédo Durand, andWilliam T. Freeman. Eulerian video magnification for revealing subtle changes inthe world.ACM Trans. Graph. (Proceedings SIGGRAPH 2012), 31(4), 2012.

2. M.Z. Poh, D.J. McDuff, and R.W. Picard. Non-contact, automated cardiac pulsemeasurements using video imaging and blind source separation.Optics Express,18(10):10762–10774, 2010.

3. M.Z. Poh, D.J. McDuff, and R.W. Picard. Advancements in noncontact, multi-parameter physiological measurements using a webcam. Biomedical Engineering,IEEE Transactions on, 58(1):7–11, 2011.

4. EF Greneker. Radar sensing of heartbeat and respiration at a distance with appli-cations of the technology. InRadar 97 (Conf. Publ. No. 449), pages 150–154. IET,1997.

5. M. Garbey, N. Sun, A. Merla, and I. Pavlidis. Contact-free measurement of cardiacpulse based on the analysis of thermal imagery.Biomedical Engineering, IEEETransactions on, 54(8):1418–1426, 2007.

6. Wim Verkruysse, Lars O Svaasand, and J Stuart Nelson. Remote plethysmographicimaging using ambient light.Optics express, 16(26):21434–21445, 2008.

7. IDC. Android marks fourth anniversary since launch with 75.0in third quarter,according to idc.http://www.idc.com/getdoc.jsp?containerId=prUS23771812.

8. P Wieringa, F Mastik, and AFW Van der Steen. Contactless multiple wavelength photoplethysmographic imaging: a first step toward “spo2 camera” technology.An-nals of biomedical engineering, 33(8):1034–1041, 2005.

9. Sijung Hu, Jia Zheng, Vassilios Chouliaras, and Ron Summers. Feasibility of imaging photoplethysmography. InBioMedical Engineering and Informatics, 2008.BMEI 2008. International Conference on, volume 2, pages 72–75. IEEE, 2008.

10. C. Liu, A. Torralba, W.T. Freeman, F. Durand, and E.H. Adelson. Motion magnification. InACM Transactions on Graphics (TOG), volume 24, pages 519–526.ACM, 2005.

11. P. Burt and E. Adelson. The laplacian pyramid as a compact image code.Communications, IEEE Transactions on, 31(4):532–540, 1983.

12. C. Liu, W.T. Freeman, R. Szeliski, and S.B. Kang. Noise estimation from a singleimage. InComputer Vision and Pattern Recognition, 2006 IEEE Computer SocietyConference on, volume 1, pages 901–908. IEEE, 2006.

13. Daniel A Litvack, Tim F Oberlander, Laurel H Carney, and J Philip Saul. Timeand frequency domain methods for heart rate variability analysis: a methodologicalcomparison.Psychophysiology, 32(5):492–504, 1995.

14. Mika P Tarvainen, Perttu O Ranta-aho, and Pasi A Karjalainen. An advanced detrending method with application to hrv analysis.Biomedical Engineering, IEEETransactions on, 49(2):172–175, 2002.

15. Bistra Nenova and Ivo Iliev. An automated algorithm for fast pulse wave detection.International Journal Bioantomation, 14(3):203–216, 2010.

16. Амирханов Б.С., Мазаков Т.Ж., Мазакова А.Т., Исимов Н.Т., Жолмагамбетова Б.Р., Әбдіразақ Б.К. Дистанционный метод мониторинга жизненных показателей человека. V Международная научно-практическая конференция "Информатика и прикладная математика. 29 сентября - 1 октября 2020 г., Алматы, Казахстан

МЕТОДЫ И АЛГОРИТМЫ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ ПОВЕРХНОСТНЫХ ДЕФЕКТОВ СВАРНЫХ СОЕДИНЕНИЙ

Емельянова М.Г.
e-mail: MYemelyanova@ektu.kz
Восточно-Казахстанский технический университет им. Д. Серикбаева, Казахстан

Аннотация. *В работе рассматривается задача автоматического обнаружения и распознавания поверхностных дефектов сварных соединений труб из нержавеющей стали в процессе производства. Предлагается алгоритм обнаружения поверхностных дефектов сварных соединений на основе метода вычитания фона. Определены классы дефектов. Предложено решение задачи классификации дефектов.*

Введение

Распознавание образов – одно из актуальных научно-практических направлений. Решение задач распознавания образов возможно благодаря развитию технических средств, компьютерных технологии, а также методов компьютерного зрения. Задачи распознавания решаются в различных областях, в том числе, в промышленности для автоматического обнаружения и классификации дефектов сварных соединений в различных изделиях.

В процессе изготовления гибких гофрированных труб из нержавеющей стали на производственной линии ведётся контроль качества сварных соединений. Постоянно осуществляется визуальный контроль сварных соединений в соответствии с международным стандартом ISO 17637:2016 [1] (ГОСТ Р ИСО 17637 – 2014 [2]), заключающийся в осмотре поверхности невооружённым глазом. На результат визуального контроля оказывает влияние человеческий фактор.

Для создания сварных соединений используется автоматическая дуговая сварка вольфрамовым электродом в инертном газе (TIG – **Tungsten Inert Gas)**. Причинами возникновения дефектов TIG-сварки могут быть: несоответствующее требованиям качество инертного газа, стали, перепады напряжения и т.д. Дефекты сварки классифицируются согласно международному стандарту ISO 6520-1:2007 [3] (ГОСТ Р ИСО 6520-1 – 2012 [4]). На рис. 1 приведены изображение сварного соединения без дефектов, а также несколько изображений дефектов, возникающих при сварке тонкостенных гибких труб из нержавеющей стали.

а) б) в) г)

Рис. 1 Изображение нормального сварного соединения а), изображения дефектов сварки гибких труб из нержавеющей стали: б) несплавление, в), прожог, г) окисление металла

Возникает задача автоматического обнаружения и распознавания поверхностных дефектов сварных соединений в процессе производства гибких труб из нержавеющей стали для исключения субъективного влияния на результат контроля.

Исследователи [5]-[11] решают задачу автоматического распознавания дефектов сварных соединений, используя различные подходы и методы. Необходимо исследование методов, разработка и реализация алгоритмов автоматического обнаружения и распознавания поверхностных дефектов сварных соединений для рассматриваемой области с учётом специфики и требований.

Методы и предлагаемый алгоритм

В процессе распознавания дефектов сварных соединений можно выделить следующие этапы: получение изображений, предварительная обработка, обнаружение дефектов, классификация дефектов [5], [6].

Для получения изображений (кадров) необходима камера и дополнительная подсветка. Полученное изображение проходит предварительную обработку: преобразование в полутоновое изображение, уменьшение шума, улучшение контрастности, выделение области интереса и т.д.

Для обнаружения дефектов на изображениях используется сегментация. В работах [5]-[7] для сегментации применяются методы пороговой обработки, методы обнаружения контуров, математическая морфология, а также методы вычитания фона.

Обнаружить изменения на кадрах видеопоследовательностей позволяют методы вычитания фона. Сначала строится модель фона, затем каждый кадр видеопоследовательности сравнивается с построенной моделью. Полученное разностное изображение фильтруется пороговым значением.

Существует множество методов построения модели фона: temporal average, temporal median, SG, MOG, KDE, SLPCA и др. [12].

Авторы [7] успешно применили модифицированный метод вычитания фона, основанный на моделях гауссовской смеси (MBS) для сегментации дефектов сварных соединений в реальном времени.

Для решения задачи автоматического обнаружения дефектов сварных соединений в процессе производства гибких труб из нержавеющей стали предлагается использовать метод вычитания фона на основе нерекурсивного метода усреднения кадров (temporal average).

Укрупнённый алгоритм обнаружения дефектов представлен следующим образом:

1. Получение s-кадров видеопоследовательности.
2. Построение модели фона на основе усреднения s-кадров.
3. Предварительная обработка поступающего кадра.
4. Выделение области интереса.
5. Вычитание фона из обработанного кадра.
6. Фильтрация разностного изображения с эмпирическим пороговым значением T, получение бинарного изображения.
7. Определение количества белых пикселей в области возможного дефекта C.

8. Сравнение величины C с эмпирическим значением P.
9. В случае выполнения условия – дефект обнаружен.
10. Выполнение морфологической операции закрытия.
11. Фильтрация по площади.
12. Локализация дефекта.
13. Через n-кадров обновление модели фона.

Значения T, P определяются экспериментальным путём.

После сегментации и локализации дефекта на изображении осуществляется классификация дефекта. Выделены следующие классы дефектов [3], [4]: несплавление, прожог, окисленная поверхность.

На этапе классификации происходит извлечение признаков из областей обнаруженных дефектов, выбираются наиболее информативные признаки, строится классификатор, оценивается точность распознавания.

На рис. 2 представлена схема системы классификации.

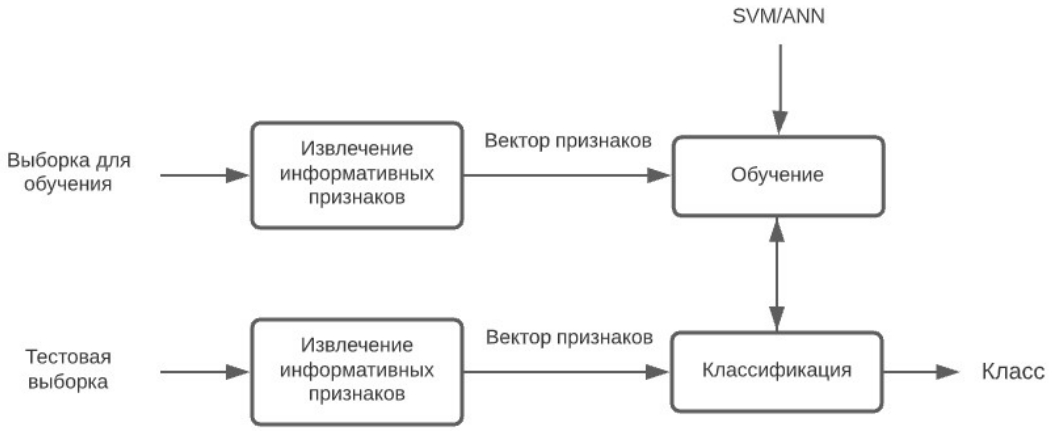


Рис. 2 Схема системы классификации

Авторы обзорной статьи [5] указывают, что в большинстве случаев для решения задачи классификации дефектов сварных соединений используются геометрические и текстурные признаки. Классификаторы создаются на основе алгоритма k-ближайших соседей (k-Nearest Neighbor – k-NN), метода опорных векторов (Support Vector Machine – SVM), нечёткого алгоритма c-средних (Fuzzy c-means), деревьев решений, нейронных сетей и др. [5].

Авторы [6] предложили классификационные правила для шести геометрических признаков, извлечённых из областей обнаруженных дефектов.

Исследователи в работах [8], [9] определили набор определённых текстурных признаков, в качестве классификатора использовали SVM.

Для решения задач классификации используются нейронные сети глубокого обучения (Deep Neural Network – DNN) [10]-[11]. В работе [10] представлена система визуального контроля для автоматического обнаружения дефектов сварки, в которой для классификации используются как традиционные методы компьютерного зрения, так и классификатор на основе DNN. В работе [11] признаки поверхностных дефектов извлекаются CNN (Convolutional Neural Network), а

классификация осуществляется с помощью алгоритма Random forest («случайный лес»).

На результат классификации влияет выбор классификатора, который зависит от входных изображений, их количества, наличия шумов, требований к скорости обработки и принятия решений.

Для описания изображений дефектов сварных соединений предлагается использовать текстурные признаки, основанные на статистических характеристиках. Статистические признаки вычисляются на основе матриц смежности уровней серого (Gray Level Co-occurrence Matrix – GLCM). GLCM представляет собой оценку плотности распределения вероятностей второго порядка, полученную по изображению в предположении, что плотность вероятности зависит лишь от расположения двух пикселей. Из матриц смежности уровней серого размером $N_g \times N_g$ извлекаются текстурные признаки Харалика (статистики второго порядка) [13].

После обнаружения дефекта на изображении (кадре) происходит извлечение признаков: energy, contrast, correlation, sum of squares, homogeneity, sum average, sum variance, sum entropy, entropy, difference variance, difference entropy, information measure of correlation 1, information measure of correlation 2.

Для обучения классификатора предлагаются методы машинного обучения SVM и ANN. Для обучения классификатора и получения высокой точности классификации необходимо накопление достаточного объёма обучающей и тестовой выборок.

Результаты и дальнейшая работа

Предложенный алгоритм автоматического обнаружения дефектов сварных соединений, расчёт значений текстурных признаков реализованы на языке программирования C# в среде Visual Studio 2019, с использованием EmguCV и Accord.NET Framework.

Алгоритм протестирован на видеопоследовательностях, содержащих кадры сварных соединении без дефектов и с дефектами.

На рис. 3 представлены некоторые результаты работы предложенного алгоритма на основе метода вычитания фона.

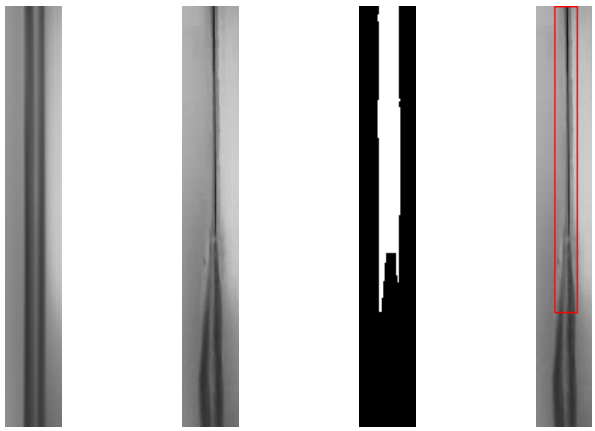
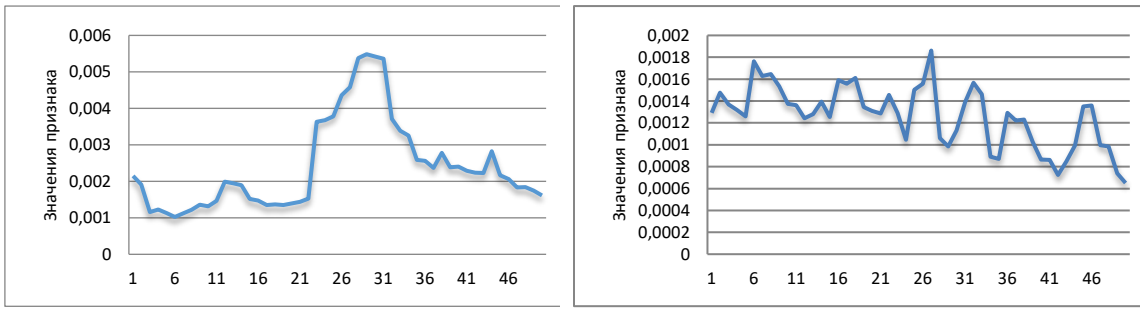


Рис. 3 Результаты обнаружения дефекта в сварном соединении на кадре видеопоследовательности: а) модель фона; б) полутоновое изображение сварного

соединения с дефектом; в) обработанное бинарное изображение; г) выделение дефектной области

В процессе экспериментальных исследований на вход алгоритма подавалось несколько тысяч кадров. На всех кадрах, содержащих дефекты, были выделены дефектные области, ложных обнаружений не было.

На рис. 4 представлены графики, построенные по значениям текстурного признака energy, полученных из областей изображений, содержащих дефекты несплавление и окисление металла.



а) б)

Рис. 4 Некоторые результаты извлечения признака energy при: а) несплавлении, б) окислении металла

Представленный в работе алгоритм позволяет решить задачу автоматического обнаружения дефектов сварных соединений на кадрах видеопоследовательностей. Значения текстурных признаков Харалика, извлекаемые из областей изображений, содержащих дефекты, могут быть использованы как компоненты векторов признаков для описания дефектов сварных соединений при решении задачи классификации.

Дальнейшая работа предполагает накопление данных для обучения и тестирования классификаторов на основе SVM, ANN, построение моделей, анализ результатов.

ЛИТЕРАТУРА

ISO 17637:2016. Non-destructive testing of welds – Visual testing of fusion-welded joints.

1. ГОСТ Р ИСО 17637-2014. Контроль неразрушающий. Визуальный контроль соединений, выполненных сваркой плавлением. – Введ. 2016-01-01. – М.: Стандартинформ, 2015.
2. ISO 6520-1:2007. Welding and allied processes – Classification of geometric imperfections in metallic materials – Part 1: Fusion welding.
3. ГОСТ Р ИСО 6520-1-2012. Сварка и родственные процессы. Классификация дефектов геометрии и сплошности в металлических материалах. Часть 1. Сварка плавлением. – Введ. 2014-01-01. – М.: Стандартинформ, 2014.
4. Hou, W. Review on computer aided weld defect detection from radiography images / W. Hou, D. Zhang, Y. Wei, J. Guo, X. Zhang // *Applied Sciences,* 2020. – Vol. *10. – N. 5.* – P. 1878. DOI: 10.3390/app10051878.
5. Muravyov, S. V. Computer-Aided Recognition of Defects in Welded Joints during Visual Inspections Based on Geometric Attributes / S. V. Muravyov, E. Y. Pogadaeva // Russian

Journal of Nondestructive Testing, 2020. – Vol. 56, N. 3. – P. 259–267. DOI: 10.1134/S1061830920030055

6. Sun, J. An effective method of weld defect detection and classification based on machine vision / J. Sun, C. Li, X.J. Wu, V. Palade, W. Fang // IEEE Trans. Ind. Inform, 2019. – Vol. 15. – N.12. – P. 6322-6333. DOI: 10.1109/TII.2019.2896357

7. Valavanis, I. Multiclass defect detection and classification in weld radiographic images using geometric and texture features / I. Valavanis, D. Kosmopoulos // Expert Systems with Applications, 2010. – Vol. 37, N.12. – P. 7606–7614. DOI: 10.1016/j.eswa.2010.04.082.

8. Jiang, H. Weld defect classification based on texture features and principal component analysis / H. Jiang, Y. Zhao, J. Gao, W. Zhao // Insight - Non-Destructive Testing and Condition Monitoring, 2016. – Vol. 58, N. 4. – P. 194-200. DOI:10.1784/insi.2016.58.4.194.

9. Sassi, P. A smart monitoring system for automatic welding defect detection / P. Sassi, P. Tripicchio, C. A. Avizzano // IEEE Transactions on Industrial Electronics, 2019. – Vol. 66, N. 12. – P. 9641-9650. DOI: 10.1109/TIE.2019.2896165.

10. Zhu, M. Deep Learning-Based Classification of Weld Surface Defects / M. Zhu, W. Ge, Z. Liu // *Applied Sciences,* 2019. – Vol. 9, P. 3312. DOI: 10.3390/app9163312.

11. Xu, Y. Background modeling methods in video analysis: a review and comparative evaluation / Y. Xu, D. Jixiang, B. Zhang, D. Xu // CAAI Transactions on Intelligence Technology, 2016. – Vol. 1, P. 43-60. DOI: 10.1016/j.trit.2016.03.005

12. Haralick, R. M. Textural Features for Image Classification / R. M. Haralick, K. Shanmugan, I. Dinstein. //IEEE Transactions on systems, man and cybernetics, volume SMC-3. – IEEE, 1979. – N. 6. – P. 610-621. – ISSN 0018- 9472.

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ НА ТЕРРИТОРИИ РЕСПУБЛИКИ КАЗАХСТАН

Каражанов Куаныш Жумагулулы.
e-mail: k_karazhanov-75@mail.ru
Академия комитета национальной безопасности Республики Казахстан, Казахстан

Аннотация: *данным докладом приводятся проблемные аспекты внедрения, применения технологий искусственного интеллекта в сфере обеспечения общественной безопасности.*

Изучая вопрос определения искусственному интеллекту (ИИ), имеющее международное юридическое обоснование или стандарт терминологий *унифицирующий «язык» на котором общается сообщество,* в информационном поле найдены разные варианты определений в разных интерпретациях.

Учитывая тематику доклада и ее дальнейшее развитие, предлагается *рассматривать ИИ как область информатики, которая занимается разработкой интеллектуальных компьютерных систем, то есть систем, обладающих возможностями, которые мы традиционно связываем с человеческим разумом, — понимание языка, обучение, способность рассуждать, решать проблемы и т. д.*

Известно, что ИИ позволяет компьютерам обучаться на собственном опыте, адаптироваться к задаваемым параметрам и выполнять те задачи, которые раньше были под силу только человеку.

В июне 2017 г. Госсовет КНР выпустил «Программу развития искусственного интеллекта нового поколения», в которой сказано, что искусственный интеллект стал новой сферой международной конкуренции. Это стратегическая технология, которая будет определять будущее развитие, международную конкурентоспособность страны, а также ее национальную безопасность и уровень влияния в мире[1].

Но пока еще степень использования AI низкая. Наилучшие варианты использования AI на предприятиях варьируются от «автоматизированных агентов обслуживания клиентов» до «автоматизации IT» и «анализа и расследования случаев мошенничества».

В целом делается вывод, что AI поможет улучшить бизнес сегодня и завтра: повысить конкурентоспособность, улучшить взаимодействие с клиентами, ускорить инновации, повысить рентабельность и производительность сотрудников[2].

[1] РСМД, Леонид Ковачич, Китай упустил промышленную революцию-не пропустит цифровую, https://russiancouncil.ru/analytics-and-comments/analytics/kitay-upustil-promyshlennuyu-revolyutsiyu-ne-propustit-tsifrovuyu

[2] Статья на ITenterprise, Искусственный интеллект (ИИ, artificial-intelligence, AI) https://www.idc-community.com/2019/03/22/artificial-intelligence-15-takeaways-from-agenda19-to-help-you-succeed-with-ai/

В настоящее время трудно найти сферу работы людей, в которой не применяются разные механизмы и машины, облегчающие труд человека или выполняющие за него какие-либо действия. Вероятно, скоро количество таких агрегатов существенно возрастёт, и применяться они станут практически везде.

Масштабы и сферы применения технологий ИИ - безграничны. Естественно, что особенностями применения ИИ является многочисленность нюансов использования ИИ, которые связаны с конкретикой каждой отдельной системы и решаемых ею задач. Но есть и общие положения, касающиеся фактически каждой области применения. В рамках данного доклада хотелось бы их максимально сузить и выделить сферы деятельности, из числа имеющих наиболее широкое и распространенное применение.

МЕДИЦИНА;
ПРОМЫШЛЕННОСТЬ;
ТРАНСПОРТ;
ОБЕСПЕЧЕНИЕ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ.

В каждой сфере ИИ может применяться и применяется практически на всех уровнях и учитывая обширность каждой сферы и уровней применения ИИ, хотелось бы также вкратце привести некоторые примеры.

Медицина:

Внедряемые и применяемые в настоящее время в современной медицине системы ИИ не только дают рекомендации докторам на основе анализа и поиска нужных решений, но и выявляют вероятность заболевания пациента на сверх ранней стадии, когда выявить её человеку практически невозможно. Анализируют данные диагнозов, отслеживают течение лечебных процедур и многое другое.

Промышленность:

ИИ в области промышленного производства – это повсеместная автоматизация производства, вплоть до полного исключения людей из этого процесса. В данной сфере ИИ позволяет контролировать процесс от покупки необходимых материалов до контроля качества товара и его отправки по назначению. Кроме того, ИИ может контролировать выработку (износ) производственных механизмов и другие параметры вплоть до контроля выполнения заданного плана

Транспорт:

Практически все виды транспорта, включая наземные, водные и воздушные на сегодня имеют вспомогательные функции основанные на ИИ, такие как контроль за техническим состоянием транспорта, агрегатов, расходом энергии, управлением ресурсами, навигацией, оптимизации приложений управления дорожным трафиком и т.д., что в свою очередь, создает оптимизацию всех процессов на транспорте. Мы можем наблюдать, как разрабатываются полностью автономные автомобили, железнодорожный транспорт, летательные аппараты. Тенденция развития ИИ на транспорте в перспективе обеспечит безопасную, эффективную и надежную транспортировку, также минимизируя пагубное воздействие на окружающую среду и общество. Внедрены технологии беспилотного движения транспорта.

Обеспечение общественной безопасности:

Одна из сфер, где наблюдается прогресс внедрения и развития технологий ИИ это – сфера обеспечения общественной безопасности. Область, где применяется ИИ для выявления, пресечения неправомерных действий и их расследование. Результаты одного исследования показали, что сотрудники, которые крадут или совершают преступления, отрицательно влияют на всех остальных (другие сотрудники начинают копировать подобную форму поведения). ИИ может

рассматривать данные организационной сети (электронную переписку, комментарии) и выявлять стрессовые зоны, возможные нарушения этических норм и многие другие формы риска несоблюдения установленных требований, а также выделять «красные зоны» для кадровых служб или директоров по обеспечению контроля за соблюдением требований, чтобы они имели возможность вмешаться для предотвращения недобросовестных действий. (Среди поставщиков в данной области такие компании, как TrustSphere, Keencorp, Volley, Cornerstone и др.)

Изучив обсуждаемые и исследуемые сообществом проблемы применения технологий ИИ в той или иной сфере, хотелось бы представить вопрос внедрения технологий ИИ в обеспечение общественной безопасности на территории Республики Казахстан.

В Республике Казахстан осуществляется активное развертывание вспомогательных средств в правоохранительной системе[3], направленных на обеспечение общественной безопасности, построенных на технологиях ИИ. Приказом министра внутренних дел Республики Казахстан, от №897-2018г.[4], принята Программа по развитию в городах систем мониторинга общественной безопасности. Данным Приказом, утверждены цель и задача создания системы мониторинга общественной безопасности, где последовательное расширение и совершенствование имеющегося технического обеспечения, создания единой координирующей платформы является одной из целей. А в числе основных задач системы мониторинга общественной безопасности обозначены функции наблюдения и своевременного информирования заинтересованных служб о зафиксированных событиях и состоянии общественной безопасности.

В реализацию достижения данных целей и решения задач, внедряются и развиваются такие системы как: выявление нарушений правил дорожного движения, распознавание образов и обработка изображений, биометрия, интеллектуальные системы управления, распознавание лица, распознавание речи.

Акцентировать свое внимание хотелось бы на системе видеонаблюдения включающей в себя интеллектуальные технологии, позволяющих отслеживать движущиеся, удаляющиеся или появляющиеся объекты, анализировать траектории движения, нестандартное поведение людей, автоматическая регистрация потенциально опасных предметов, распознавание номеров транспортных средств, обнаружение и фиксацию нарушений правил дорожного движения и т.д.

Известно, что применяемые на сегодня системы «интеллектуального» видеонаблюдения, направленных на обеспечение общественной безопасности на территории Республики Казахстан, ограничены в своих функциональных возможностях в связи с необходимостью обязательного подтверждения каждой применяемой системы (технологии) соответствия техническому регламенту и установленным стандартам, соответственно легитимность их применения государственными органами (в данном случае органы внутренних дел) требует

[3] В соответствии с Законом РК от 06.01.2012 г. «О национальной безопасности Республики Казахстан», органы внутренних дел Республик Казахстан, наделены полномочиями исполнительного органа, осуществляющему охрану общественного порядка, в также межведомственную координацию деятельности по обеспечению общественной безопасности.

[4] Приказ министра внутренних дел РК от 10 января 2018 года № 897 «Об утверждении Программы по развитию в городах систем мониторинга общественной безопасности».

прохождения обязательной сертификации[5] в рамках национального технического регулирования.

Касательно вопроса существующего порядка и правил подтверждения соответствия продукции, Приказом Министра по инвестициям Республики Казахстан, утверждены Правила подтверждения соответствия[6], применяемым при подтверждении продукции или услуг (в виде декларирования соответствия или сертификации) требованиям, установленным техническими регламентами, стандартами или условиями договоров, в части требований к продукции и взаимосвязанным с продукцией процессами, нерегулированных техническими регламентами ЕАЭС, международными соглашениями об обороте различных видов продукции и другими документами, составляющих нормативную базу ЕАЭС в области технического регулирования.

Подтверждение соответствия той или иной продукции установленным требованиям является продолжительным процессом, требующим временных и материальных затрат, что негативно сказывается, на государственном развитии технологий ИИ.

Из известных технологий «интеллектуального» видеонаблюдения, применяемых в РК в рамках обеспечения общественной безопасности можно представить:

Pelco Indura[7]

детекторы для мониторинга дорожного движения (сертифицированная система):

детектор аварий;
проезд сплошной;
движение по полосе движения встречного направления;
неправильная парковка;
превышение скоростного режима;
пересечение стоп-линий на запрещающий сигнал светофора;
отслеживание пробок;
контроль трафика (распознавание и фиксация государственных номеров проезжающего автотранспорта);
и др. виды фиксации действий водителей и событий на дороге.

Кроме того, технологии Pelco Indura функционально имеют следующие опции детекторов, которые могут быть использованы в обеспечении общественной безопасности **(несертифицированы)**:

режим «праздношатание» - определяет, когда люди или транспортные средства остаются в определенной зоне дольше, чем установлено в системе;
детекция скопления людей;
режим фиксации абнормального поведения-драка, резкое перемещение человека за короткий период времени;
фиксация упавшего человека;
удаление объекта из зоны наблюдения;
оставленный или появившийся предмет

[5] п.п. 11) Закона РК от 30 декабря 2020 года №396-IV «О техническом регулировании».
[6] Приказ Министра по инвестициям и развитию РК от 12 октября 2018 года «Об утверждении правил подтверждения соответствия».
[7] НТЦ-NTC НП новые проекты, система интеллектуального видеонаблюдения для государственной безопасности и крупных бизнес структур, https://www.ntc-np.kz/index.php?option=com_content&view=article&id=24&ltemid=15&lang=ru

Аппаратно-программный комплекс автоматического распознавания государственных регистрационных знаков транспортных средств и фото – «Сергек»[8]:

детекторы для мониторинга дорожного движения (сертифицированная система):

определение скоростного режима;
проезд сплошной;
движение по полосе движения встречного направления;
движение по полосе «BUS LANE»;
пересечение стоп-линий на запрещающий сигнал светофора;
контроль трафика (распознавание и фиксация государственных номеров проезжающего автотранспорта);
распознавание государственных номеров
и др. виды фиксации действий водителей и событий на дороге.

Видеокамеры системы АПК «Сергек» устанавливаются не только на дорогах для мониторинга дорожного движения, но и в общественных местах.

Установленные и применяемые в обеспечении общественной безопасности технологии и системы могут быть интегрированы между собой, модернизированы и усовершенствованы, например технологиями бизнес-аналитики, интеллектуальными системами информационной безопасности, машинный перевод и т.д. (несертифицированы).

Так как каждая из систем имеет уже разработанные и установленные в них дополнительные технологии ИИ, не предусмотренных в официально применяемых, их использование позволило бы снизить правонарушения на основании прогнозирования и выявления тех или иных фактов, а также увеличить количество раскрываемых преступлений.

К таким технологиям относятся системы распознавания личности по лицу, речи, голосу, радужке глаз, отпечатка пальцев.

При этом, в целях перспективного усовершенствования можно будет расширить возможности комплексов, разрабатываемыми специалистами мирового сообщества системами распознавания личности по походке и другим физиологическим признакам человеческого тела (телосложение, конечности, очертания головы и т.д.).

Технологии искусственного интеллекта широко востребованы в самых разных отраслях. Среди основных факторов, сдерживающих их полномасштабное практическое использование - неразвитость нормативной базы. При этом именно проработанная нормативно-техническая база обеспечивает заданное качество применения технологии и соответствующий эффект.

С учетом сфер и масштабов применения технологий ИИ, их скорость развития в той или иной области, любая из них, внедряющая у себя технологии ИИ имеет огромные преимущества перед теми, кто их не использует или не внедряет.

В целях расширения возможностей, применяемых в Республике Казахстан систем и технологий, направленных на обеспечение общественной безопасности, ускорения процессов подтверждения и стандартизации внедряемых продуктов,

[8] Tengrinews, Разбираемся в «Сергек»: Как измеряется скорость, помогут ли антирадары. – https://www.tengrinews.kz/kazakhstan_news/razbiraemsya-sergek-izmeryaetsya-skorost-pomogut-antiradaryi-327753/amp/

необходимо усовершенствовать нормативно-правовую базу технического регулирования и действующего порядка сертификации. При этом, в процессе разработки проектов привлекать независимых специалистов из сторонних организаций, квалифицированных (сертифицированных) в области IT/AI-технологий.

Литература (использованы источники из INTERNET):

1. ITenterprise, Искусственный интеллект (ИИ, artificial-intelligence, AI) https://www.idc-community.com/2019/03/22/artificial-intelligence-15-takeaways-from-agenda19-to-help-you-succeed-with-ai/, просмотр 17 августа 2021года.

2. РСМД, Леонид Ковачич, Китай упустил промышленную революцию-не пропустит цифровую, https://russiancouncil.ru/analytics-and-comments/analytics/kitay-upustil-promyshlennuyu-revolyutsiyu-ne-propustit-tsifrovuyu, просмотр 18 августа 2021года.

3. НТЦ-NTC НП новые проекты, система интеллектуального видеонаблюдения для государственной безопасности и крупных бизнес структур, https://www.ntc-np.kz/index.php?option=com_content&view=article&id=24&ltemid=15&lang=ru, просмотр 19 августа 2021 года.

4. Tengrinews, Разбираемся в «Сергек»: Как измеряется скорость, помогут ли антирадары. – https://www.tengrinews.kz/kazakhstan_news/razbiraemsya-sergek-izmeryaetsya-skorost-pomogut-antiradaryi-327753/amp/, 20 августа 2021 года.

НЕКОТОРЫЕ ПРОБЛЕМЫ РАБОТЫ С БАЙЕСОВСКИМИ СЕТЯМИ

Мамырбаев О.Ж., Шаяхметова А.С., Литвиненко Н.Г.
asemshayakhmetova@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Искусственный интеллект широко используется при решении различных проблем в различных областях науки, экономики, производства и общественной жизни. Наиболее популярным направлением использования искусственного интеллекта с начала 2000 годов стало использование в исследованиях аппарата байесовских сетей. Во многом это обусловлено наличием неопределенностей в большинстве изучаемых проблем, желанием исследователей получать вероятностные оценки различных факторов изучаемых процессов, понимать зависимости между различными изучаемыми факторами. Байесовские сети позволяют решить эти и многие другие проблемы*.

Введение

В различных областях науки и прикладных исследованиях байесовские сети являются мощным инструментом для изучения сложных процессов, обладающих причинно-следственными вероятностными связями. Возникла потребность в программных инструментах, обеспечивающих реализацию моделей, основанных на аппарате байесовских сетей. Рынок программных продуктов быстро отреагировал на данную потребность. Появилось много прекрасных программных продуктов для работы с байесовскими сетями [1]. Одним из таких продуктов является AgenaRisk. В данной работе приводится пример учебной модели на программном инструменте AgenaRisk.

Цель данной работы рассмотреть типичные задачи, решаемые с использованием байесовских сетей, а также некоторые элементарные способы использования сетей.

Рассматривается учебная модель Wet Grass. Данная модель также используется во многих статьях и книгах, как пример в различных программных продуктах [2,3]. Байесовская сеть, соответствующая данной модели, приведена на рисунке 1.

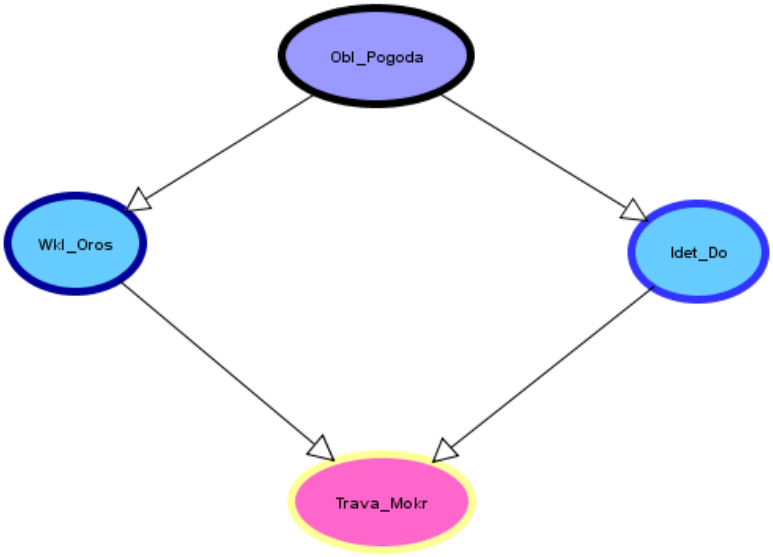


Рис. 1 Модель предложенной байесовской сети

Байесовская сеть очень простая: содержит всего четыре узла и четыре дуги. Опишем содержательную часть модели.

Требуется отслеживать, чтобы на лужайке была мокрая трава. Трава может быть мокрой, если пошел дождь, или потому что включена дождевальная установка. Узлы байесовской сети представляют переменные. Априорно для данных узлов известно:

- С вероятностью 30% стоит облачная погода.
- С вероятностью 10% идет дождь.
- С вероятностью 70% работает дождевальная установка.
- С вероятностью 90% трава мокрая.

Здесь пока не учтены вероятностные связи между узлами. Они приведены ниже.

- Существует вероятностная зависимость между облачной погодой и дождем.

Облачно	Идет дождь	
	Да	Нет
Да	0.30	0.70
Нет	0.05	0.95

- Существует вероятностная зависимость между облачной погодой и включенной дождевальной установкой. В пасмурную погоду установка с большой вероятностью будет выключена.

Облачно	Установка включена	
	Да	Нет
Да	0.60	0.40
Нет	0.80	0.20

- Существует вероятностная зависимость между дождем, включенной установкой и мокрой травой.

Установка включена	**Идет дождь**	Трава мокрая Да	Нет
Да	**Да**	0.95	0.05
Да	**Нет**	0.70	0.30
Нет	**Да**	0.80	0.20
Нет	**Нет**	0.05	0.95

Вероятностные связи приведут после пересчета к новым (апостериорным) значениям узлов (рисунок 2).

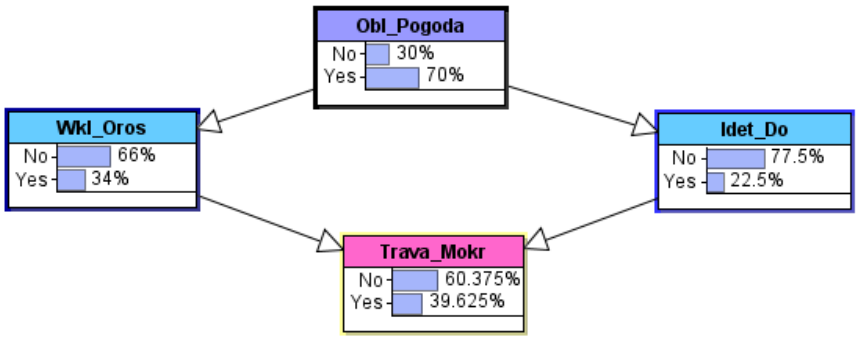


Рис. 2 Вероятностная связь узлов

Данные для узлов примут следующие значения:

- С вероятностью 30% стоит облачная погода.
- С вероятностью 22.5% идет дождь.
- С вероятностью 66% работает дождевальная установка.
- С вероятностью 57.875% трава мокрая.
- Неожиданный результат. Априорные знания были весьма неточны.

Алгоритм построение данной байесовской сети

Шаг 1. Запускаем программу AgenaRisk. В всплывающем списке выбираем режим No Action. (Рисунок 3).

Шаг 2. Выбираем пункт меню File | Create New Model.

На вертикальном меню панели Risk Map выбираем кнопку с овалом (новый узел сети) и в нужном месте панели Risk Map кликаем левой кнопкой мышки. Получим стандартное изображение узла. Исправляем некоторые свойства данного узла.

Шаг 3. На панели Risk Map вызываем контекстное меню (правая кнопка мышки), и выбираем пункт Properties.

Шаг 4. В пункте Node Details изменяем имя узла (Рисунке 4).

Шаг 5. В пункте Node States изменяем статус узла на Yes|No.

Шаг 6. В пункте Node Probability Table заполняем таблицу вероятностей для данного узла. Считаем равновероятным, что погода будет облачной или ясной.

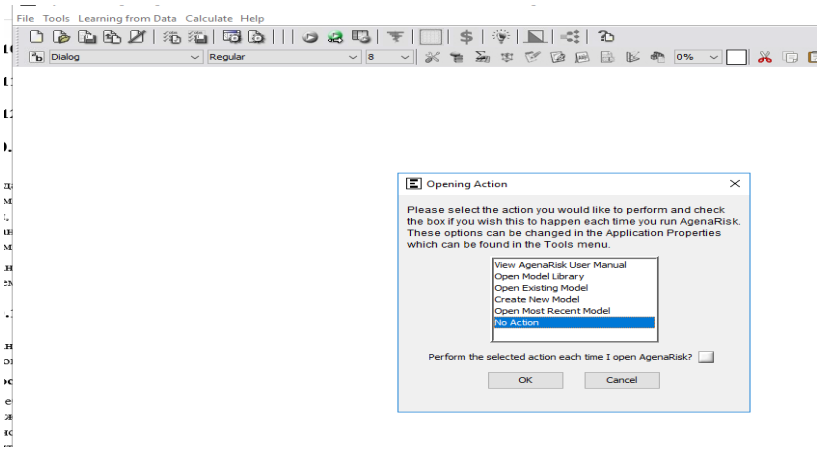


Рис. 3 Окно Opening Action

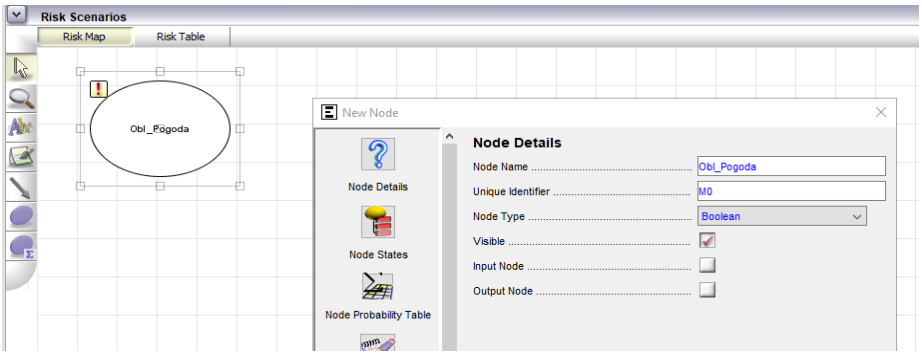


Рис. 4 Окно Node Details

Узел будет иметь вид как на рисунке 5.

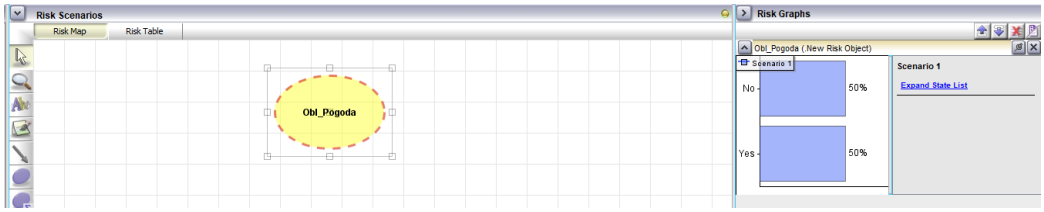


Рис. 5 Вид готового узла

Остальные узлы можно построить аналогичным способом.

2 Типы моделирования в AgenaRisk

Современные алгоритмы, реализованные в AgenaRisk, позволяют выполнять следующие типы решения проблем и моделирования [4]:

- Представление экспертного суждения с использованием субъективной вероятности.
- Объединение данных с экспертной оценкой.
- Моделирование статистических распределений для прогнозного вывода, как альтернатива моделированию Монте-Карло.
- Диагностический вывод для приложений машинного обучения.

- Иерархическое моделирование, как альтернатива цепям Монте-Карло Маркова (MCMC).
- Построение гибридных моделей, содержащих дискретные и непрерывные неопределенные переменные.
- Смешанное моделирование дискретных и непрерывных распределений.
- Объектно-ориентированное моделирование сложных систем с участием нескольких объектов и интерфейсов.
- Динамическое моделирование основанных на времени или развивающихся систем (таких как анализ Маркова).

3 Сравнение байесовских и нейронных сетей

Принципиальное различие между двумя типами сетей состоит в том, что персептрон в скрытых слоях не имеет логической пользовательской интерпретации, тогда как все узлы байесовской сети представляют понятия, которые хорошо известны исследователю и достаточно четко определены в изучаемой области [5]. Значения узлов и таблицы вероятности узлов байесовской сети могут быть предметом обсуждения независимо от их функций в сети. Но нет смысла обсуждать значения узлов и весов в нейронной сети.

Построение байесовской сети требует четкого знания изучаемой области. Если знания образуются лишь на основе обучения, более разумно использовать нейронные сети [6].

Сложность построения байесовской сети заключается в том, что для этого необходимо знать слишком много, порой достаточно сложных, таблиц вероятностей [7]. Аналогично, для построения нейронных сетей требуется знать множество весов и порогов, полученных лишь с помощью обучения. В нейронных сетях нельзя использовать ранее полученные знания [8].

В байесовских сетях вероятности могут быть оценены с использованием комбинации теоретического понимания изучаемого процесса, эмпирических исследований, независимых от построенной системы, обучения и различных субъективных оценок экспертов [9,10].

В нейронных сетях достаточно жестко определены входные узлы, выходные узлы, расчетные узлы. В байесовских сетях подобного жесткого деления узлов нет. Практически любой узел байесовской сети может получать входную информацию, или быть промежуточным узлом, или быть узлом, содержащим результаты расчетов.

Заключение. Таким образом, при байесовском подходе все величины и параметры считаются случайными, так как на практике точное значение параметров распределения обычно нам не известно.

Байесовский подход работает даже тогда, когда невозможно провести ни одного испытания. При проведении различных испытаний мы накапливаем различные знания об исследуемом событии. Байесовский подход позволяет постепенно уточнять вероятность исследуемого события на основании вновь полученных знаний. При этом испытания могут лишь косвенно отражать суть исследуемого события.

Работа выполнена по проекту ГФ AP09259309 «Информационная модель и программный инструментарий системы автоматического поиска и анализа многоязычного противоправного веб-контента на базе онтологического подхода» (2021-2023).

Литература

1 Литвиненко Н.Г., Литвиненко А.Г., Мамырбаев О.Ж., Шаяхметова А.С. Работа с Байесовскими сетями в BAYESIALAB / Н.Г. Литвиненко – Алматы: ИИВТ, 2018. – 311 с.

2 Fenton N., Neil M. Risk Assessment and Decision Analysis with Bayesian Networks. - Queen Mary, University of London and Agena Ltd. CRC Press. - ISBN: 9781439809105, ISBN 10: 1439809100

3 Джарратано Д., Райли Г. Экспертные системы: принципы разработки и программирования / Д. Джарратано - Издательский дом Вильямс. - ISBN: 978-5-8459-1156-8, 2007. -1152 с.

4 Рассел С., Норвиг П. Искусственный интеллект: современный подход / С. Рассел - Издательский дом Вильямс, ISBN: 5-8459-0887-6, 2006. -1408 с.

5 Гнеденко Б.В. Курс теории вероятностей / Б.В. Гнеденко – М.: Едиториал УРСС, 2005. – 448 с.

6 Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман – М.: Высш. шк., 2013. - 479 с.

7 Кремер Н.Ш. Теория вероятностей и математическая статистика / Н.Ш. Кремер – М.: ЮНИТИ-ДАНА, 2014. – 573 с.

8 Карпов Д.В., Теория графов. - https://logic.pdmi.ras.ru/~dvk/graphs_ dk.pdf (01.08.2021)

9 Diestel R. Graph Theory, Electronic Edition / R. Diestel - NY: Springer-Verlag, 2015. – 422 p.

10 Barber D. Bayesian Reasoning and Machine Learning. - http://web4.cs.ucl.ac.uk/staff/D.Barber/textbook/090310.pdf (01.08.2021)

РАСПОЗНАВАНИЯ КАЗАХСКОЙ РЕЧИ НА ОСНОВЕ ИНТЕГРАЛЬНОЙ МОДЕЛИ RNN-T

Мамырбаев О.Ж.[1,2], Оралбекова Д.О.[1,3], Othman M.[4], Тулендиев Д.М.[1], Жумажанов Б.[1], Турдалыкызы Т.[1]
e-mail: morkenj@mail.ru, dinaoral@mail.ru, d.tulendiyev@gmail.com
[1]*Институт информационных и вычислительных технологий КН МОН РК, Казахстан*
[2]*Казахский национальный университет им. аль-Фараби, Казахстан*
[3]*Satbayev University, Казахстан*
[4]*Universiti Putra Malaysia, Kuala Lumpur, Malaysia*

Аннотация. *Самыми популярными системами распознавания речи на сегодня являются системы на основе интегральной (end-to-end) архитектуры, а именно те модели, которые напрямую выводят последовательность слов с учетом входного звука в режиме реального времени, что представляют собой онлайновые модели end-to-end. Распознавание потоковой речи позволяет передавать поток звука в преобразование речи в текст и получать результаты распознавания речи потока в реальном времени по мере обработки звука. В данной статье рассмотрена и реализована популярная модель на основе RNN-T для распознавания казахской речи. Также приведен анализ работ, связанные с распознаванием казахской речи на основе модели CTC. Полученные результаты продемонстрировали, что модель на основе RNN-T может хорошо работать без дополнительных компонентов, и показала лучший результат на нашем наборе данных.*

1 Введение. В современном мире распознавание речи играет значимую роль при взаимодействии человека с машиной и техникой. Целью распознавания речи является конвертирование человеческой речи в машиночитаемый формат. Технология speech to text применяется в широких кругах задач, как управление интерфейсом, голосовой поиск, синтез речи и т.д.

До появления глубокого обучения, в задачах распознавания речи широко использовалась модель на основе скрытых марковских моделей (HMM) с гауссовским распределением плотностей вероятностей (GMM). Глубокие нейронные сети начали применять для акустического моделирования вместо GMM, что привело к улучшению результатов [1]. Архитектура HMM-DNN стало одной из распространенной моделью в задаче распознавания слитной речи.

Вскоре распространение получила другая модель, которая является интегральной моделью. В исследовательской работе [2] для построения акустической модели использовались только DNN, а в работах [3, 4] с помощью других архитектур искусственных нейронных сетей (ИНС) были реализованы языковые модели и словари. Кроме того, для выделения признаков из исходного сигнала использовались свёрточные нейронные сети [5]. Из этого следует, что для разработки системы автоматического распознавания речи можно применять разные архитектуры ИНС на всех этапах распознавания, и это делает ее эффективной с точки зрения производительности по сравнению с другими популярными системами. И это является интегральным подходом.

Модели на основе коннекционной временной классификации [6] (CTC), рекуррентный нейронный преобразователь [7] (Recurrent Neural Transducer, RNN-T), модели, на основе механизма внимания [8, 9], и модели, на основе условных случайных полей (CRF) [10] являются наглядными примерами интегральных систем.

Существует огромный интерес к обучению интегральных моделей для ASR, которые напрямую выводят последовательность слов с учетом входного звука. Для реализации такой системы применяются онлайн-модели для интегральных систем, наиболее популярным является RNN-T.

Для построения интегральных моделей требуется большое количество речевых данных для обучения сети, что является проблематичной для языков с ограниченными обучающими данными. И одним из этих языков является казахский язык. До сегодняшнего дня были разработаны системы на основе моделей CTC для распознавания казахской речи с разными наборами тренировочных данных. В настоящий момент не существуют исследований и работ по реализации интегральной системы для распознавания казахской речи на основе RNN-T.

В этой работе мы предлагаем модель на основе RNN-T для распознавания казахской речи.

2 Литературный обзор. Архитектура RNN-T состоит из сети транскрипции, сети прогнозирования и объединённой сети. Помимо этого, в данной модели присутствует обратная связь, которая позволяет модели учитывать ранее распознанные символы для передачи их во входную часть сети.

В [11] модель RNN-T показала лучший результат – снижение WER до 15,0%, чем гибридная модель. В работе [12] было обнаружено, что модель RNN-T и RNN-T, дополненный вниманием, сопоставимы по своим характеристикам с сильной современной базовой линией на наборе для тестирования диктовки.

Kanishka Rao и др. [13] обнаружили, что предварительное обучение кодера RNN-T с помощью CTC приводит к относительному улучшению WER на 5%, а использование более глубокого 8-уровневого кодера вместо 5-уровневого кодера дополнительно улучшает относительное значение WER на 10%.

В [14] был представлен RNN-T для распознавания непрерывной речи с большим словарным запасом китайского языка. Для улучшения модели была предложена стратегия для снижения скорости обучения, которая помогает ускорить сходимость модели. В итоге экперимента, система достигла 16,9% CER в тестовом наборе.

В статье [15] была усовершенствовано обучение RNN-T в следующих аспектах: 1) был оптимизирован алгоритм обучения RNN-T, 2) были предложены более улучшенные архитектуры моделей для реализации модели RNN-T с очень высокой точностью, Эта улучшенная модель RNN-T достиг к снижению WER до 15,0%.

3 Модель RNN-T. Reccurent neural transducer **(**RNN-T) был впервые упомянут в работах [7, 16] как модификация модели коннекционной временной классификации (CTC) [3] для задач маркировки последовательностей, где выравнивание между входной последовательностью x и выходными целями l неизвестно. Это достигается в формулировке CTC путем введения дополнительной метки, что является пустой меткой, которая генерирует вероятность вывода метки, соответствующей данному входному кадру. Тем не менее основным ограничением

CTC является его предположение, что выходные данные модели в данном кадре не зависят от предыдущих выходных меток, т.е. являются независимыми: $l_t \perp\!\!\!\perp l_j \mid x$ для $t<j$.

Модель RNN-T состоит из кодера [17], сети прогнозирования и совместной сети; как описано в работе [18], модель RNN-T имеет схожую структуру, как в других архитектурах интегральной модели, как кодер-декодер с механизмом внимания, если декодер можем представить в качестве соединения компонентов сети прогнозирования и объединенной сети. RNN является кодером, который преобразует входные акустические данные в промежуточное представление высокого уровня, и выполняет ту же функцию что и AM в стандартном системе распознавания речи. Следовательно, выходные данные сети RNN, обусловлен последовательностью предыдущих акустических данных, как и в модели CTC. RNN-T исключает предположение об условной независимости в CTC, добавляя компонент сеть прогнозирования RNN, которая явно обусловлена предсказанных историей предыдущих непустых целей модели. К примеру, сеть прогнозирования принимает в качестве входных данных последнюю непустую метку для создания выходных данных. В конце концов, объединенная сеть представляет собой сеть с прямой связью, которая соединяет выходные данные сети прогнозирования и кодера для создания логитов. Затем сопровождается слоем softmax для получения распределения по следующему выходному символу (рис. 1).

В модель RNN-T подается следующий акустический кадр $X = (x_1, ..., x_t)$ для каждого этапа вывода и ранее предсказанная метка l_{m-1}, из которой модель производит следующие вероятности выходных меток $P(l|t, m)$. В случае, если предсказуемая метка является не пустым, то сеть прогнозирования обновляется этой меткой в качестве входных данных для генерации следующих вероятностей выходной метки $P(l|t, m+1)$. И напротив, если будет пустая метка, то следующий акустический кадр применяется для обновления кодера, при этом сохраняются те же выходные данные сети прогнозирования, что приводит к $P(l|t+1, m)$ [14]. Следовательно, данная модель передает полученные результаты распознавания в поток, при этом параллельно обновляя кодера и сеть прогнозирования, в зависимости от того, является ли предсказуемая метка пустой или непустой. Вывод данных прерывается, когда в последнем кадре выводится пробел.

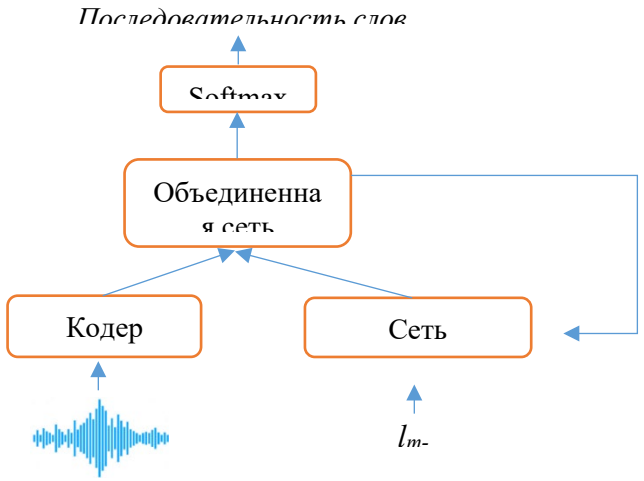


Рисунок 1: Структура RNN-T

Во время логического вывода наиболее вероятная последовательность меток вычисляется с использованием поиска луча, как описано в [18], с незначительным изменением, которое, как было обнаружено, делает алгоритм менее ресурсоемким без ухудшения производительности: мы пропускаем суммирование по префиксам в *pref (l)*, если несколько гипотез не идентичны.

Необходимо обратить внимание, что в отличие от других архитектур потокового кодера-декодера, как Neural Transducer, сеть прогнозирования не зависит от выходных данных кодера. Это позволяет предварительно обучить декодер в качестве языковой модели RNN на текстовых данных.

4 Корпус для обучения. Для обучения модели RNN-T был выбран речевой корпус, который содержит более 300 часов речи, собранный в лаборатории «Компьютерной инженерии интеллектуальных систем» ИИВТ МОН РК [19]. Данный корпус состоит из записей носителей казахского языка разных полов и возрастов; телефонных разговоров с транскрипциями; некоторые записи были взяты с новостных сайтов и художественных аудиокниг.

5 Эксперименты и результаты. Для сравнительного анализа были рассмотрены работы [19, 20], которые связаны к интегральному распознаванию казахской речи (табл.1).

В работе [19] была реализована интегральная модель CTC. Был использован 123-часовой корпус для обучения.

В [20] была построена архитектура на основе RNN с 2 слоями долгосрочной краткосрочной памяти и с 1 плотным слоем в рамках трансферного обучения. Модель была обучена на 20-часовом корпусе казахской речи. В качестве функции потерь была применена CTC.

Таблица 1. Результаты работ по интегральной модели и нашей модели

Model	WER, %	CER, %	Объем данных, ч
Amirgaliyev et al. (LSTM with Russian model)	–	24	20
(BiLSTM with Russian model)	–	32	
Mamyrbayev et al. (MLP	63.26	39.11	126
LSTM	46.51	24.43	
Conv+LSTM	39.31	22.92	
BLSTM	20.66	13.61	
ResNet)	19.57	11.52	
Наша модель (RNN-T)	15.8	10.6	300

Полученные результаты продемонстрировали, что модель RNN-T для казахского языка может отлично работать без дополнительной внешней языковой модели и показала лучший результат по сравнению с другими интегральными моделями.

6 Conclusion. В данной работе представлено текущее состояние интегральных систем распознавания речи, а именно модели RNN-T, для распознавания потоковой речи. Была построена архитектура данной модели с помощью нейронных сетей, как LSTM и BiLSTM. Результаты проделанной работы показали, что реализованная модель может достигать хороших показателей и без применения языковых моделей для казахского языка и превзошла другие интегральные модели, которые были

обучены меньшим объемом речевых данных и показала лучшие результаты по распознаванию казахской речи по точности распознавания символов 10.6%. Помимо этого, система на основе модели RNN-T, позволяет использовать на портативных устройствах, т.к. будет занимать меньший объем памяти.

В дальнейших исследованиях планируется проведение экспериментов других видов интегральных моделей.

7 Благодарности. Работа выполнена при финансовой поддержке Комитета науки Министерства образования и науки Республики Казахстан (грант № AP08855743).

8. Литература

1. Hinton, Geoffrey & Deng, li & Yu, Dong & Dahl, George & Mohamed, Abdel-rahman & Jaitly, Navdeep & Senior, Andrew & Vanhoucke, Vincent & Nguyen, Patrick & Sainath, Tara & Kingsbury, Brian. (2012). Deep Neural Networks for Acoustic Modeling in Speech Recognition. Signal Processing Magazine, IEEE, vol. 29, no. 6.
2. D. Yu and J. Li, "Recent progresses in deep learning based acoustic models," in IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 3, pp. 396-409, 2017, doi: 10.1109/JAS.2017.7510508.
3. W. Ko, B. Tseng and H. Lee, "Recurrent Neural Network based language modeling with controllable external Memory," 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, 2017, pp. 5705-5709, doi: 10.1109/ICASSP.2017.7953249.
4. Sundermeyer, Martin & Schluter, Ralf & Ney, Hermann. (2012). LSTM Neural Networks for Language Modeling.
5. M. Jogin, Mohana, M. S. Madhulika, G. D. Divya, R. K. Meghana and S. Apoorva, "Feature Extraction using Convolution Neural Networks (CNN) and Deep Learning," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 2018, pp. 2319-2323, doi: 10.1109/RTEICT42901.2018.9012507.
6. Graves A., Fernandez S., Gomez F., and Schmidhuber J. Connectionist Temporal Classification: Labelling Unsegmented Sequence Data with Recurrent Neural Networks. In ICML, Pittsburgh, USA, 2006.
7. Graves, Alex & Mohamed, Abdel-rahman & Hinton, Geoffrey. Speech Recognition with Deep Recurrent Neural Networks. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings. 2013.
8. Chorowski J. K., Bahdanau D., Serdyuk D., Cho, K., and Bengio Y. Attention-Based Models for Speech Recognition. In Advances in Neural Information Processing Systems, 2015, pp. 577–585, Montréal, Canada.
9. Wang, D.; Wang, X.; Lv, S. An Overview of End-to-End Automatic Speech Recognition. Symmetry 2019, 11, 1018.
10. E. Fosler-Lussier, Y. He, P. Jyothi, and R. Prabhavalkar, “Conditional random fields in speech, audio, and language processing,” Proceedings of the IEEE, vol. 101, no. 5, pp. 1054–1075, 2013.
11. J. Li, R. Zhao, H. Hu and Y. Gong, "Improving RNN Transducer Modeling for End-to-End Speech Recognition," 2019 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU), SG, Singapore, 2019, pp. 114-121.
12. Prabhavalkar, Rohit & Rao, Kanishka & Sainath, Tara & Li, Bo & Johnson, Leif & Jaitly, Navdeep. A Comparison of Sequence-to-Sequence Models for Speech Recognition. pp. 939-943. 10.21437/Interspeech. 2017-233.

13. Kanishka Rao et al., “Exploring architectures, data and units for streaming end-to-end speech recognition with rnn-transducer,” in 2017 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU). IEEE, 2017, pp. 193–199.

14. S. Wang, P. Zhou, W. Chen, J. Jia and L. Xie, "Exploring RNN-Transducer for Chinese speech recognition," 2019 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Lanzhou, China, 2019, pp. 1364-1369, doi: 10.1109/APSIPAASC47483.2019.9023133.

15. Li, Jinyu & Hu, Hu & Gong, Yifan. (2019). Improving RNN Transducer Modeling for End-to-End Speech Recognition. 114-121. 10.1109/ASRU46091.2019.9003906.

16. Graves, A. Sequence transduction with recurrent neural networks, 2012, arXiv:1211.3711.

17. Y. He et al., "Streaming End-to-end Speech Recognition for Mobile Devices," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom, 2019, pp. 6381-6385.

18. R. Prabhavalkar, K. Rao, T. N. Sainath, B. Li, L. Johnson, and N. Jaitly, “A comparison of sequence-tosequence models for speech recognition,” in Interspeech, 2017.

19. Mamyrbayev O., Alimhan K., Zhumazhanov B., Turdalykyzy T., Gusmanova F. (2020). End-to-End Speech Recognition in Agglutinative Languages. 10.1007/978-3-030-42058-1_33.

20. Kuanyshbay D., Amirgaliyev Y., Baimuratov O. (2020). Development of Automatic Speech Recognition for Kazakh Language using Transfer Learning. International Journal of Advanced Trends in Computer Science and Engineering. 9. 5880-5886. 10.30534/ijatcse/2020/249942020.

ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ОБУЧЕНИЯ

Муратбеков М.М., Барлыбаев А.Б., Алтынбек С.А.
madimm@list.ru, frank-ab@mail.ru, serik_AA@bk.ru

Абстракт

В этой работе рассматривается проблема создания или разработки интеллектуальной системы обучения (ИТС) с применением графической вероятностной модели как основная компонента по части интеллектуального анализа, а также проблемы, которые могут возникнуть при этом.

Ключевые слова: *искусственный интеллект, граф связи, сети Байеса, вывод Байеса.*

Введение

Интеллектуальные системы обучения (ИСО) - это сложные компьютерные программы, которые управляют различными неоднородными видами знаний, от предметной области до педагогических знаний. Следовательно, создание такой системы - непростая задача. Создатели ИСО должны быть хорошо подготовлены, чтобы решать множество проблем, связанных с их процессом создания. Ресурсы необходимые для создания ИСО, поступают из нескольких областей исследований, включая искусственный интеллект, когнитивные науки, образование, человеко-компьютерное взаимодействие и программное обеспечение. Этот междисциплинарный фундамент делает процесс построения ИСО чрезвычайно сложной задачей, учитывая, что авторы могут иметь очень разные взгляды на целевую систему. Некоторые пропагандируют педагогическую точность (гарантируя, что принятие решений при обучении основано на здравых педагогических принципах), в то время как другие сосредоточены на эффективной диагностике ошибок учащихся (с использованием соответствующей структуры знаний и алгоритмов для правильной интерпретации решений учащихся).

Еще в 1999 году специалист-исследователь департамента компьютерных наук Массачусетского университета Том Мюррей в своей работе «Создание интеллектуальных систем обучения: анализ и уровень развития» выделил семь различных классов систем обучения, каждый из которых соответствует разным взглядам создателей ИСО, обусловленным потребностями создателей. Исследование Мюррей ясно показало, что большинство существующих авторских систем было разработано для построения части или целиком определенного класса ИСО. Кроме того, отсутствуют методы и стандартные инструменты, которые могли бы облегчить процесс создания.

Споры о том, улучшает ли обучение использование той или иной технологии передачи образовательной информации продолжаются и среди населения, и у специалистов. С одной стороны, давно признано, что специализированные технологии передачи могут обеспечить эффективный и своевременный доступ к учебным материалам; а другие утверждают, что технологии - это просто средства обучения, которые сами по себе не влияют на успеваемость обучающихся. По сведениям из [16], метааналитические исследования в области медиа показывают, что обучающиеся получают значительную пользу в обучении от аудиовизуальных

или компьютерных носителей, в отличие от обычного обучения; однако те же исследования также предполагают, что причиной этих преимуществ является не средство обучения, а стратегии обучения, встроенные в учебные материалы. Также предполагается, что на обучение больше влияет содержание и учебная стратегия в учебных материалах, чем тип технологии, используемой для преподавания. Чтобы способствовать развитию мышления более высокого порядка онлайн-обучение в сети должно создавать сложные виды деятельности. Такие сложности позволяют учащимся связывать новую информацию со старой; получить осмысленные знания; и использовать свои метакогнитивные способности; следовательно, именно учебная стратегия, а не технология, влияет на качество обучения, с другой стороны, утверждается, что определенные атрибуты компьютера необходимы для того, чтобы дать обучающимся реальные модели и симуляции; таким образом, среда действительно влияет на обучение. Предполагается, что не компьютер сам по себе заставляет студентов учиться, а проектирование реальных моделей и симуляций, а также взаимодействие обучаемых с этими моделями и симуляторами.

Онлайн-обучение позволяет участникам учебного процесса свернуть время и пространство, но учебные материалы должны быть разработаны таким образом, чтобы вовлекать учащегося и способствовать обучению. Метод передачи обеспечивает гибкий доступ из любого места и, как правило, в любое время, но при обучении должны использоваться разумные принципы учебного проектирования. Онлайн-обучение многообещающе, но требует приверженности и ресурсов и должно проводиться правильно. Правильное выполнение означает, что онлайн-учебные материалы должны разрабатываться должным образом, с упором на учащихся и обучение, и что необходимо оказывать адекватную поддержку. Также онлайн-обучение должно иметь высокую достоверность относительно системы идентификации, высокую интерактивность и высокую степень обратной связи.

Для онлайн-обучения использовались разные термины, что затрудняет выработку общего определения. Названия, которые обычно используемые для онлайн-обучения: электронное обучение, интернет-обучение, распределенное обучение, сетевое обучение, дистанционное обучение, виртуальное обучение, компьютерное обучение. Все эти термины подразумевают, что учащийся или находится на расстоянии от наставника или инструктора, или учащийся использует какую-либо технологию (обычно компьютер) для доступа к учебным материалам. Также учащийся использует технологии для взаимодействия с наставником или инструктором и с другими учащимися, и что учащимся предоставляется некоторая форма поддержки.

В литературе есть много определений онлайн-обучения, отражающих разнообразие практик и связанных с ними технологий. Некоторые специалисты определяет онлайн-обучение как учебный материал, который представляется на компьютере, другие определяет онлайн-обучение как новаторский подход к обучению удаленной аудитории с использованием Интернета в качестве среды обучения. Однако онлайн-обучение включает в себя нечто большее, чем просто представление и передачу материалов с использованием Интернета: учащийся и процесс обучения должны быть в центре внимания онлайн-обучения. Исходя из вышесказанных убеждений собирательное определение онлайн-обучение, это использование Интернета:

- для доступа к учебным материалам;
-среда взаимодействия с контентом, преподавателем и другими учащимися;

-для получения поддержки в процессе обучения, чтобы получить знания, сформировать личный смысл и развиваться на основе полученного опыта.

В этой работе будет использоваться больше комбинированный термин «дистанционное обучение в режиме онлайн» или просто «онлайн-обучение» вкратце, подразумевая первое.

Хотя по мнениям специалистов создания общей теории онлайн-обучения почти невыполнимая задача, однако мы здесь будем обсуждать и некоторым образом попытаться систематизировать основы теории образования для разработки эффективных учебных материалов в режиме онлайн. По пути предлагается модель разработки интеллектуальной системы дистанционного обучения в режиме онлайн, основанная на соответствующей теории образования.

По определению Ассоциации по развитию искусственного интеллекта (AAAI-Association for the advancement of artificial intelligence - США) *интеллектуальная система обучения* (ITS- Intelligent Tutoring System) - это *«образовательное программное обеспечение, содержащее компонент искусственного интеллекта* (ИИ). Эти системы достигают своего «интеллекта», представляя педагогические решения о том, как достичь, а также информацию об учащемся. Каждая ИСО как программное обеспечение должна иметь следующие четыре модельных компонента:

- Знание предметной области (предметная модель);
- Знание стратегии обучения (педагогическая модель);
- Знания учащихся (модель учащегося);
- Коммуникационная модель.

Программное обеспечение отслеживает работу студентов, по ходу адаптируя отзывы и подсказки. Собирая информацию об успеваемости конкретного ученика, программа может делать выводы о сильных и слабых сторонах и предлагать доработки». Элемент ИИ - ключевой компонент индивидуализированных систем обучения. За последние десять лет был разработан ряд различных систем, обеспечивающих интеллектуальное обучение. Однако эти системы развивались очень узко с точки зрения предметной области и образовательных целей.

1 Вероятностные графические модели

Здесь мы опишем структуру вероятностных графических моделей, которая обеспечивает механизм использования структуры в сложных дистрибутивах для их компактного описания и таким образом, который позволяет их конструировать и эффективно использовать. Рассмотрим очень простую постановку диагностики обучения, в которой мы сосредоточены на двух видах успеваемости – хорошая и низкая, они не исключают друг друга, поскольку у обучающиеся может быть хорошая и низкая успеваемость, либо даже неуспеваемость. Таким образом, у нас могут быть две случайные величины с двоичными значениями: хорошая успеваемость и низкая успеваемость. У нас также есть 4-значная случайная величина четверть, которая коррелирует как с хорошей успеваемостью, так и с плохой успеваемостью. У нас также могут быть два признака: *онлайн обучение* и *офлайн обучение*, каждый из которых также имеет двоичное значение. В целом, наше вероятностное пространство имеет $2 \times 2 \times 4 \times 2 \times 2 = 64$ значения (см. таблицу 2), соответствующих возможным присвоениям этим пяти переменным. Учитывая распределение успеваемости по этому пространству, мы можем, например, задавать такие вопросы, как, например, насколько вероятно, *что у ученика хороша*

успеваемость, учитывая, что это 4 четверть, и что у него онлайн обучение, он офлайн не занимается; в качестве вероятностного выражения этот запрос будет обозначен

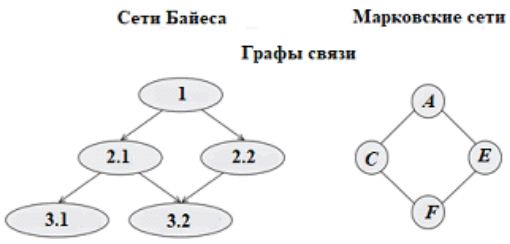
P (хорошая успеваемость = правда|четверть = 4, онлайн обучение = правда, офлайн = ложь).

Таблица 2-Множество значений вероятностного пространства

	признаки	**значения**	**всего**
1	Хорошая успеваемость	да, нет	2^1
2	Слабая успеваемость	да, нет	2^2
3	онлайн	да, нет	2^3
4	офлайн	да, нет	2^4
5	четверть	I, II, III, IV	$4*2^4$
Итого	5	12	64

Вероятностные графические модели используют графическое представление в качестве основы для компактного кодирования сложного распределения в многомерном пространстве. В этом графическом представлении, показанном на рисунке 1, *узлы* (или овалы) соответствуют *переменным* в нашей предметной области, *ребра* соответствуют прямым вероятностным взаимодействиям между ними. Например, рисунок 1а (вверху) иллюстрирует одну возможную структуру графа. На этом графе мы видим, что нет прямого взаимодействия между *онлайн обучением* и *четвертью*, но оба напрямую взаимодействуют с *хорошей успеваемостью*.

Существует двойная точка зрения, которую можно использовать для интерпретации структуры этого графа. С одной стороны, граф - это компактное представление набора зависимостей, которые сохраняются в распределении; эти свойства принимают форму: X не зависит от Y для данного Z (*условная независимость*), обозначается $(X \perp Y|Z)$ для некоторых подмножеств переменных *X, Y, Z.* Например, наше «целевое» распределение *P* для предыдущего примера - кодирование распределения наши представления об этой конкретной ситуации - могут удовлетворить условную независимость



1-четверть **(Q)**, 2.1-хорошая успеваемость **(H)**, 2.2-низкая успеваемость **(P)**, 3.1 –оффлайн **(V)**, 3.2-онлайн **(D)**

Независимость

$(H \perp B|Q)$
$(B \perp Q|D,V)$
$(H \perp V|D)$
$(A \perp F|C,E)$
$(C \perp E|A,F)$

Факторизация

a) $P(Q,H,B,V,D) = P(Q)P(H|Q)P(B|Q)P(B|D,V)P(H|D)$

b) $P(Q,H,B,V,D) = \frac{1}{Z}\phi_1(A,C)\phi_2(C,E)\phi_3(E,F)\phi_4(F,A)$

Рисунок 1. *Различные точки зрения на вероятностные графические модели: вверху - графическое представление; посередине - зависимости, индуцированные структурой графа; внизу - факторизация, вызванная структурой графа. (а) Образец байесовской сети. (б) Условная марковская сеть.*

(онлайн ⊥четверть | хорошая успеваемость, плохая успеваемость).

Это утверждение подтверждает, что

P (онлайн| хорошая успеваемость, плохая успеваемость, четверть) = P (онлайн| хорошая успеваемость, плохая успеваемость);

То есть, если нас интересует распределение вероятности учащегося с онлайн обучением, и мы знаем, его успеваемость, тогда четверть *не является* информативной. Обратите внимание, что это утверждение не означает, что четверть не зависит от онлайн обучения; просто всю информацию необходимую о внедрении онлайн обучения мы получаем от зная успеваемость, не в течении четверти. На рисунке 1а (в центре) показан набор предположений о независимости, связанных с графиком на рисунке 1а (вверху).

Другая перспектива заключается в том, что граф определяет структуру для компактного представления многомерного распределения: вместо того, чтобы кодировать вероятность каждого возможного присвоения (факторного) всех переменных в нашей области, мы можем «разбить» распределение на более мелкие факторы, каждый из которых имеет гораздо меньшее пространство возможностей. Затем мы можем определить общее совместное распределение как произведение этих факторов. Например, на рисунке 1 (а-внизу) показана факторизация распределения, связанного с графиком на рисунке 1 (вверху). Он утверждает,

например, что вероятность события «4 четверть, успеваемость плохая, онлайн обучение, офлайн не ведется» может быть получена путем умножения пяти чисел:
P (четверть = 4),
P (успеваемость плохая = истина| четверть = 4),
P (успеваемость хорошая = ложь| четверть = 4),
P (онлайн = истина | плохая успеваемость = истина, хорошая успеваемость = ложь) и
P (офлайн = ложь | онлайн = истина).

Эта параметризация значительно более компактна, нуждается только 3+ 4+ 4+ 4+ 2 = 17 требуемых параметров, в отличие от 63 требуемых для исходного совместного распределения (64-й параметр полностью определяется остальными, так как сумма по всем значениям в совместном распределении должна составлять 1). Структура графа определяет факторизацию связанного с ней распределения *P* - набора факторов и переменных, которые они охватывают.

Оказывается, что эти две точки зрения - граф как представление взаимосвязей и граф как структура для факторизации распределения - в глубоком смысле эквивалентны. Именно свойства независимости распределения позволяют компактно представить его в факторизованной форме. И наоборот, конкретная факторизация распределения гарантирует сохранение определенных зависимостей.

Мы описываем два семейства графических представлений распределений. Одна из них, называемая *байесовскими сетями*, использует ориентированный граф (где у ребер есть источник и цель), как показано на рисунке 1 (слева вверху). Вторая, называемая сетями Маркова, использует неориентированный граф, как показано на рисунке 1 (справа вверху). Его также можно рассматривать как определение набора утверждений независимости (рисунок 1[справа в середине] или как кодирование компактной факторизации распределения (рисунок 1 [справа внизу]). Оба представления обеспечивают двойственность независимости и факторизации, но они различаются в наборе зависимостей, которые они могут кодировать, и в факторизации распределения, которое они вызывают.

2 Представление, вывод, обучение

Графический язык использует структуру, которая присутствует во многих дистрибутивах, которые мы хотим кодировать на практике: свойство, что переменные имеют тенденцию напрямую взаимодействовать только с малым избранным количеством других переменных. Распределения, которые демонстрируют этот тип структуры, обычно могут быть закодированы естественно и компактно с использованием графической модели. У такой платформы много преимуществ.

Во-первых, это часто позволяет легко записать распределение, даже в тех случаях, когда явное представление совместного распределения является астрономически большим. Важно отметить, что тип представления, обеспечиваемый этой структурой, является прозрачным, поскольку эксперт-человек может понять и оценить его семантику и свойства. Это свойство важно для построения моделей, которые точно отражают наше понимание предметной области. Непрозрачные модели легко могут привести к необъяснимым и даже нежелательным ответам.

Во-вторых, как мы показываем, та же самая структура часто также позволяет эффективно использовать распределение для вывода - ответа на запросы, используя распределение в качестве нашей модели мира. В частности, мы предоставляем алгоритмы для вычисления апостериорной вероятности одних переменных с учетом

данных о других. Например, мы можем заметить, что сейчас весна, и у ученика офлайн обучение, и мы хотим знать, насколько вероятно, что у него будет хорошая успеваемость, вопрос этот формально можно записать как

P (хорошая успеваемость = правда | четверть = 4(весна), офлайн обучение = правда).

Эти алгоритмы вывода работают непосредственно со структурой графа и обычно на порядки быстрее, чем явное манипулирование совместным распределением.

В-третьих, эта структура способствует эффективному построению этих моделей, будь то специалистом-человеком или автоматически, путем изучения данных модели, которая обеспечивает хорошее приближение к нашему прошлому опыту. Например, у нас может быть журнал записей учеников классного руководителя, и мы хотим изучить вероятностную модель, кодирующую распределение, соответствующее нашему совокупному опыту. Вероятностные графические модели поддерживают подход к построению моделей основанный на данных, который очень эффективен на практике. При таком подходе эксперт-человек дает некоторые приблизительные рекомендации по моделированию данной области. Например, человек обычно указывает атрибуты, которые должна содержать модель, часто некоторые из основных зависимостей, которые она должна кодировать, возможно, и другие аспекты. Однако детали обычно заполняются автоматически путем подгонки модели к данным. Модели, созданные с помощью этого процесса, обычно намного лучше отражают предметную область, чем модели, созданные исключительно вручную. Более того, иногда они могут выявить удивительные связи между переменными и предоставить новое понимание предметной области.

Платформы вероятностных графических моделей довольно широки и включают в себя как множество различных типов моделей, так и ряд связанных с ними методов. В этой книге описаны несколько типов моделей. Для каждого из них мы описываем три основных краеугольных камня*: представление, вывод и обучение*.

Выводы

Три основных компонента - *представление, умозаключение и обучение* - являются критическими компонентами при построении интеллектуальной системы. Нам нужно декларативное представление, которое является разумной кодировкой нашей модели и нужно уметь эффективно использовать это представление, чтобы отвечать на широкий круг интересующих вопросов. Более того, должны иметь возможность получить распределение, сочетая экспертные знания и накопленные данные. Вероятностные графические модели - одна из небольшой группы программных платформ (фреймворков), которые поддерживают все три возможности для широкого круга задач.

Работа выполнена при поддержке грантового финансирования проектов Министерством образования и науки Республики Казахстан (грант № AP08856687).

Литература

[1] Rodrigo A. Collazo, Christiane Görgen, Jim Q. Smith. CHAIN EVENT GRAPHS. Chapman & Hall/CRC Computer Science and Data Analysis Series. 2018 by Taylor & Francis Group, LLC.

[2] Lorna M. Barclay, Rodrigo A. Collazo, Jim Q. Smith. The dynamic chain event graph. Electronic Journal of Statistics, Vol. 9 (2015) 2130–2169. ISSN: 1935-7524. DOI: 10.1214/15-EJS1068

[3] Rodrigo A. Collazo, Jim Q. Smith. A New Family of Non-Local Priors for Chain Event Graph Model Selection. Bayesian Analysis (2016) 11, Number 4, pp. 1165–1201.

[4] Aditi Shenvi, Jim Q. Smith. A Bayesian Dynamic Graphical Model for Recurrent Events in Public Health. https://arxiv.org/abs/1811.08872

[5] Rachel L. Wilkerson and Jim Q. Smith. Bayesian Diagnostics for Chain Event Graphs. https://arxiv.org/abs/1910.04679

[6] Ioannis Magnisalis, Stavros Demetriadis, and Anastasios Karakostas. Adaptive and Intelligent Systems for Collaborative Learning Support: A Review of the Field. IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES, VOL. 4, NO. 1, JANUARY-MARCH 2011.

[7] Adam C Sales, and John F Pane. The Role of mastery learning in an an intelligent tutoring system: Principal Stratification on a latent variable // Annals of Applied Statistics.V13, N 1 (2019), 420-443.

[8] Finn V. Jensen and Thomas D. Nielsen. Bayesian Networks and Decision Graphs. Information Science and Statistics. New York, NY 10013, USA. Springer Science +Business Media, LLC. February 8, 2007.

[9] Хлопотов Максим Валерьевич. Применение байесовской сети при построении моделей обучающихся для оценки уровня сформированности компетенций. Интернет-журнал «НАУКОВЕДЕНИЕ» http://naukovedenie.ru Выпуск 5 (24), сентябрь – октябрь 2014.

[10] Murray W.R. Control for Intelligent Tutoring Systems: A Blackboard-based Dynamic Instructional Planner // Proceedings of the 4th International Conference on Artificial Intellegence and Education. Amsterdam, Nitherlands. 1989. P. 150-168.

[11] Peter Thwaites, Jim Q. Smith, Robert G. Cowell. Propagation using Chain Event. Graphshttps://www.researchgate.net/publication/226423268_Propagation_using_Chain_Event_Graphs

[12] M. Mayo, A. Mitrovic. Optimising ITS Behaviour with Bayesian Networks and Decision Theory. International Journal of Artificial Intelligence in Education (2001), 12, 124-153

[13] Hyacinth S. Nwana. Intelligent Tutoring Systems: an overview. *Artificial Intelligence Review,* (1990) 4, 251-277

ПРИМЕНЕНИЕ МЕТОДА ПОИСКА С ЧЕРЕДУЮЩИМИСЯ ОКРЕСТНОСТЯМИ VNS ДЛЯ РЕШЕНИЯ ЗАДАЧИ ГЛОБАЛЬНОЙ ОПТИМИЗАЦИИ В ПРОЦЕССЕ КЛАСТЕРНОГО АНАЛИЗА СЕГМЕНТОВ РЕЧЕВОГО СИГНАЛА

Мусабаев Р.Р., Красовицкий А.М., Меркебаев А.
e-mail: rmusab@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В данной статье дано изложение сущности метода Variable Neighborhood Searsh (VNS) и его применение при построении новых метаэвристических методов кластеризации на примере решения задачи кластерного анализа речевых сигналов. Построение новых метаэвристических методов на основе подхода VNS с использованием в качестве базового метода алгоритма k-средних позволяет строить алгоритмы обладающие глобальными оптимизационными свойствами что обеспечивает более качественные результаты кластеризации в смысле минимума целевого критерия по сравнению с базовым алгоритмом k-means.*

Стандартный алгоритм кластеризации k-средних является алгоритмом локального поиска. То есть он выдаёт локально оптимальное решение сходясь к локальному минимуму и на этом останавливается, что не всегда обеспечивает достаточную точность кластеризации. То есть выдается результат кластеризации, но при этом нельзя гарантировать что это самый наилучший из возможных результатов. Поэтому при кластеризации речевого сигнала актуальной остается задача применение более продвинутых метаэвристик использующих в своей основе стандартный алгоритм k-средних. Такие метоэвристики относятся к классу метаэвристик глобальной оптимизации.

Одним из эффективных методов построения метаэвристик глобальной оптимизации является метод поиска с чередующимися окрестностями – Variable Neighborhood Search (VNS) [1]. Данный метод нашел широкое применение в решении различных оптимизационных задач [1-2].

С точки зрения задачи кластеризации глобальная оптимизация заключается в том, что заставить алгоритм кластеризации не останавливался при достижении одного из локальных минимумов, а продолжать свою работу находя всё более лучшие и лучшие глобальные минимумы с точки зрения минимума критерия сумма квадратов расстояний от от объектов до соответствующих им центроидов (SSD). В данном случае алгоритм кластеризации k-средних будет являться базовой эвристикой, которая в свою очередь встраивается в метаэвристику в которой используются более высокоуровневый подход глобального поиска оптимального решения задачи кластеризации используя в качестве алгоритма локального поиска сам алгоритм кластеризации k-средних.

Существуют различные вариации для встраивания алгоритма кластеризации k-средних и получения на его основе методов глобальной кластеризации. В основе большинства алгоритмов глобальной оптимизации лежат более простые эвристики

или алгоритмы локального поиска. В данном случае при решении задачи кластеризации под локальным поиском подразумевается стандартный запуск алгоритма кластеризации k-средних с некоторых начальных центроидов. То есть входной информации поступающей на вход локального поиска является инициализация центроидов, а выходной информации является результат итеративного перераспределения объектов по мере их близости к имеющимся центроидам с последующим пересчётом самих центроидов как центра масс полученных кластеров. Данный процесс продолжается итеративно до тех пор, пока не будет получено такого распределения объектов по кластерам, что на следующей итерации не происходит перераспределения объектов между кластерами (достигнута сходимость).

Основная идея глобального поиска заключается в итеративном перезапуске алгоритма кластеризации k-средних и выбора наилучшего решения среди выполненных кластеризаций в смысле минимума SSD, то есть наилучшего распределение объектов по кластерам который обеспечивает минимум критерия SSD. То есть итеративно повторяется один и тот же процесс кластеризации с разными начальными условиями (в данном случае начальными центроидами), но каждый раз мы запоминаем самый наилучший полученный результат, который становится текущем наилучшим результатам, полученным в процессе итеративного перезапуска алгоритма кластеризации. При этом каждый новый перезапуск алгоритма кластеризации в процессе локального поиска инициализируется наилучшим решением, полученным на предыдущих этапах, но при этом это наилучшее решение подвергается некоторой модификации. Регулируя степень модификации предыдущего наилучшего решения, мы генерируем окрестное решение, которое проверяется на оптимальность. Здесь используется фундаментальные знания о том в большинстве задач все возможные оптимальные решения чем-то похожи друг на друга. Таким образом находится наилучшее возможное решение в череде повторяющихся кластеризации, но при этом каждая новая повторяющаяся кластеризация инициализируется слегка модифицированном наилучшим до этого полученным решением. В данном случае под решением подразумевается вариант распределения объектов по кластерам. То есть решение слегка модифицируется тем самым достигается вариабельность при поиске в надежде на то, что данная модификация приведет к улучшениям в процессе кластеризации. Здесь используется предположение что, модифицируя уже в некотором смысле хорошее решение можно прийти к ещё более лучшему решению, чем заново искать более лучшее решение с некоторой случайной точки. То есть меняя по определённым стратегиям полученные центроиды или меняя распределение объектов по центроидам мы можем ожидать, что эти изменения приведут к своего рода выходу из локальных минимумов, тем самым процесс кластеризации будет продолжен, а продолжение итераций k-means всегда приводит в результате к уменьшению критерия SSD и как следствие к более качественным результатам кластеризации.

В ходе проведённых экспериментов предложенный подход показал более качественные результаты по сравнению с базовым алгоритмом кластеризации.

Данная публикация выполнена в рамках гранта AP08856034 «Робастное автоматическое распознавание речевых сигналов с самообучением» финснсируемого КН МОН РК.

Литература

1. Hansen P., Mladenović N., Variable neighborhood search: Principles and applications, European Journal of Operational Research, Volume 130, Issue 3, 2001, pp. 449-467

2. Mladenovic N., Jarboui B., Elleuch S., Mussabayev R., Rusetskaya O. (2021) Variable Neighborhood Programming as a Tool of Machine Learning. In: Pardalos P.M., Rasskazova V., Vrahatis M.N. (eds) Black Box Optimization, Machine Learning, and No-Free Lunch Theorems. Springer Optimization and Its Applications, vol 170. Springer, Cham.

3. Akhmetov I., Mladenovic N., Mussabayev R. (2021) Using K-Means and Variable Neighborhood Search for Automatic Summarization of Scientific Articles. In: Mladenovic N., Sleptchenko A., Sifaleras A., Omar M. (eds) Variable Neighborhood Search. ICVNS 2021. Lecture Notes in Computer Science, vol 12559. Springer, Cham.

АНАЛИЗА И РАСПОЗНАВАНИЯ ИНФОРМАЦИОННЫХ СТРУКТУР РЕЧЕВОГО СИГНАЛА

Мусабаев Р.Р.
e-mail: rmusab@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Описаны подходы, использованные для анализа и распознавания информационных структур речевого сигнала. Вводится определение базовых элементов анализа речевого сигнала. Информационная структура речевого сигнала рассматривается как последовательное объединение базовых элементов в различные последовательно вложенные друг в друга иерархические уровни. Задача автоматического получения фонетической разметки/транскрипции речевого сигнала с её отображением/привязкой на временную шкалу сигнала является основополагающей задачей в речевых технологиях. Описаны принципы выбора целевого критерия для оценивания меры качества полученных результатов интерпретируемого кодирования. Рассмотрены алгоритмические особенности организации процесса многоуровневого анализа речевых сигналов.*

Введение

Одной из достаточно сложных и при этом интересных задач является задача обнаружения информационных структур и паттернов в анализируемом речевом сигнале без использования дополнительных внешних источников информации кроме самого анализируемого речевого сигнала либо с их минимальным использованием. На начальном этапе, как и при решении любой другой достаточно комплексной задачи вводятся определённые ограничения:

1) Записывается и анализируется речь одного конкретного диктора;

2) Запись производится в достаточно идеальных звукоизолированных студийных условиях с использованием профессионального оборудования что минимизирует вероятность возникновения внешних шумовых помех и максимизирует качество и разборчивость записанной речи;

3) Хотя произносимый диктором текст заранее известен, но он не используется в процессе основного анализа речевого сигнала, однако его достаточно малая часть будет использована впоследствии для оценки качества анализа/выявления/распознавания информационных структур речевого сигнала.

Предполагается, что чем продолжительнее будет анализируемый речевой сигнал, тем более качественно можно будет выполнить такого рода анализ.

На последующих этапах эти ограничения могут быть пересмотрены и изменены. Например, будут уже анализироваться запись смешанной речи (по дикторам/языкам) и в условиях внешнего шума. Но пока на первом этапе будет осуществлена попытка решения задачи при вышеперечисленных условиях/ограничениях.

Пусть имеется речевой сигнал $S = (s_1, \dots, s_N)$ заданный упорядоченным множеством своих дискретных выборок/измерений s_i, каждая из которых задаёт значение амплитуды сигнала и имеет порядковый индекс $i = 1,2, \dots, N$. Частота дискретизации/сэмплирования сигнала $f_s = 44\,000$ Гц $= 44$ кГц определяет

количество измерений сигнала, производимых за 1 секунду. Зная частоту дискретизации и индекс выборки s_i легко вычислить время в секундах прошедшее с момента начала записи сигнала до данной выборки $t_i = 1/44000 \cdot (i-1)$.

Как известно необработанный/сырой речевой сигнал является достаточно избыточным с точки зрения соотношения объёма информации необходимой для представления исходного речевого сигнала к объёму его конечного информационного содержания. Так если частота дискретизации при записи речевого сигнала в мультимедийном качестве без сжатия составляет 44 000 дискретных выборок в секунду (44 кГц), то за секунду при обычном темпе речи человек успевает произнести порядка 7-8 фонем/звуков в секунду. Если для представления каждой выборки речевого сигнала требуется 2 байта, а для кодирования фонемы один байт, то мы имеем следующее соотношение объёмов информации речь/транскрипция: 44000*2/8 = 11000. Это говорит о том, что сырой речевой сигнал как правило на несколько порядков избыточнее полезной информации, которую он несёт. Именно по причине факта своей информационной избыточности речевые сигналы достаточно хорошо поддаются сжатию специальными алгоритмами типа MP3.

Базовыми элементами при анализе речевого сигнала S является его кратковременные участки W_i полученные в результате последовательного равномерного разбиения сигнала S на M кратковременных взаимно перекрывающиися фрагментов/окон (степень перекрытия обычно равна 2/3) имеющие одинаковую фиксированную длину порядка 20 мс., $i = 1,2,\dots,M$. Для каждого такого базового элемента W_i мы знаем соответствующие ему индексы начальной и конечной выборок сигнала (т.е. имеем привязку к временно́й шкале сигнала) и соответствующее ему векторное представление V_i, полученное в процессе параметризации $A_p(W_i) = V_i$, где $A_p()$ – некоторый специализированный алгоритм параметризации, например, алгоритм для вычисления нормализированных MFCCs (Mel-frequency cepstral coefficients). Также у нас есть некоторая функция $f(i,j)$ которая позволяет вычислить меру близости/сходства между векторными представлениями V_i и V_j любых двух базовых элементов. В качестве меры близости $f(i,j)$ может выступать, например, простое евклидово расстояние. Таким образом базовый элемент анализа может быть представлен в следующем виде: $E_i = (t_i^1, t_i^2, W_i, V_i)$, где t_i^1 и t_i^2 соответственно время начальной и конечной выборки участка сигнала, W_i – исходный участок сигнала, V_i – его векторное представление.

Под информационной структурой речевого сигнала будем понимать последовательное объединение базовых элементов E_i в различные последовательно вложенные друг в друга иерархические уровни. Каждый последующий иерархический уровень определяет более высокоуровневую функцию/смысл/назначение локально сгруппированных в него базовых элементов E_i (пример возможных последовательно вложенных друг в друга иерархических уровней: сегмент E_i → субфонема → фонема → субслово → слово → фраза/синтагма → предложение → текст). Иерархическое объединение базовых элементов в различные функциональные уровни может быть хорошо формализовано с помощью гиперграфовых структур.

Задача автоматического получения фонетической разметки/транскрипции речевого сигнала с её отображением/привязкой на временную шкалу сигнала является основополагающей задачей в речевых технологиях. Именно на основе

последующего анализа характеристик полученной разметки (гиперграфа) можно решать следующие практические задачи: определение эмоций, идентификация диктора, разделение дикторов, синтез речи и др. Так как в основе всех перечисленных задач лежит анализ динамических и статистических характеристик речевого сигнала которые и отражает полученная фонетическая разметка формализованная в виде соответствующего гиперграфа.

Под информационными структурами понимаются: имеющиеся уровни кодирования/упаковки информации, перечень имеющихся на каждом уровне функциональных классов, имеющиеся связи и отношения между различными классами как на одном уровне, так и между различными уровнями. Результатом анализа информационной структуры речевого сигнала является соответствующая многоуровневая транскрипция, формализованная в виде гиперграфа. Главным свойством данной транскрипции должно являться её интерпретируемость экспертным или алгоритмическим методом. Полученная комплексная транскрипция должна с одной стороны по возможности минимизировать объём информации, представленной в речевом сигнале (т.е. содержать соответствующий информационный экстракт), а с другой стороны полученный код/транскрипция должны обладать по возможности максимальной степенью интерпретируемости. Т.е. минимизация объёма кодируемого/транскрибируемого информационного содержания и максимизация степени его интерпретируемости.

Так как процесс параметризации последовательности отдельных фрагментов W_i речевого сигнала является одним из самых первых этапов, то назовём данный этап «низкоуровневой параметризацией». Таким образом, в результате низкоуровневой параметризации мы имеем отображение каждого участка сигнала W_i в n-мерное пространство его вещественных признаков $V_i \in \mathbb{R}^n$ или n-компонентное кодирование речевого сигнала вещественными признаками. Требуется построить алгоритм, использующий функцию $f(i,j)$ для трансформации имеющегося n-компонентного вещественного последовательного кода в однокомпонентный (одномерный) последовательный категориальный интерпретируемый код. Т.е. перейти от n-компонентного вещественного кодирования речевого сигнала к однокомпонентному (одномерному) категориальному интерпретируемому кодированию. Под «категориальностью» понимается принадлежность объекта к конкретному функциональному или семантическому классу. Так как мы имеем последовательно-иерархическую упаковку базовых элементов в гиперграф, то при решении различных прикладных задач могут представлять интерес различные уровни данного гиперграфа. Фактически информация представленная на последнем уровене и является результатом распознавания речевого сигнала. Т.е. это наивысший осмысленный уровень обобщения/формализации информации, представленной в виде конкретного речевого сигнала.

Выбор целевого критерия качества

При построении подобного алгоритма важно правильно выбрать целевую функцию, которая будет использоваться для оценивания меры качества полученных результатов интерпретируемого кодирования. Очевидно, что чем лучше полученный код может быть отображен на имеющееся эталонное текстовое/фонетическое представление сигнала (скрытое на этапе формирования целевого кода) тем более качественным в смысле адекватности и интерпретируемости является алгоритм и параметры кодирования. Т.е. целевая

кодовая последовательность должна отображать свойства последовательности фонем (фонетической транскрипции) соответствующего речевого сигнала записанных экспертом. При этом для нашей постановки задачи совсем не обязательно иметь массированную фонетическую транскрипцию всех сигналов входящих в анализируемый корпус, а достаточно иметь фонетическую транскрипцию только для относительно короткого сигнала (длительность сигнала фонетическую транскрипцию которого мы знаем и используем в целевой функции для оценки качества значительно меньше суммарной длительности всех остальных сигналов входящих в анализируемый корпус) который является неким эталоном качества отображения сигнала в фонетическую последовательность. Наличие подобной целевой функции открывает достаточно широкие возможности для применения методов глобальной и комбинаторной оптимизации в процессе построения/синтеза метаэвристик для интерпретируемого кодирования речевых сигналов. Эталонное отображение является всего лишь «замочной скважиной» для получения оценки качества и её оптимизации. Достаточно малозначительная длительность эталонного отображения позволяет пренебречь затратами на её получение. Что нельзя сказать о затратах, требуемых для получения полной фонетической разметки всего анализируемого речевого корпуса. Здесь возможны два основных подхода к использованию эталонного отображения: 1) использование только для финальной оценки качества результатов интерпретируемого кодирования; 2) использование в итеративном процессе с целью оптимизации целевой функции качества. Первый подход можно считать полностью основанным на самообучении. Второй же подход нельзя назвать чистым самообучением, а скорее машинным обучением по очень слаборазмеченным данным. Слаборазмеченные данные как составная часть в общем неразмеченных больших данных и являются той «замочной скважиной» для получения их полной разметки.

В качестве такой меры качества может выступить целевая функция качества, используемая в методе выравнивания последовательностей (sequence alignment). Имея интерпретируемое кодовое представление речевого сигнала в виде последовательности чередующихся фонетических классов мы можем попытаться её сначала отобразить (mapping) а потом и выровнять (alignment) с имеющимся текстом или его фонетической транскрипцией в случае если мы используем слаборазмеченные данные. Если же мы совсем не используем размеченных данных, то в качестве критерия качества интерпретируемого кодирования является оценка меры повторяемости/регулярности фрагментов полученного кода для различных дикторов и произносимых ими текстов на неизвестном языке. Чем более стабильно мы будем получать одинаковое количество фонетических классов, их контекстов, статистических характеристик и отношений, тем о большей степени стабильности и интерпретируемости можно говорить, что является косвенным признаком качества распознавания информационных структур.

Обобщённая формулировка задачи с учётом целевого критерия качества

Краткая обобщённая формулировка задачи: построение эффективного самообучающегося алгоритма для отображения n-мерного вещественного последовательного кода в одномерный категориальный последовательный код с минимальным числом возможных категориальных значений и с максимально возможным сохранением полезных/информативных/интерпретативных свойств

кодируемого речевого сигнала. При этом одним из критериев качества является адекватность кодирования, выражаемая в наблюдаемой общности контекстных характеристик получаемого кода коррелирующих с наблюдаемой контекстной общностью характеристик базовых элементов в анализируемом сигнале. То есть должна иметь место корреляция общности контекстов: общие контексты в сигнале должны соответствовать общим контекстам в коде. Вторым критерием качества является объем получаемого кода. По аналогии с "интерпретируемым машинным обучением" данный алгоритм можно назвать "интерпретируемое категориальное кодирование со сжатием".

Алгоритмические особенности организации процесса многоуровневого анализа речевых сигналов

Для того чтобы осуществлять математический анализ и распознавание информационных структур речевого сигнала необходимо на первом уровне разделить сигнал на два основных класса: нужно отделить речь от сегментов, в которых речь не содержится (межречевые паузы). Таким образом анализируемый сигнал на самом базовом уровне анализа можно поделить и проклассифицировать на два основополагающих класса: сегменты соответствующие и несоответствующие речевой активности. Группа алгоритмов которая решает данную задачу называется Voice Activity Detection (VAD) с помощью которых разделяются сегменты с голосовой активностью от сегментов без голосовой активности. После того как мы помощью специализированных VAD алгоритмов удалось разделить речь на два этих класса, то дальнейшем анализу подвергаются именно сегменты, относящиеся к классу сегментов, содержащих речевую активность. На последующем этапе в самом классе речевой активности необходимо выявить уже такие сегменты, которые обладают стационарными или переходными спектральными характеристиками. Для этого речевой сигнал делится на множество последовательно идущих перекрывающихся фреймов, обычно длина такого фрейма составляет порядка 15-20 миллисекунд. При этом подряд идущие окна обычно перекрываются, что придаёт результатам анализа более плавные характеристики. Чем больше степень перекрытия и чем меньше длина окна тем больше фреймов мы получаем в результате. Каждый полученный фрейм в дальнейшем подвергается процессу векторизации для того чтобы перейти от достаточно избыточного исходного представления сигнала к более компактному и сжатому параметрическому представлению. Для векторизации фреймов используются различные специализированные алгоритмы. Можно сказать, что таким образом получаются эмбеддинги фреймов, т.е. для каждого фреймана получается его векторное представление или embedding. В дальнейшем векторное представление этих фреймов уже используется как базовая единица на последующих этапах анализа.

Кластеризация базовых элементов анализа речевого сигнала и идентификация оптимального количества кластеров

На начальном этапе для анализа структурных особенностей речевого сигнала очень важное значение имеет применение алгоритмов кластеризации. На первом этапе нужно определить количество низкоуровневых элементарных сегментов. Это фрагменты речевого сигнала, которые имеют самостоятельную смысловую нагрузку. То есть сначала необходимо выделить и кластеризовать базовые элементы анализа. Но при кластеризации возникает вопрос определения количества кластеров, которые изначально неизвестны. Необходимость применения

кластеризации заключается в том, что мы предполагаем, что сам по себе сегментированный на фреймы речевой сигнал несет определенную избыточность в смысле наличия и повторяемости однотипных фреймов. То есть мы предполагаем, что в речевом сигнале имеются однотипные фреймы, которые в процессе кластеризации могут быть объединены в так называемые кластеры по мере общности их свойств. При этом свойства задаются их векторными представлениями, полученными на основе алгоритма параметризации. То есть мы должны выделить однородные по свойствам группы фреймов, являющихся базовыми объектами анализа и пометить каждую такую группу как объекты, относящиеся к определенному функциональному классу. Самая же первоочередная задача — это определение количества таких классов. Первоочередная задача, которая встаёт на начальном этапе анализа структуры речевого сигнала это определение количества элементов в данной структуре или базовых единиц анализа. То есть мы должны знать сколько базовых единиц анализа будут использованы на данном уровне анализа (уровней может быть несколько). Таким образом перед нами возникают две задачи: первая задача — это определение количества элементов анализа на заданном уровне анализа, а вторая задача — это группировка всего имеющегося множества элементов анализа в однородные по совокупности свойств группы. Для решения обоих задач можно использовать один и тот же инструмент - а именно алгоритм кластеризации k-means.

Таким образом, если мы имеем последовательность фреймов и каждый отдельно взятый фрейм задан некоторым вектором в n-мерном векторном пространстве своих признаков, то мы можем ввести некоторую функцию для вычисления близости между любыми двумя отдельно взятыми фреймами. Такая функция может быть использована в качестве метрики в процессе кластеризации имеющегося множество фреймов. Выполняя кластеризацию имеющегося множество фреймов, мы выделяем структурные особенности распределения полученных классов в речевом сигнале: то есть выделяем локализированные либо распределённые группы однородных фреймов, имеющих близкие характеристики в n-мерном векторном пространстве. Перед выполнением процедуры кластеризации в большинстве случаев необходимо знать требуемое количество кластеров. Требуемое количество кластеров и будет соответствовать количеству целевых функциональных классов, на которые будет разбито всё множество базовых элементов анализа составляющих анализируемый сигнал. Существуют метаэвристики с помощью которых можно идентифицировать оптимальное количество кластеров для конкретного набора объектов. Одной из них является «метод локтя» - Elbow Method при котором отыскивается точка максимального перегиба в динамике целевого критерия кластеризации. Так используя процедуру кластеризации k-means, можно последовательно прокластеризовать всё множество фреймов на разное число кластеров в искомом диапазоне, и для каждого результата кластеризации, соответствующего определённому числу кластеров, можно вычислить оценку целевого критерия качества кластеризации (SSD – sum-of-squared distances). Проанализировав динамику изменения SSD, можно найти момент её максимального перепада. То есть нужно найти такое количество кластеров k, при котором, по сравнению с предыдущей кластеризацией, имеет место максимальный перепад в динамике целевого критерия: $\arg\max_{k\in[1,K]} SSD_{k-1} - SSD_k$. При этом следует

заметить, что стандартный алгоритм k-means имеет свойство локальной сходимости, т.е. его использование не гарантирует достижения глобального оптимума критерия качества кластеризации SSD. Это приводит к тому, что алгоритм k-means в большинстве случаев даёт результат кластеризации обладающими свойством локальной оптимальности, т.е. существует вероятность что при отличающейся инициализации данного алгоритма можно получить другой результат кластеризации который может быть лучше или хуже в смысле минимума SSD. Поэтому чтобы получить более адекватную динамику SSD при кластеризации с разным числом кластеров необходимо вместо стандартного k-means использовать более продвинутые метаэвристики на его основе которые обеспечивают сходимость к глобальному оптимуму SSD при кластеризации на заданное число кластеров k.

Идентифицированное оптимальное количество кластеров k и будет для нас размерам алфавита первого уровня. То есть для нас в данном случае алфавитом первого уровня является кластера векторных представлений соответствующих отдельно взятых фреймов. При этом можно использовать разные подходы для получения кластеров базовых элементов анализа. Первый возможный подход — это кластеризация стандартными алгоритмами только на основе самих векторных представлений: если мы просто все имеющиеся векторные представления кластеризируемых объектов объединяем в одно единое множество (dataset), а затем осуществляем его кластеризацию стандартными методами на требуемое k кластеров. Второй более продвинутый возможный подход – это учитывание в процессе кластеризации какой-то дополнительной специфичной информации (task-specific information) которая может быть полезна в процессе кластеризации. Надо использовать информацию о структуре речевого сигнала для того, чтобы эффективно осуществлять кластеризацию этого речевого сигнала. То есть чем больше мы будем использовать дополнительной полезной информации, тем более вероятно получение более качественного результата кластеризации. Особенно зная свойства анализируемого сигнала мы можем расширить функционал кластеризации. Например, так как мы знаем, что два рядом расположенных фрейма с достаточно большой вероятностью могут быть отнесены к одному кластеру. То есть чем ближе находятся два отдельно взятых фрейма в сигнале, тем больше вероятность того, что они относятся к одному классу или кластеру. Использование этой дополнительной специфичной задаче-ориентированной информации (task-specific information) позволит улучшить качество кластеризации.

Для решения задачи математического анализа и распознавания информационных структур в речевом сигнале можно использовать два факта о свойствах речевого сигнала: первый факт заключается в том, что речевой сигнал является последовательностью базовых элементов анализа, то есть он не имеет последовательность протяжённый во времени структуру. Второй факт заключается в том, что речевой сигнал содержит вложенные друг в друга по принципу иерархических отношений разноуровневые объекты анализа, обладающие контекстной зависимостью своих характеристик. То есть он содержит отдельные фонемы, которые и образуют некоторую последовательность звуков, которые в свою очередь объединяются в слова. То есть мы имеем свойства протяженности во времени, вложенности и контекстной зависимости анализируемых структур. Используя данные три факта о свойствах речевого сигнала мы можем усовершенствовать процедуру кластеризации так чтобы использование этих фактов давало дополнительную информацию для повышения качества кластерного иерархического разбиения базовых элементов анализа. Чем больше дополнительной

информации о речевом сигнале мы включаем в процесс его векторизации и кластеризации тем более вероятно то что мы получим более качественные результаты кластеризации. Исходя из вышеперечисленных свойств речевого сигнала модифицировав соответствующим образом алгоритм кластеризации мы можем ожидать что в результате кластеризации будут образовывать локализованные во времени последовательности однотипных фреймов сменяющие друг друга. То есть сначала идут компактно локализированные последовательности фреймов одного типа, которые переходят в последовательность фреймов другого типа. То есть проведя кластеризацию и визуализировав результат кластеризации по принадлежности базовых элементов к классам/кластерам, то есть визуализировав принадлежность последовательности фреймов к определённым классам или кластерам мы обнаружим что локализированные последовательности одного класса/типа сменяются локализированными последовательностями другого класса. Они соединяются в одни локальные группы, а затем они сменяются на локальные группы другого типа. Но при этом если мы будем анализировать близость свойств близлежащих либо непосредственно стоящих друг за другом фреймов друг с другом, то мы увидим, что эти свойства от одного фрейма другому меняются достаточно плавно при высокой частоте фреймирования речевого сигнала. То есть у нас есть локальность и плавность изменения свойств последовательных фреймов. Хотя мы и можем выделить однородные группы, но всегда между этими однородными группами будут так называемые пограничные объекты, то есть объекты, которые с какой-то достаточно равной долей вероятности могут быть отнесены к обеим смежным разнотипным последовательностям. То есть это некоторые переходные процессы, которые происходят в процессе речеобразования. Это означает что в речевом сигнале не происходит чёткая дискретная смена локальных характеристик. Таким образом у нас есть постепенно происходящий плавный процесс смены одной акустической характеристики в сигнале на другую акустическую характеристику. То есть мы можем речевой сигнал на начальном этапе анализа рассматривать как акустический процесс и попытаться выделить в этом речевом сигнале акустические события. Например, мы знаем, что различные участки речевого сигнала могут обладать различными спектральными характеристиками. Важно анализировать соотношения спектральных характеристик в анализируемых и сопоставляемых фреймах сигнала. Например, в каком-то фрейме могут быть больше представленной низкие частоты с достаточно высокой периодичностью характеристик. В других же акустических сегментах наоборот могут практически отсутствовать низкие частоты, а преобладать будут именно высокие частоты. Также будут присутствовать акустические сегменты которые вообще не содержат никакой информации - это может быть просто тишина. При этом есть определенные резонансные частоты в спектре. Эти резонансные частоты постепенно сменяются, смещаясь из одной области резонансных частот в другую область резонансных частот. Учитывая эти свойства речевого сигнала в процессе анализа можно добиться повышения качества результатов кластеризации и тем самым повысить результат распознавания речевого сигнала.

Одной из первоочередных задач в процессе начального анализа является сегментация речевого сигнала на акустические события. То есть элементом второго уровня анализа является объединение базовых элементов в сегменты характеризующие акустические события. Мы можем ожидать что одна фонема

может содержать в себе несколько различных акустических событий. Проклассифицировав и сгруппировав их соответствующим образом, мы можем найти соответствия (mapping) между суперсегментными единицами анализа в речевом сигнале и с некоторым фонетическим уровнем, который может в свою очередь коррелировать с символьным представлением текста.

Применяя различные метаэвристики в основе которых лежит данный алгоритм можно как определять оптимальное количество кластеров можно, так и в последующем откластеризовать имеющийся dataset на идентифицированное количество кластеров. Используя особенности данного алгоритма кластеризации можно решить задачу определения оптимального количества кластеров или оптимального количества базовых элементов анализа при распознавании речи.

Данная публикация выполнена в рамках гранта AP08856034 «Робастное автоматическое распознавание речевых сигналов с самообучением» финснсируемого КН МОН РК.

Литература

1. Mubeen, Nafeesa; Shahina, A.; Khan, A. Nayeemulla; Vinoth, G.; , "Combining spectral features of standard and Throat Microphones for speaker identification", Recent Trends In Information Technology (ICRTIT), 2012 International Conference on , pp.119-122, 19-21 April 2012.

2. G. Almpanidis, M.Kotti, and C. Kotropoulos, “Robust detection of phone boundaries using model selection criteria with few observations”, IEEE Trans. Audio, Speech, and Language Processing, vol. 17, no. 2, pp. 287-298, Feb. 2009.

3. T. Quatieri, K. Brady, D. Messing, J. Campbell, W. Campbell, M. Brandstein, C. Weinstein, J. Tardelli, and P. Gatewood, “Exploiting nonacoustic sensors for speech encoding”, IEEE Trans. Audio, Speech, Lang. Process., vol. 14, no. 2, pp. 533–544, Mar. 2006.

4. Ostendorf M., Bulyko I., "The impact of speech recognition on speech synthesis", Proc. IEEE Workshop on Speech Synthesis, 2002. (12 пт.)

МОДЕЛИ И МЕТОДЫ АВТОМАТИЧЕСКОГО ФОРМИРОВАНИЯ, АНАЛИЗА И ОБРАБОТКИ ЦИФРОВОГО ОБРАЗА ЛИЧНОСТИ.

Рудаков В.П.
e-mail: v.rudakov@aues.kz
Алматинский Университет Энергетики и Связи
КН МОН РК, Казахстан

Аннотация

Автором проводилось исследование в направлении голосовой идентификации и обработки цифрового образа личности, в результате которого была создана система, включающая в себя функции идентификации диктора, а также диаризации нескольких разных дикторов во время записи посредством заранее записанных голосовых профилей. Было проведено исследование методов голосовой идентификации. На данный момент времени подобные исследования очень важны в нахождении новых методов защиты информации и улучшения тех методов, которые уже используются на практике.

В общем случае биометрия основана на измерении уникальных характеристик конкретного человека. В качестве таких характеристик могут быть использованы биологические признаки, такие как отпечатки пальцев, радужная оболочка глаза, ДНК и т. п., или поведенческие характеристики, полученные в процессе учебы или работы. К последним относятся голос, походка, жесты, почерк и т. п. До недавнего времени поведенческие характеристики мало применялись в системах идентификации в связи с очевидными недостатками. Голос может измениться вследствие болезни, возрастных изменений или воздействия окружающей среды (например, высокий уровень шума). Однако в настоящее время с появлением эффективных методов цифровой обработки сигналов интерес к данной тематике в мире значительно возрос.

В данной статье будет рассматриваться голосовая идентификация для устройств контроля доступа к какой-либо информации. Преимуществом данного решения является простота аппаратно-программной реализации. Для получения голосового отпечатка требуется только микрофон и аналого-цифровой преобразователь. Данными устройствами оснащены практически все современные настольные и мобильные компьютеры. Задача голосовой идентификации или распознавания диктора по голосу сводится к тому, чтобы выделить, классифицировать и соответствующим образом отреагировать на человеческую речь из входного звукового потока. При этом обычно выделяют три подзадачи: получение голосового отпечатка, идентификация и верификация.

GMM – Gauss Mixture Models – метод аппроксимации плотности вероятности. Метод GMM может рассматриваться как расширение метода векторного квантования. При векторном квантовании, также известном как метод центроидов, создается кодовая книга для непересекающихся областей в пространстве признаков, обычно с помощью кластеризации методом K-means. Векторное квантование является простейшей моделью в системах распознавания диктора независимо от

контекста. В отличие от векторного квантования, GMM использует перекрывающиеся области в пространстве признаков.

С целью уменьшения сложности оптимизационной задачи поиска параметров смеси нормальных распределений применяется алгоритм EM (expectation-maximization), в котором алгоритм кластеризации K-means может использоваться для поиска начальных приближений. Рассматриваются алгоритмы, в которых требуется небольшое число или даже отсутствие итераций в алгоритме EM. При формировании алгоритма EM важную роль играют критерии эффективности и разделимости.

Критерий эффективности $C(O_k)$ описания выборки смесью из k компонент, включает в себя штраф на число компонент.

$$C(O_k) = -2L(O_k) + 2E(O_k) + \vartheta(O_k) log\ m\ . \quad (1)$$

Здесь $L(O_k)$ – логарифм функции правдоподобия, $E(O_k)$ – энтропия, $\vartheta(O_k)$ – число свободных параметров в смеси O_k, m – число элементов в выборке. Логарифм функции правдоподобия $L(O_k)$ определяется как:

$$L(O_k) = \sum_{i=1}^{m} ln \sum_{j=1}^{k} w_j \varphi(x_i; \theta_j). \quad (2)$$

Энтропия $E(O_k)$ записывается формулой:

$$E(O_k) = -\sum_{i=1}^{m} \sum_{j=1}^{k} g_{ij} \log (g_{ij}) \geq 0. \quad (3)$$

Здесь $g_{ij} = P(\theta_j; x_i)$ – апостериорная вероятность того, что обучающий объект x_i был сгенерирован j-й компонентой смеси.

Критерий разделимости $S(j; O_k)$, характеризующий качество описания j-й компонентой смеси принадлежащих ей объектов, описан формулой:

$$S(j; O_k) = \int f_j(x; O_k) ln \frac{f_i(x; O_k)}{\varphi(x; O_j)} dx, \quad (4)$$

где $f_j(x; O_k)$ - локальная плотность выборки для j-го распределения. Распределение с наибольшим $S(j; O_k)$ имеет наихудшую оценку локальной плотности и, следовательно, является первым кандидатом на разделение.

Все гауссовы компоненты референтной модели предварительно кластеризуются в дерево, и соответствующие акустические пространства отображаются в структурно разделенные области. При этом достигается ускорение примерно в 16 раз с ухудшением ошибки лишь на 1%. Поскольку GMM не опирается на фонетические элементы, то в системах, независимых от контекста, возникает разногласие между обучающим и распознаваемым контекстом. Этот недостаток пытаются преодолеть либо с помощью фонетического дерева решений или создания GMM для каждого фонетического элемента или части слога [1].

Метод опорных векторов (SVM) активно используется в различных системах распознавания образов после публикации монографии. Этот метод позволяет построить гиперплоскость в многомерном пространстве, разделяющую два класса, например, параметров целевого диктора и параметров дикторов из референтной базы. Гиперплоскость вычисляется с использованием не всех векторов параметров,

а только специально выбранных. Эти вектора и называются опорными. Поскольку разделяющая поверхность в исходном пространстве параметров не обязательно соответствует гиперплоскости, то выполняется нелинейное преобразование пространства измеренных параметров в некоторое пространство признаков более высокой размерности. Это нелинейное преобразование должно удовлетворять требованию линейной разделимости в новом пространстве признаков. Если это условие выполняется, то разделяющая поверхность в гиперплоскости строится методом опорных векторов. Очевидно, что успех применения метода опорных векторов зависит от того, насколько удачно подобрано нелинейное преобразование в каждом конкретном случае при распознавании дикторов.

Метод опорных векторов применяется для верификации дикторов часто в комбинации с методом GMM или HMM. Метод опорных векторов применяется также к просодическим параметрам и признакам высокого уровня.

К распознаванию дикторов применяется и метод скрытых Марковских моделей (HMM), хорошо зарекомендовавший себя в задачах автоматического распознавания речи. В частности, предполагается, что для коротких фраз длительностью в несколько секунд для контестно-зависимого подхода лучше всего применять фонемно-зависимые HMM, а не модели на основе вероятностей перехода от кадра к кадру длительностью 10 – 20 мс. Метод скрытых марковсикх моделей может использоваться в совокупности с методом GMM.

Искусственные нейронные сети (ANN – Artificial Neuron Net) применяются при распознавании диктора. ANN применяется к сигнал-остатку на периоде основного тона.

Эффективность применения конкретного типа классификатора зависит от того, происходит ли сравнение параметров целевого диктора с общим распределением параметров в референтной базе, с N-ближайшими по результатам обучения, с каждым диктором из референтной базы, или с дикторами-кластерами этой базы.

Первоначальным этапом голосовой идентификации является получение речевых признаков диктора (рис. 1.1). Для этого необходимы микрофон, фильтр и аналого-цифровой преобразователь (АЦП) для дальнейшей работы с цифровой записью голоса.

С выхода микрофона сигнал подается на вход блока фильтрации. Следующим этапом является прохождение АЦП. Далее оцифрованный сигнал попадает в блок цифровой обработки. В блоке цифровой обработки сигнал фильтруется и преобразуется в вектор, с которым в дальнейшем будет работать микропроцессор и нейросетевой обработчик. Для последующего сравнения с сохраненным ранее голосовым отпечатком диктора полученный вектор заносится в энергонезависимую память. После сравнения отпечатка в памяти с полученным отпечатком, программа подаёт команду доступа (пройдено или не пройдено).

Сам процесс голосовой идентификации не требователен к ресурсам и состоит из двух этапов. На первом этапе осуществляется получение голосового отпечатка диктора и преобразование к виду, в котором его можно будет сравнить с другими. Второй этап заключается в сравнении голосовых отпечатков при помощи обученной нейронной сети.

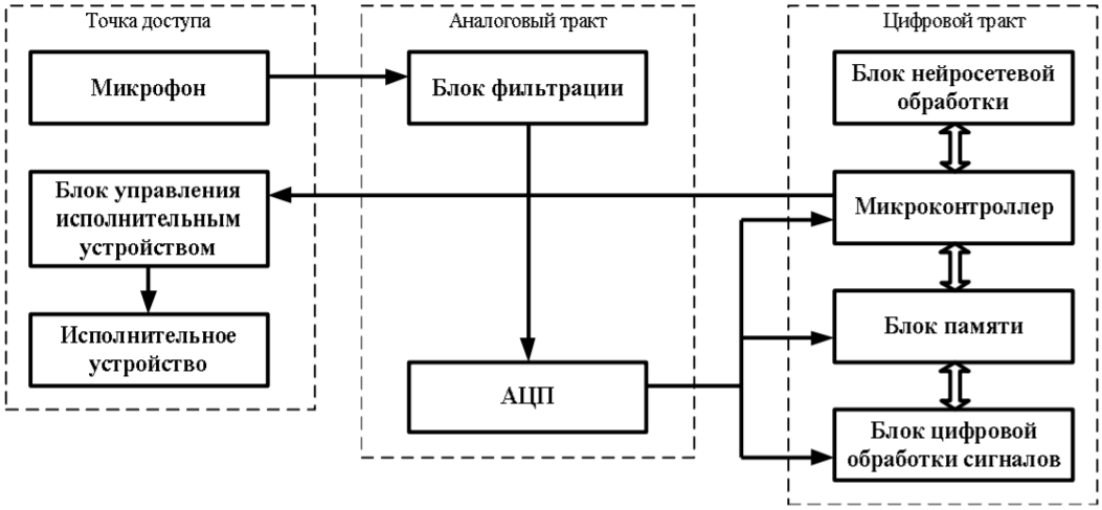


Рисунок 1.1 – Архитектура программно-аппаратных средств системы контроля доступа в помещение (пример).

Для реализации процесса преобразования аудиозаписи производится определённый порядок действий. При помощи микрофона получается запись голоса диктора. Наиболее оптимальным является получение WAV файла ввиду простоты работы с ним. Полученную запись голоса следует разделить на кадры. Результат такого разделения представлен на рисунке 1.2. Данное действие необходимо для более простой работы с записанной звуковой дорожкой. Далее все вычисления будут производиться с каждым кадром в отдельности.

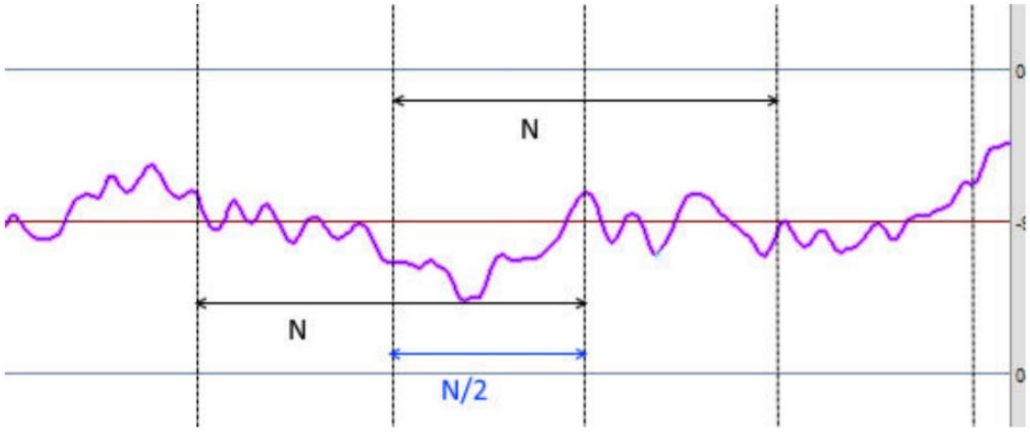


Рисунок 1.2 – График звуковой волны.

Результатом этапа получения голосового отпечатка является сохраненный, для определенного диктора, набор мел-кепстральных коэффициентов. В предложенном алгоритме получения отпечатка использовались наиболее быстрые методы обработки голосового сигнала. Для определенных задач данный набор действий может не подойти ввиду нехватки точности вычислений. Однако для данной задачи информация о голосе является достаточной.

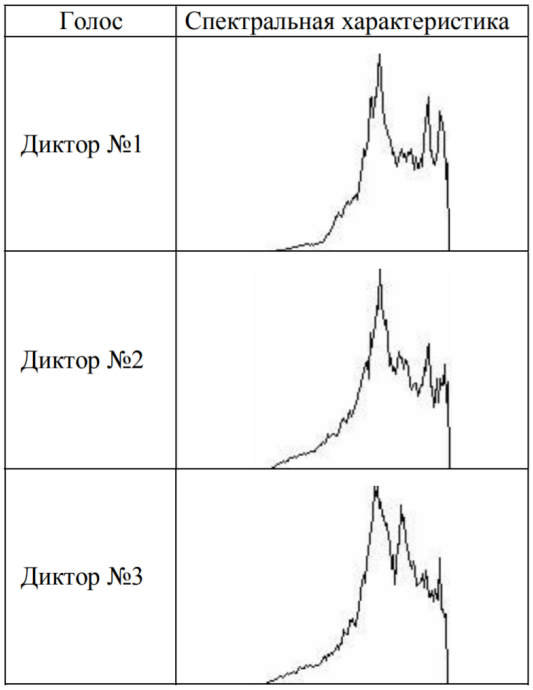


Рисунок 1.3 – графические отображения мел-кепстральных векторов, полученные от разных дикторов для слова «один».

Анализ представленных в таблице результатов показывает, что для одинакового слова, используемого при получении голосового отпечатка, результирующие векторы характеристик различны и могут быть использованы для идентификации дикторов.

Методика работы нейронной сети в стандартном варианте состоит из трёх действий [2]:

1. Обучение:
   – нумерация входного вектора;
   – подача вектора на вход сети;
   – вычисление сумм в узлах слоя Кохонена;
   – активация узла с суммой 1, если такового нет – повтор пункта «с»;
   – коррекция веса узла по формуле: $w_n = w_0 + \alpha(x - w_0)$, где w_n – новое значение веса; w_0 – старое значение; α – скорость обучения; x – величина входа.
2. Идентификация:
   – нумерация входного вектора;
   – подача вектора на вход сети;
   – вычисление сумм в узлах слоя Кохонена;
   – активация узла с суммой 1, если такового нет – повтор пункта «с»;
   – получение классифицируемого вектора.
3. Верификация:
   – нахождение среднеквадратического отклонения между точками введенного вектора и имеющегося в памяти (классифицируемого);
   – сверка полученных значений отклонения с пороговым значением.

В системах санкционирования доступа идентификация диктора может применяться в тех случаях, когда, по условиям эксплуатации, предусматривается проверка личности только одного диктора. В этом случае нет необходимости в указании идентификатора этого диктора. Решение принимается путем сравнения голоса на входе системы идентификации с характеристиками единственного пользователя. Вариант задачи идентификации состоит в идентификации диктора из некоторой группы, а не отдельного диктора (например, при групповом допуске в помещение или доступе к информации).

Если число потенциальных пользователей не слишком велико, то идентификация конкретного диктора также возможна без использования идентификатора. В этом случае поочередно выполняется проверка гипотезы о принадлежности поступившего на вход систем идентификации голоса к каждому из представленных в группе дикторов. Идентификация осуществляется путем выбора того диктора, для которого достигнуто наилучшее значение правдоподобия. Число дикторов, для которых еще возможно использование идентификации вместо верификации, определяется вычислительной мощностью системы и допустимым временем задержки. В случае массового обслуживания, когда число пользователей слишком велико, идентификация практически неприменима.

У любого человека есть свои особые вокальные характеристики, определяемые индивидуальной структурой его голосового аппарата. Прислушиваясь к разговору, человек может на уровне подсознания идентифицировать голоса любых других людей, однако разработка автоматического распознавателя речи сопряжена со значительными трудностями.

Задача распознавания человека по голосу состоит в выделении из входного аудиопотока человеческой речи, ее классификации и распознавания. При этом обычно решаются две подзадачи: распознавание говорящего и проверка. Для решения этих подзадач можно определить метод расчета степени сходства выборки с опорными сигналами. Степень сходства опорной и тестовой выборок можно рассчитать с использованием определенной меры расстояния или с использованием вероятностных критериев. Алгоритм идентификации говорящего можно также определить как текстозависимый и текстонезависимый. Если алгоритм идентификации речи зависит от текста, то в нем можно использовать как фиксированные заранее фразы, так и фразы, которые генерируются системой распознавания. Текстонезависимые системы необходимы для обработки произвольной речи.

В настоящее время широко распространены следующие способы для моделирования говорящего человека:

• для класса текстозависимых систем – динамическое преобразование времени (Dynamic Time Warping; DTW) и скрытые марковские модели (Hidden Markov Model; HMM);

• для класса текстонезависимых систем – векторное квантование (Vector Quantification; VQ), модели гауссовой модели смеси (GMM) и метод опорных векторв (опорная векторная машина (SVM).

Dynamic Time Warping (DTW) – алгоритм динамического преобразования шкалы времени, метод динамического программирования, позволяющий находить расстояние между двумя временными рядами. Как правило, такие последовательности имеют разную длину, поэтому приходится производить измерения с различными скоростями. Основное преимущество данного алгоритма – это простота реализации. Хотя этот алгоритм с успехом используется в различных

приложениях, иногда он дает неверные результаты. Алгоритм пытается исправить несогласованность оси x путем преобразования оси y, что может вызвать выравнивание, в котором одна точка исходного временного ряда связана с довольно большим массивом точек другого временного ряда [7]. Другая проблема при реализации данного алгоритма заключается в том, что ему трудно обнаружить выравнивание двух строк в связи с тем, что некоторое значение (которое может иметь вид пика, впадины, плато, максимума или минимума функции) одного ряда расположится несколько выше или несколько ниже соответствующей точки в другом ряду.

Если для решения задачи распознавания нескольких классов применяется метод опорных векторов, то часто можно использовать стратегию «один против другого». Это требует построения q-классификаторов, при этом каждый классификатор можно обучить отличию одного конкретного класса от других. При решении задачи идентификации объект будет определен как принадлежащий к классу, классификатор которого дает максимальное значение разделяющей функции f(x). Метод опорных векторов предполагает высокую точность классификации, имеет теоретическое обоснование, позволяет применение различных подходов к классификации в соответствии с выбором основной функции. Среди недостатков метода нужно отметить необходимость выбора ядра, а также достаточно большое время, необходимое для произведения процедуры обучения алгоритма для решения задачи многоклассового распознавания.

Модели гауссовых смесей могут быть применимы не только для моделирования характеристик голоса говорящего, но и для записи сигнала голоса и окружающей среды. Каждый из компонентов модели отражает некоторые общие особенности голоса, но индивидуальные при их воспроизведении каждым говорящим. Модели гауссовых смесей доказали свою эффективность, так как обладают высокой точностью распознавания. Именно поэтому этот подход может быть успешно использован для решения проблемы идентификации текстонезависимого говорящего

Принципиальный недостаток всех методов биометрии, кроме речевого, состоит в постоянстве используемого биометрического кода, т.к. отпечатки пальцев или ладоней, рисунок радужной оболочки и черты лица неизменны для индивидуума. Этот недостаток препятствует применению этих методов в случаях, требующих особо высокой надежности идентификации личности, поскольку неизменный биометрический код может быть считан путем злонамеренного вторжения в программу распознавания.

В отличие от биометрии по фиксированным параметрам, верификация по голосу обладает практически неограниченным потенциалом для снижения ошибки за счет использования все более длинных речевых сообщений. Верификации по голосу может использоваться в темноте, на расстоянии, в частности, по стандартному телефонному каналу, в условиях, когда невозможно получить изображение лица.

Примеры конкретных применений верификации диктора охватывают широкий спектр приложений:

- распоряжение финансовыми процессами по электронным или телефонным каналам (управление банковским счетом, электронная коммерция, подтверждение права пользования кредитной картой);

- разрешение на смену пароля или PIN-кода;
- доступ к компьютеру или отдельным программам компьютера (вход в Интернет, доступ к конфиденциальным документам, базам данных и т.д.);
- разрешение на вход в помещение, открывание сейфа;
- управление механизмами и системами (например, запуск двигателя автомобиля);
- мониторинг того, кто, когда и к каким компьютерным ресурсам имел доступ.

Добавление акустического распознавания диктора в несколько раз уменьшает ошибку распознавания по лицу/фигуре, но добавление визуальной информации лишь ненамного улучшает решение по акустике.

Литература

1. Сорокин, Вьюгин, Танатыкин «Информационные технологии в технических и социально-экономических системах», Том 12, №1, стр. 1-30, 2012;

2. Меньшаков П.А., Мурашко И.А. «Методика голосовой идентификации на основе нейронных сетей», 2017;

ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ УНИФИЦИРОВАННОЙ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ СЛОЖНЫМИ ОБЪЕКТАМИ

Самигулина Г.А., Самигулина З.И.
galinasamigulina@mail.ru, zarinasamigulina@mail.ru
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
Казахстанско-Британский технический университет, Казахстан

Аннотация. *Разработка интеллектуальных систем управления на основе алгоритмов искусственных иммунных систем (ИИС), адаптированных под требования производственной среды, является актуальной задачей. Интеграция существующих отдельных алгоритмов функционирования ИИС и их модификаций в единую информационную систему позволяет перейти на более высокий и эффективный уровень интеллектуализации промышленного производства. Статья посвящена разработке онтологической модели унифицированной искусственной иммунной системы (УИИС) в среде Protégé для управления сложными объектами. Осуществлена классификация и систематизация существующих модифицированных алгоритмов ИИС для создания онтологии УИИС. Приведён пример составления технологической цепочки и формирования оптимальных сценариев иммунного ответа на основе УИИС.*

Искусственный интеллект (ИИ) успешно используется во многих областях промышленности [1]. В разработке распределённых систем управления на основе методов искусственного интеллекта и программируемых логических контроллеров, а также поддержке проектов и стартапов в данной области [2] заинтересованы ведущие производители промышленного оборудования, такие как: Siemens, Honeywell, Mitsubishi Electric, Schneider Electric, Yokogawa и т.д. Подобные системы нацелены на обработку больших производственных данных, прогноз и принятие решений. Аналитическая компания IDC (International Data Corporation, USA) [3] с огромным штатом аналитиков из различных стран мира специализирующаяся на изучении мирового рынка информационных технологий и коммуникаций прогнозирует большие перспективы развития промышленного ИИ для реализации программы «Индустрия 4.0». Международная компания Roland Berger в своих исследованиях рассматривает долгосрочное влияние ИИ на промышленное производство. К 2035 году интеллектуальные системы могут обеспечить рост прибыли в размере 420 миллиардов евро только в западной Европе [4]. Международная сеть компаний PwC (PricewaterhouseCoopers) прогнозирует к 2030 году рост прибыли в мировой экономике за счёт развития ИИ до 15.7 триллионов долларов.

Среди методов ИИ, успешно применяющихся в промышленности широкое распространение получили нейронные сети. Например, в работе [5] рассматривается использование сетей глубокого обучения (DL), таких как: Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Deep Reinforcement Learning (DRL) и др. для создания интеллектуальных производств. Также для решения различных инженерных задач успешно применяются алгоритмы роевого интеллекта

[6]. Например, исследования [7] посвящены процедуре проектирования ПИД-регулятора, в котором оптимальные параметры получаются путем решения задачи оптимизации с ограничениями. Целевая функция задается в виде абсолютной интегральной ошибки. Оптимизация осуществляется на основе алгоритма роя частиц (PSO).

Особый интерес вызывают искусственные иммунные системы (ИИС) [8] и модифицированные алгоритмы на их основе для решения инженерных задач. Биоинспирированные перспективные алгоритмы ИИС применяются для исследований в области промышленной автоматизации, обладают свойствами адаптивности, самоорганизации и возможностью принятия решений в незнакомой ситуации для управления сложными объектами. Например, в работе [9] с помощью ИИС осуществляется диагностика неисправностей полупроводникового оборудования. В качестве основных отказов рассматривается старение деталей и модулей с течением времени. Результаты экспериментов показали высокую эффективность применения ИИС. Исследования [10] посвящены применению генетического нечёткого иммунного ПИД алгоритма (Genetic Fuzzy Immune PID Algorithm, GFI_PID_A) для круиз-контроля коммерческого транспорта. Перспективность разработанного алгоритма подтвердило проведённое моделирование.

Попытки создания унифицированной искусственной иммунной системы (УИИС) были предприняты в работе [11]. Классические алгоритмы ИИС представляют собой изолированные механизмы иммунной системы и имеют ограниченный спектр применения, тогда как реальная иммунная система человека функционирует как единая система. В данном исследовании рассматриваются некоторые алгоритмы ИИС и методология проектирования УИИС.

Таким образом, фундаментальные исследования в области создания УИИС на основе систематизации, классификации и многокомпонентной оценки эффективности модифицированных алгоритмов ИИС для создания интеллектуальной системы управления сложными объектами является актуальным новым этапом развития промышленного искусственного интеллекта, адаптированного под производственную среду и современную программно-аппаратную базу.

Постановка задачи исследований формулируется следующим образом: необходимо разработать онтологическую модель унифицированной искусственной иммунной системы [12], построенной с помощью систематизации и классификации модифицированных алгоритмов ИИС с учётом их слабых и сильных сторон для выбора наиболее эффективных механизмов иммунного ответа.

Определение 1. Под ИИС понимается вычислительная система, основанная на принципах теоретической иммунологии и наблюдаемых иммунных функциях, принципах и моделях для решения различных прикладных задач [13].

Определение 2. Под модифицированным алгоритмом искусственных иммунных систем (МИИС) понимается улучшенный алгоритм прогнозирования с оптимальным набором данных, полученных с помощью выделения информативных признаков на основе биоинспирированных методов ИИ [14] или путём модификации частей алгоритма с целью улучшения прогностических способностей исходной модели.

Определение 3. Под иммунным ответом понимается автоматизированный выбор технологической цепочки на основе интеллектуального анализа

производственных многомерных данных, различных по своей структуре, типу, размеру и т.д. для управления сложным объектом [15].

Определение 4. Технологическая цепочка представляет собой совокупность команд для формирования оптимальных сценариев управления сложным объектом и оперативной корректировки управляющего воздействия посредством микропроцессорной техники. Для создания УИИС разработана база данных модифицированных алгоритмов ИИС. В качестве примера представлены алгоритмы в соответствии с тремя классами:

1 класс. Модифицированные алгоритмы ИИС на основе теории клонального отбора.

2 класс. Модифицированные алгоритмы ИИС на основе негативного отбора.

3 класс. Модифицированные алгоритмы ИИС на основе иммунносетевого подхода.

Систематизация алгоритмов осуществлялась по областям применения и типам решаемой задачи (например, распознавание образов, выделение информативных признаков, задача оптимизации и т.д.). База данных модифицированных алгоритмов ИИС используется для разработки онтологической модели УИИС в пакете прикладных программ Protégé. Разработанная укрупнённая архитектура интеллектуальной системы управления сложными объектами на основе УИИС разделена на 3 уровня:

1 уровень: Обеспечивает доступ к базе данных модифицированных алгоритмов ИИС и выбор наилучшего алгоритма в соответствии с критериями решаемой задачи.

2 уровень: Отвечает за сбор и обработку производственных данных со сложного объекта управления и интеллектуальный анализ данных на основе модифицированного алгоритма ИИС, выбранного на 1 уровне. На основе полученных данных формируется технологическая цепочка для иммунного ответа.

3 уровень. В соответствии с технологической цепочкой выбирается оптимальный сценарий управления сложным объектом и осуществляется оперативная корректировка за счёт воздействия на исполнительные механизмы.

На рисунке 1 показана графическая визуализация онтологической модели УИИС. Графическое представление позволяет наглядно увидеть существующие связи между классами онтологической модели.

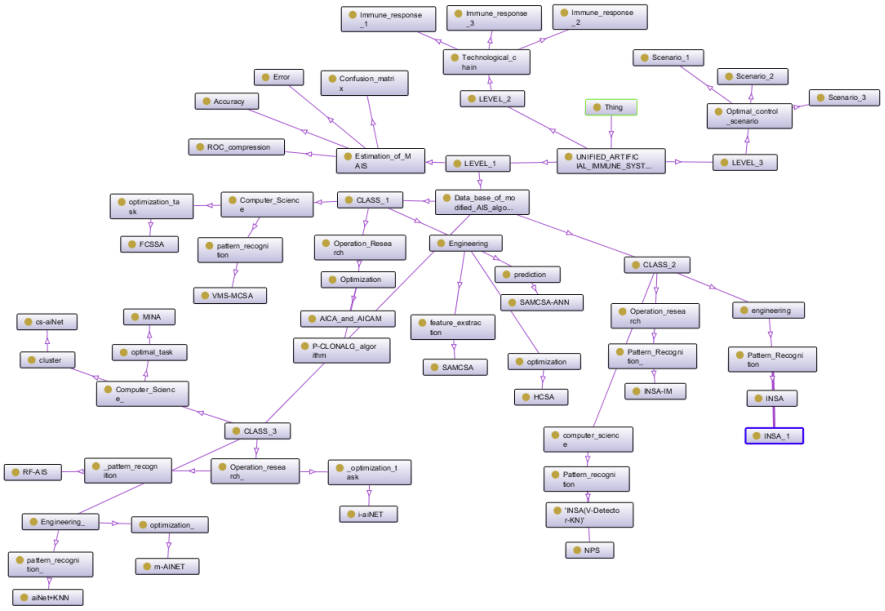


Рис.1 Графическое представление онтологической модели УИИС

Данная УИИС позволяет обрабатывать производственные данные с учётом ограничений накладываемых на работу оборудования и типов решаемых задач на основе модифицированных алгоритмов ИИС, наиболее подходящих под конкретную проблему. По результатам обработки данных формируется иммунный ответ в виде технологических цепочек, которые будут отличаться в зависимости от объекта управления и технических регламентов эксплуатации оборудования. Рассмотрим в качестве примера фрагмент технологической цепочки сформированный для сложного объекта управления Установки 700, предприятия ТенгизШевройл для охлаждения, сепарации и фракционирования очищенного газа [14]:

T_Chain1 <Valve_D701.F; Pump_D701.F; Pump_D702.T; Valve_D702.T; M_Def.T>,

где *Valve_D701.F* – обозначает команду на отключение клапана подачи газа на колонну D701, символ *«.F» (False)* даёт сигнал на контроллер о закрытии клапана D701, в противном случае символ *«.T» (True)* говорит об открытии клапана;

Pump_D701.F – отключение насоса установки D701;

Pump_D702.T – включение насоса D702;

Valve_D702.T – открытие клапана подачи газа на колонну D702;

M_Def.T – осуществить запись сведений об ошибке, префикс M обозначает, что переменная записывается в память «Memory» контроллера или связанного устройства архивирования данных.

На основе полученных технологических цепочек осуществляется выбор оптимального сценария управления сложным объектом:

Scenario 1 {T_Chain1, T_Chain2, T_Chain3 ... T_Chaink },

где *k* – количество полученных технологических цепочек.

Таким образом, разработка УИИС на основе МИИС позволяет использовать более гибкий подход к решению производственных проблем за счёт формирования эффективного иммунного ответа, адекватного требованиям производственной среды. Предложенная интеллектуальная система управления на основе УИИС обладает следующими достоинствами: возможностью обработки производственных

данных во времени, близком к реальному; способностью расширения базы данных модифицированных алгоритмов ИИС; более эффективного иммунного ответа за счёт выбора наиболее подходящих алгоритмов; возможностью применения для решения различных производственных задач (диагностики оборудования, прогнозирования, оптимального распределения ресурсов, оперативного управления и т.д.); возможностью работы с современной микропроцессорной техникой и распределёнными системами управления предприятия.

Работы проводятся по гранту №AP09258508 КН МОН РК «Разработка интеллектуальной технологии управления сложными объектами на основе унифицированной искусственной иммунной системы для промышленной автоматизации с использованием современной микропроцессорной техники» (2021-2023 г.г).

Литература

1. Li, Q. Application of Artificial Intelligence in Industrial Automation Control System / Q. Li // Proceeding of IOP Conference: Earth and Environmental Science, 2021. – Vol. 647. – P. 1-6.

2. Malmaison, R. Start-ups from Schneider Electric and Microsoft's joint accelerator are transforming the energy sector in Europe with artificial intelligence / R. Malmaiso. - Press release Schneider Electric, 2020. – P.1-3.

3. Jyoti, R., Schubmehl, D., Sutherland, H. IBM Think 2021: AI, and More AI Plus Automation Innovations for Enterprises Takes Center Stage. - https://www.idc.com/ (16.08.2021).

4. Utilizing the digitally generated data for a leap in productivity. - https://new.siemens.com (16.08.2021).

5. Hernavs, J., Ficko, M., Berus, L., Rudolf, R., Klančnik, S. Deep Learning in Industry 4.0 – brief overview / J. Hernavs, M. Ficko, L. Berus, R. Rudolf, S. Klančnik // Journal of Production Engineering. – 2018. – Vol. 21(2). – P. 1-6.

6. Kumar, A., Rathore, P.S., Díaz, V.G., Agrawal, R. Swarm Intelligence Optimization: Algorithms and Applications / A. Kumar, P.S. Rathore, V.G. Díaz, R. Agrawal. - Willey, 2021. 384 p.

7. Bošković, M.Č., Rapaić, M.R., Jeličić, Z.D. Particle Swarm Optimization of PID Controller under Constraints on Performance and Robustness / M.Č. Bošković, M.R. Rapaić, Z.D. Jeličić // International Journal Of Electrical Engineering And Computing. – 2018. – Vol. 2(1). DOI:https://doi.org/10.7251/IJEEC1801001B.

8. Mikherski, R.M., Mikherskii, M.R. Analysis of the Use of Artificial Immune Systems / R.M. Mikherski, M.R. Mikherskii // Proceeding of IOP Conference Series: Materials Science and Engineering. – 2021. – Vol. 1069. - P. 1-6.

9. Park, H., Choi, J., Kim, D., Hong, S. Artificial Immune System for Fault Detection and Classification of Semiconductor Equipment / H. Park, J. Choi, D. Kim, S. Hong // Electronics. – 2021. –Vol. 10(8). – P. 944.

10. Jing, Z. Application of genetic fuzzy immune PID algorithm in cruise control for commercial vehicles / Z. Jing // AIP Advances. – 2020. – Vol. 10. –P. 1-8.

11. Chen, Y., Wang, Q., Tang, Q.Z., Tang, C. Unified Artificial Immune System / Y. Chen, Q. Wang, Q.Z. Tang, C. Tang // Proceeding of 5th International Conference and Computational Intelligence and Communication Networks. – 2013. – P. 617-621.

12. Samigulina, G.A., Samigulina, Z.I. Development of intelligent technology for control complex objects based on a unified artificial immune system / G.A. Samigulina, Z.I. Samigulina // Bulletin of the National Technical University KhPI. A series of Information and Modeling. – 2020. – Vol. 2(4). – P. 117-122.

13. Timmis, J., Knight, T., de Castro, L.N., Hart, E. An overview of Artificial Immune Systems / J. Timmis, T. Knight, L.N. de Castro, E. Hart // Computation in Cells and Tissues. – 2004. – P. 51-91.

14. Samigulina, G.A., Samigulina, Z.I. Development of a Knowledge Base for a Unified Artificial Immune System for Complex Objects Control / G.A. Samigulina, Z.I. Samigulina // Proceeding of International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). – 2021. – P. 807-811. DOI: 10.1109/ICIEAM51226.2021.9446418.

15. Samigulina, G.A., Samigulina, Z.I. Development of a Unified Artificial Immune System for Intelligent Technology of Complex Industrial Automation Objects Control in the Oil and Gas Industry / G.A. Samigulina, Z.I. Samigulina // Chapter in book: Human Centred Intelligent Systems. Proceeding of 14 Int. conf.: Human centered intelligent systems (HCIS-21). - Springer, KES, 2021. - P. 86-96. DOI:10.1007/978-981-16-3264-8_9.

РАЗВИТИЕ ПРИНЦИПОВ АДАПТАЦИИ AIS НА КЛАСС РАСПРЕДЕЛЁННЫХ СИСТЕМ УПРАВЛЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ

Ширяева О.И.
e-mail: oshiryayeva@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Получены результаты развития принципов адаптации алгоритмов искусственных иммунных систем на класс распределённых систем управления для решения задач оптимального управления. Получены условия интеграции современной микропроцессорной техники, реализующей законы типового регулирования в распределённой системе управления, с алгоритмами искусственных иммунных систем (AIS). Решена задача синтеза I-PD регулятора для двухконтурной распределённой системы управления технологическим процессом очистки природного газа от различных примесей дистилляционной колонны.*

Ключевые слова. *Искусственные иммунные системы (AIS), адаптация, распределённая система управления, оптимальное управление,технологический процесс.*

Введение. В настоящее время алгоритмы и методы искусственного интеллекта интенсивно используются для решения различных задач анализа и синтеза систем управления. Нейронные сети, генетический алгоритм, биоинспирированные алгоритмы – все эти методы зарекомендовали себя эффективно для обработки данных, синтеза оптимального управления и других задач, связанных с системами управления. Широкие исследования ведутся и в области искусственных иммунных систем, на основе которых строятся информационные системы защиты, системы оптимального управления и пр. [1].

В соответствии с работами по биологии, нервная и иммунная системы различных организмов обладают свойством адаптации и пластичности [2]. Это свойство представляет интерес для разработчиков методов оптимизации на основе искусственных иммунных систем (artificial immune system, AIS) и их развитие на класс распределённых систем управления. Для решения задач, связанных с моделирование, анализом и синтезом распределённых систем управления можно использовать свойства искусственных иммунных систем, как адаптивной вычислительной системы [3]. В настоящее время одним свойств искусственных иммунных систем является их двойная пластичность [4], которая отражает способность иммунной системы к адаптации на основе параметрических и структурных изменений. В связи с этим возникает необходимость моделирования, анализа и синтеза сложных систем управления с учётом алгоритма искусственных иммунных систем.

Само свойство адаптации и параметрической пластичности интерпретируется как свойство системы изменять параметры функционирования для повышения её эффективности. Структурная пластичность соответствует свойству адаптации

системы управления. Это обуславливает использование данных свойств для систем управления с переменным регулятором (рисунок 1).

На рисунке 1: PV – текущее значение выходного сигнала объекта управления; SV – заданный сигнал процесса; E – ошибка рассогласования между значениями выходного сигнала объекта управления и заданного сигнала; MV – управляющее воздействие для объекта управления.

Параметры регулятора с переменной структурой (рисунок 2) настраиваются на основе алгоритма AIS, с учётом свойств двойной пластичности и адаптируемости, что позволяет структурно менять параметры в процессе работы.

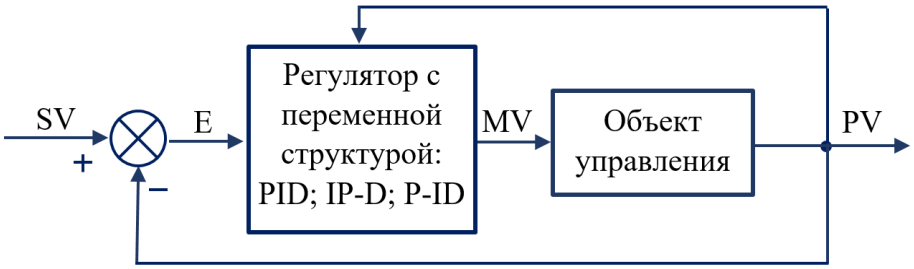


Рис. 1. Схема распределённой системы управления с переменным регулятором

Закон PID управления, в котором управляющее воздействие формируется на основе ошибки рассогласования:

$$MV(t) = K_p \cdot K_s \cdot \left\{ E(t) + \frac{1}{T_i} \int_{t=0}^{t_1} E(t)dt + T_d \frac{dE(t)}{dt} \right\}, \quad (1)$$

где K_p – пропорциональный коэффициент усиления; K_s – коэффициент усиления, определяющий допустимый диапазон изменения для устойчивости замкнутой системы управления; T_i – постоянная интегрирования; T_d – постоянная дифференцирования.

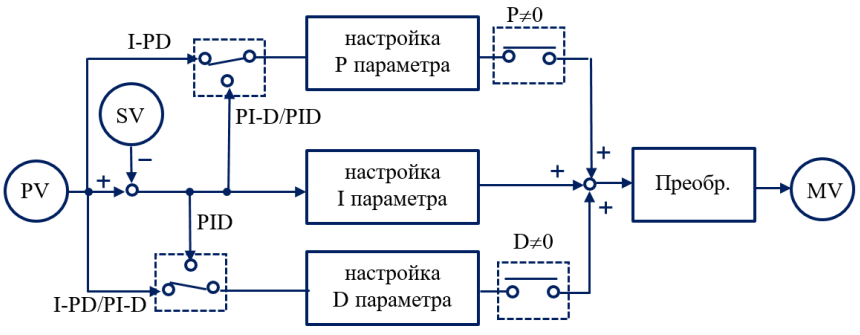


Рис. 2. Схема переменного регулятора распределённой системы

Закон I-PD управления (рисунок 3):

$$MV(t) = K_p \cdot K_s \cdot \left\{ -PV(t) + \frac{1}{T_i} \int_{t=0}^{t_1} E(t)dt - T_d \frac{dPV(t)}{dt} \right\}. \quad (2)$$

в котором управляющее воздействие формируется на основе ошибки рассогласования, E, и изменения выходного сигнала PV.

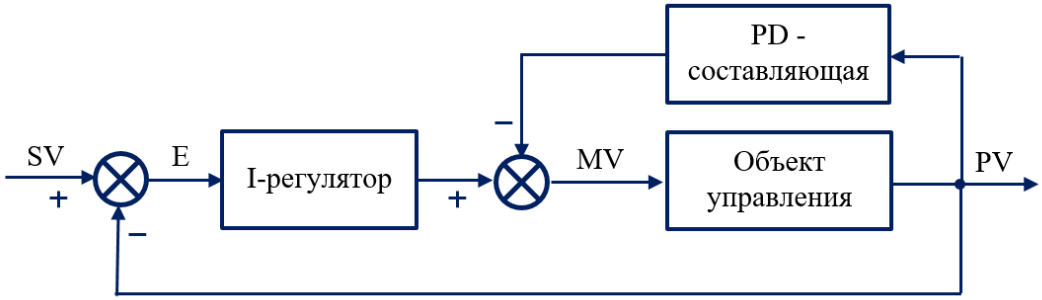


Рис. 3. Схема системы управления с I-PD регулятором

Закон PI-D управления (рисунок 4):

$$MV(t) = K_p \cdot K_s \cdot \left\{ E(t) + \frac{1}{T_i} \int_{t=0}^{t_1} E(t)dt - T_d \frac{dPV(t)}{dt} \right\}. \quad (3)$$

в котором управляющее воздействие формируется на основе ошибки рассогласования, E, и изменения выходного сигнала PV:

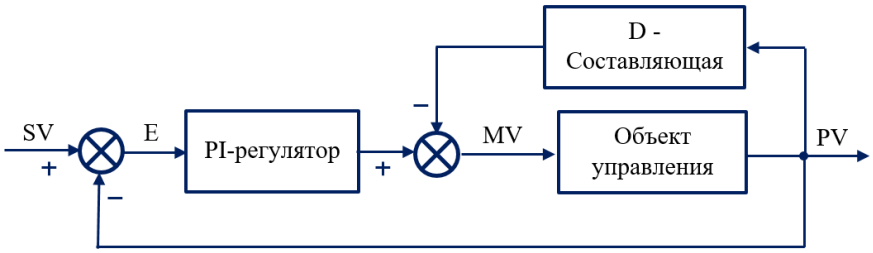


Рис. 4. Схема системы управления с PI-D регулятором

Алгоритм AIS используется для получения значений параметров регуляторов (1-3). Для этого решается тривиальная оптимизационная задачи с поиском минимума квадратичного критерия качества [5]:

$$ISE = \int_{t=0}^{t_1} E^2(t)dt = \int_{t=0}^{t_1} (SV(t) - PV(t))^2(t)dt, \quad \rightarrow \min. \quad (4)$$

Среди стандартных шагов популяционного цикла интеллектуального алгоритма AIS имеет место шаг, связанный со свойством бипластичности - адаптация: инициализация, аффинность, адаптация, селекция, клонирование,

мутация, выбор лучшего клона. В соответствии со свойством пластичности и адаптируемости данный алгоритм обеспечивает изменение структуры регулятора, позволяющего минимизировать критерий качества (4).

В качестве примера используем передаточные функции двухконтурной системы управления процессами очистки природного газа от различных примесей дистилляционной колонны [5]:

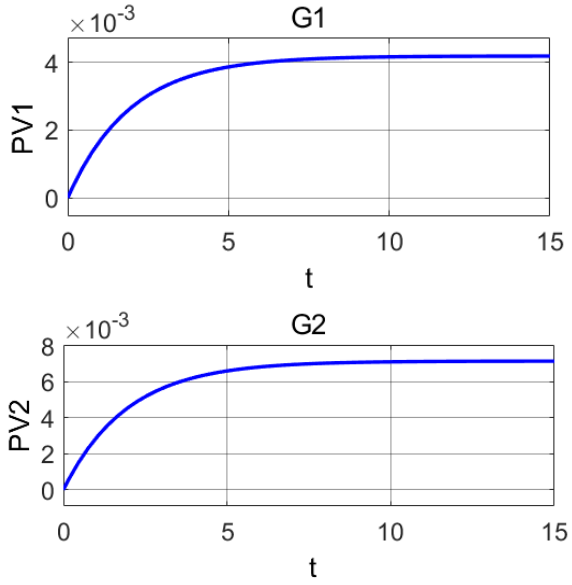
$$G_1(s) = \frac{0.0042}{1.9588s + 1}; \qquad G_2(s) = \frac{0.0072}{1.9588s + 1}. \tag{5}$$

Для формирования требований к желаемой динамики получены переходные процессы (рисунок 5), где PV1 и PV2 – текущие значения выходных сигналов двух контуров. В качестве желаемых сигналов SV1 и SV2 – единичный ступенчатый сигнал.

Для реализации желаемой динамики, введём в рассмотрение интегральный квадратичный критерий качеств:

$$ISE = \int_{t=0}^{t_1} E^2(t)dt = \int_{t=0}^{t_1} (SV(t) - PV(t))^2 dt, \quad \to \min. \tag{6}$$

Критерий (6) является целевой функцией для оптимизационной задачи нахождения минимума на основе алгоритмов искусственного интеллекта.



а) 1 контур б) 2 контур

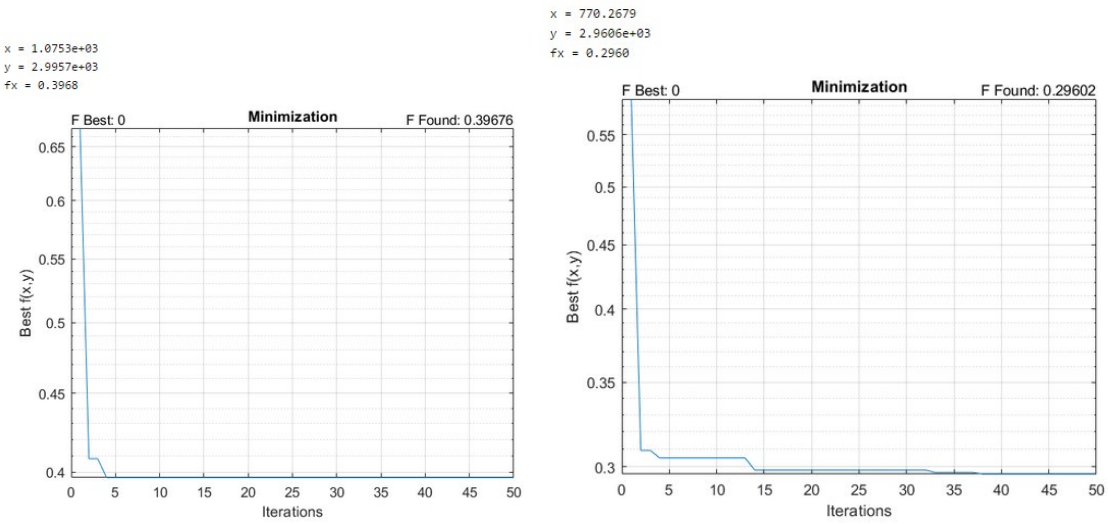
Рис. 5. Переходные процессы контуров

В этом случает поставленная задача сводится к следующей: найти неизвестные параметры регуляторов, которые обеспечивают минимум критерию качества (6) на основе алгоритма искусственного интеллекта AIS и его свойства адаптации.

Приведём результаты синтеза I-PD регулятора (2) распределённой системы. Для поиска неизвестных параметров K_p, T_i, T_d, используется методология,

представленная в работе [5]. В соответствии с ней формируется начальная популяция, которая представляет собой параметры регуляторов из диапазона допустимых значений, удовлетворяющего свойству устойчивости замкнутой системы. Затем производится полный цикл вычислений, на основе шагов поискового AIS. Общие настройки алгоритма: n=100 – размер популяции; ab=cadeia(n,44) – популяция антител; gen=50 – число генераций; pm=0.5 – вероятность мутации; d=0.3 – популяция, которая подвергается случайным перестановкам; beta=0.5 – множитель, контролирующий количество клонов.

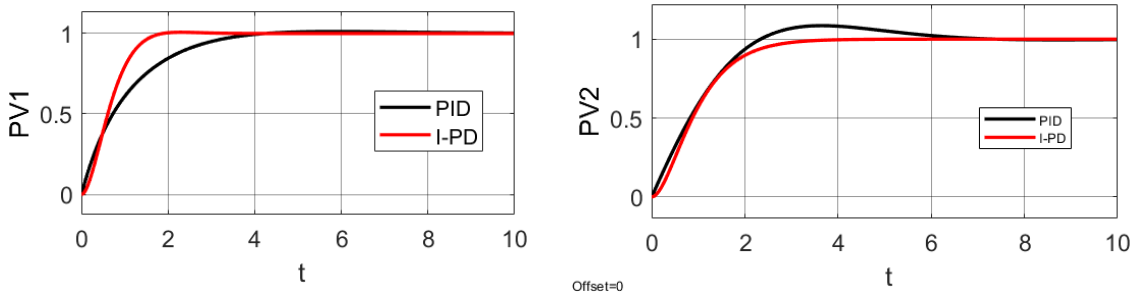
На рисунке 6 представлены удовлетворительные результаты оценки работы алгоритма AIS для двух контуров (5).



а) 1 контур б) 2 контур

Рис. 6. Оценка работы алгоритма AIS для двух контуров

В результате применения алгоритма AIS и его свойства адаптации были найдены параметры I-PD регулятора. Для сравнения, получены параметры PID регулятора на основе PID Tuner среды MATLAB. Результаты моделирования двух контуров (5) объекта с регуляторами I-PD и PID, представлены на рисунке 7.



а) 1 контур б) 2 контур

Рис. 7. Переходные процессы объекта управления с регуляторами

По полученным результатам моделирования можно сделать вывод об эффективности I-PD регуляторов, настроенных алгоритмом AIS, с точки зрения прямых оценок качества переходных процессов: время регулирования, перерегулирование, время нарастания.

Заключение. Для распределённой системы управления, с использованием интеллектуального алгоритма AIS и его свойства адаптации, получены результаты синтеза регуляторов. Приведено решение задачи синтеза I-PD регуляторов для двухконтурной системы управления технологическим процессом очистки природного газа от различных примесей дистилляционной колонны, с достижением желаемой динамики. На основе полученных результатов можно сделать выводы об эффективности использования алгоритмов искусственных иммунных систем со свойством адаптации для решения задач синтеза оптимального управления для распределённых систем.

Данное исследование было профинансировано Комитетом Науки Министерства Образования и Науки Республики Казахстан (грант № AP08855743).

Литература

1. Dasgupta, D. Artificial immune systems and their applications / D. Dasgupta. – Springer, 2014. – 306 p.

2. Люпина, Ю.В., Орлова, А.Ш., Горностаев, Н.Г., Карпова, Я.Д. Пластичность нервной и иммунной систем у различных организмов: роль протеасом / Ю.В. Люпина, А.Ш. Орлова, Н.Г. Горностаев, Я.Д. Карпова // Журнал общей биологии. – 2014. – том 75. – № 1. – С. 3-24.

3. Кушнир, Н.В., Кушнир, А.В., Анацкая, Е.В., Катышева, П.А., Устинов, К.Г. Искусственные иммунные системы: обзор и современное состояние / Н.В. Кушнир, А.В. Кушнир, Е.В Анацкая, П.А. Катышева, К.Г. Устинов // Научные труды КубГТУ. – №12. – 2015. – 10 с.

4. Woodland, D. Plasticity in Adaptive Immunity / D. Woodland // Viral immunology. – 2016. – Vol. 26. – №5. – P. 301.

5. Ширяева, О.И. Реализация SMART-технологии построения оптимальных систем на основе модифицированных алгоритмов / О.И. Ширяева // Вісник Національного технічного університету "Харківський політехнічний інститут". – Харків: НТУ "ХПІ". – 2020. – № 1(3). – С.41-49.

ОТРАЖЕНИЕ ПАНДЕМИИ COVID-19 В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

Якунин К.О., Мухамедиев Р.И., Елис М., Рабкан Я., Сымагулов А., Кучин Я., Мухамедиева Е.
email: yakunin.k@mail.ru
Институт информационных и вычислительных технологий КН МОН РК
Satbayev University (КазНИТУ)
University of Zilina

Аннотация. *В статье анализируется "отражение" темы COVID-19 в средствах массовой информации Республики Казахстан и Российской Федерации. Использован корпус СМИ объемом около 1 млн. публикаций и данные ВОЗ. С помощью тематического моделирования и анализа корреляционных зависимостей было установлено как сходство, так и некоторое различие в публикационной активности СМИ. В частности, в обеих странах активность СМИ коррелирует с абсолютными показателями числа новых инфицированных и числа умерших. Коэффициент корреляции составляет 0,6-0,8. Однако СМИ учитывают долю положительных тестов на коронавирус и скорость размножения вируса (reproduction rate) в гораздо меньшей степени). Коэффициент корреляции составляет 0,4-0,6. В российских СМИ наблюдается высокая корреляция (0,75) с изменениями в мерах по ограничению распространения инфекции, предпринимаемых государством, в то время как в Казахстане эта корреляция значительно ниже (0,4).*

Ключевые слова. *COVID-19, анализ СМИ, тематическое моделирование, BigARTM.*

I. Введение

Система здравоохранения как фактор устойчивого и стабильного роста благосостояния населения является одним из главных приоритетов в Казахстане. В докладе Главы государства "Третья модернизация Казахстана: Глобальная конкурентоспособность" от 3 марта 2017 года включены вопросы здравоохранения [1], разработана Государственная программа здравоохранения Республики Казахстан "Денсаулык", основной целью которой является укрепление здоровья населения для обеспечения устойчивого социально-экономического развития страны. Однако, как в Казахстане, так и в глобальном масштабе, системы здравоохранения сталкиваются с множеством проблем, вызывающих повышенный спрос на медицинские услуги, высокие ожидания населения и растущие затраты [2]. Относительная неэффективность и низкая производительность в секторе здравоохранения привели к увеличению фискальных ограничений, что, в свою очередь, способствовало росту социальной напряженности и снижению экономического роста во время пандемии, что было отмечено COVID-19 [3]. В системе здравоохранения важна не только экономическая, но и социальная и медицинская эффективность; "медицинские мероприятия лечебно-профилактического характера могут быть экономически невыгодными, но медико-социальный эффект требует их проведения" [4].

В то же время неадекватное представительство органов здравоохранения в медиапространстве способствует распространению слухов и дезинформации [5], влияет на психическое здоровье населения [6]. В работе оценивается медиа-эффект COVID-19, проявившийся во время пандемии в Казахстане и России. Анализируются сходства и различия в отражении в СМИ процессов в здравоохранении и обществе, связанных с COVID-19.

В процессе исследования был использован следующий корпус [7]. Архитектура системы, использованной в ходе исследования, и основы методологии описаны в [8].

II. Методы и данные

Корпус новостей из российских и казахстанских СМИ с 2000 по 2020 год из 30 основных источников, включая социальные сети (VK.com, YouTube, Instagram и Telegram) и новостные сайты [7]. Он включает 4 233 990 документов из казахстанских источников и 2 027 963 документа из российских источников (рис. 1).

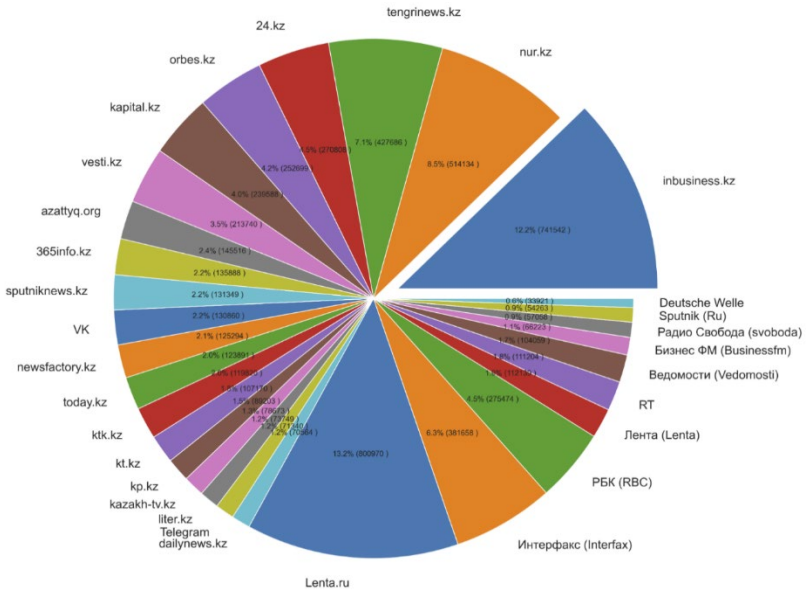


Рис. 1. Основные источники корпуса

A. Данные COVID

Для анализа объективности отражения пандемии COVID-19 в СМИ были использованы данные Центра системной науки и инженерии (CSSE) Университета Джона Хопкинса [8], а именно, были рассмотрены следующие ежедневные показатели отдельно для Казахстана и Российской Федерации:

- Количество новых случаев, сглаженных в соответствии с методикой CSSE.
- Количество новых смертей, сглаженных в соответствии с CSSE-методологией.
- Скорость репродукции вируса.
- Количество новых тестов.
- Показатель положительных результатов - соотношение положительных результатов тестов среди всех проведенных тестов.
- Тесты на один случай - показатель, обратный показателю положительных тестов.
- Индекс строгости - мера строгости ограничений в связи с пандемией, согласно методологии ВОЗ.

Наш подход к анализу СМИ основан на тематическом моделировании (ТМ) [9]. ТМ — это метод, основанный на статистических характеристиках коллекций документов, который используется в задачах автоматического обобщения, информационного поиска и кластеризации. ТМ преобразует в алгоритм интуитивное понимание того, что документы в коллекции образуют группы, в которых различается частота встречаемости слов или словосочетаний. В основе ТМ лежит статистическая модель естественного языка. Вероятностный ТМ описывает документы (М) дискретным распределением на множестве тем (Т), а темы - дискретным распределением на множестве терминов [9].

Для построения тематической модели корпуса документов используется очень популярное латентное распределение Дирихле (LDA) [10]. Некоторым обобщением LDA является аддитивная регуляризация тематических моделей (ARTM), реализованная в виде библиотеки BigARTM [11].

Мы применили тематическую модель BigARTM к корпусу из 1 116 272 новостных публикаций из более чем 30 крупнейших российских и казахстанских интернет-ресурсов.

Рассматриваемый временной интервал охватывает период с 01.01.2020 по 25.02.2021. Сначала была рассчитана тематическая модель с 200 темами, которую мы называем начальной тематической моделью или тематической моделью уровня 0. Затем эксперты вручную отобрали темы, связанные с медициной, пандемией и здравоохранением, и отфильтровали подкорпус, выбрав только те новостные публикации, которые имеют отношение к выбранным темам с весом θ-матрицы выше заданного порога (в данном случае 0,05). Эта тематическая модель называется тематической моделью первого уровня по медицине. Однако тематическая модель 11-го уровня по медицине содержала часть нерелевантных или противоречивых документов и тем, и для улучшения качества подкорпуса, относящегося к медицине и здравоохранению, описанный процесс был повторен с целью получения моделей 2-го и 3-го уровней.

При проведении окончательного анализа использовались три тематические модели:

- Уровень-0 (начальный) тематическая модель, которая содержит общие темы по основным областям человеческой деятельности, включая экономику, политику, культуру, образование и т.д.
- Уровень-2 - содержит темы, в основном связанные с медициной, пандемией и т.д., но также содержит некоторые пересекающиеся темы, такие как ограничения в образовании, спорте и общественной жизни из-за пандемии, общая ситуация в экономике и т.д.
- Уровень-3 - содержит только темы, относящиеся к медицине и здравоохранению.
- Тематическая модель уровня-1 не подходит для запланированного анализа из-за большой доли нерелевантных тем.

Затем для каждой из рассматриваемых тематических моделей была рассчитана суточная динамика относительного веса тем. Относительный вес темы — это отношение суммы весов всех опубликованных в данный день документов по данной теме к сумме весов документов по всем темам. Другими словами, это отношение столбца θ-матрицы, представляющего данную тему, к сумме всей θ-матрицы. Таким образом, этот показатель показывает долю информации, относящейся к данной теме на данную дату, и может принимать значения от 0 до 1.

Б. Метод

Для извлечения тематической структуры корпуса используется метод, основанный на тематической модели BigARTM. BigARTM — это библиотека с открытым исходным кодом для тематического моделирования больших коллекций текстовых документов и наборов транзакционных данных. Тематическая модель определяет, к каким темам относится каждый документ и какие слова описывают каждую тему. Модель обучается без учителя (unsupervised learning) [12]. Затем рассчитывается коэффициент корреляции Пирсона. Этот коэффициент используется для описания корреляции между двумя группами различных данных, т.е. коэффициент корреляции между каждой независимой переменной и зависимой переменной. Коэффициент корреляции Пирсона рассчитывается между ежедневными относительными весами тем и вышеупомянутыми показателями ВОЗ, а затем для нахождения тем с наибольшей корреляцией. Преимущество использования этого метода заключается в том, что взаимосвязь между переменными может быть четко определена и выражена количественно. Затем полученная информация может быть использована для анализа и интерпретирована экспертами. Предлагается провести данный анализ посредством следующих фильтров и параметров:

1) Для Российской Федерации и Республики Казахстан отдельно.
2) Для каждого из трех уровней тематических моделей отдельно.
3) Для каждого из 7 индикаторов ВОЗ, выбранных для анализа.

III. Результаты и обсуждения

В результате применения предложенного метода было получено 42 отсортированных списка тем с корреляцией с соответствующими показателями, что представляет собой анализ по 2 странам, 3 моделям тем и 7 различным показателям. Затем списки верхних и нижних тем с соответствующими значениями корреляции Пирсона были вручную проанализированы экспертами для того, чтобы попытаться сделать некоторые выводы. Таблица 1 иллюстрирует пример анализируемых данных.

Таблица 1. Корреляция между количеством новых смертей от COVID и темами СМИ из модели тем уровня-0 (начальной)

Корреляция	**Название темы (главные слова)**	**Объем темы (документы)**
0.91	Вакцина, вакцинация, лекарство, коронавирус, тест, спутник, российский	15434
0.86	Петербург, Санкт-Петербург, Петербург, Ленинградская область, Москва, отчет_смертей, COVID	1495
0.77	Здоровье, продукт, врач, алкоголь, организм, питание, здоровый	8318
0.74	Рассказать, фото, приехать, уехать, туризм, вернуться, поехать	2693

Корреляция	**Название темы (главные слова)**	**Объем темы (документы)**
0.67	Температура, градус, ночь, снег, погода, воздух, сильный	8196

В ходе интерпретации полученных результатов были сделаны следующие выводы.

- Если рассматривать различные показатели COVID, то новые случаи смерти и новые случаи заболевания имеют более высокую максимальную корреляцию между странами и тематическими моделями (обычно около 0,6-0,8). Однако более объективные показатели, такие как уровень воспроизводства, уровень положительных результатов и количество тестов на один случай, имеют более низкую максимальную корреляцию (обычно около 0,4-0,6). Таким образом, мы утверждаем, что обычно СМИ реагируют предвзято, раздувая или сдувая общественное мнение об эпидемиологической ситуации на основе абсолютных цифр. Например, количество новых случаев бесполезно, если не известно, сколько тестов было проведено, что делает показатель положительных тестов более полезным. Однако СМИ в Казахстане и России, похоже, не учитывают такие данные.
- В Российской Федерации есть темы с высокой корреляцией с индексом строгости (0,75), в то время как в Казахстане самая высокая корреляция с индексом строгости составляет всего 0,43. Это указывает на то, что в Казахстане существует диссонанс между пандемическими ограничениями и тем, как они отражаются в СМИ.
- В Казахстане тема с самой высокой корреляцией (0,8) с количеством новых смертей — это тема, касающаяся "кислорода, расследований, хищений", что может быть интерпретировано как одна из причин скачков количества смертей. В то же время в России темы с наибольшей корреляцией с числом новых смертей (0,82-0,84) связаны с вакцинацией и новой вакциной " Спутник-V". Похоже, была предпринята попытка сгладить панику среди людей, представив им перспективы способов остановить эпидемию.
- Несмотря на то, что это нелогично, существует значительная отрицательная корреляция (-0,3 - -0,4) между количеством новых смертей и случаев заболевания и темами, связанными с экономикой и банковским делом. Похоже, что хотя негативное влияние пандемии на экономику очевидно, в периоды более тяжелых эпидемиологических ситуаций СМИ не уделяли большого внимания экономике и политике, в то время как другие, более нейтральные темы, такие как знаменитости, образ жизни, культура и искусство, не имеют значительной корреляции с эпидемиологическими показателями.

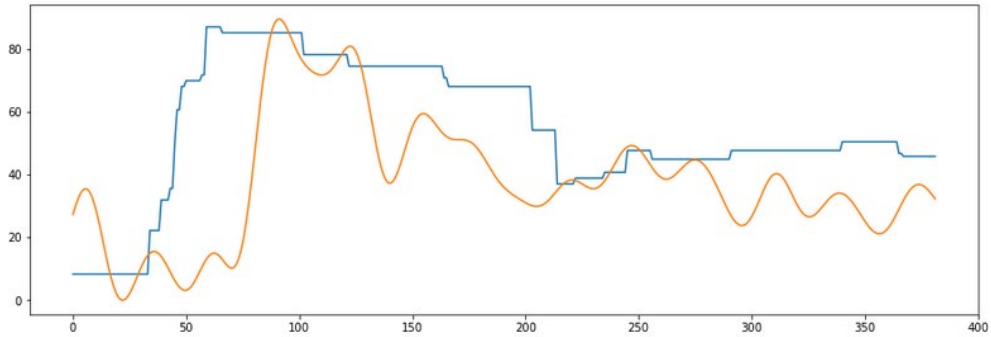


Рис. 2. Синяя линия - индекс строгости в России, желтая линия - тема с наибольшей корреляцией (0,75), относящаяся к сообщениям о случаях COVID в разных регионах.

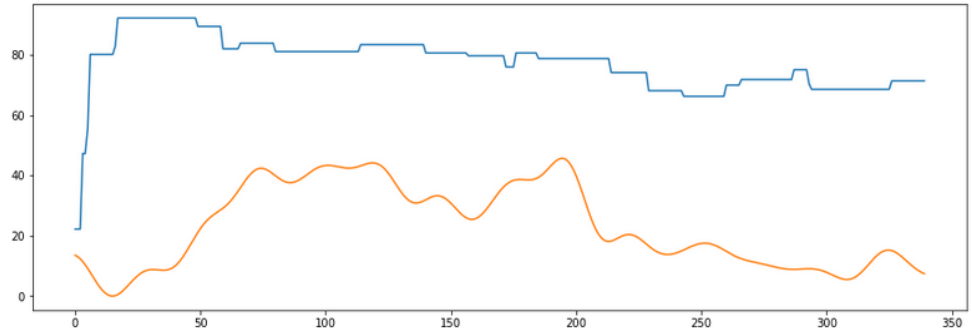


Рис. 3. Синяя линия - индекс строгости в Казахстане, желтая линия - тема с самой высокой корреляцией (0,43), относящаяся к сообщениям о случаях COVID в разных регионах.

IV. ЗАКЛЮЧЕНИЕ

В заключение был предложен метод анализа того, как объективные статистические показатели, связанные с COVID, отражаются в СМИ. Метод основан на применении тематической модели BigARTM для получения тематической структуры корпуса, для последующего проведения корреляционного анализа с показателями COVID, такими как количество новых случаев, процент положительных тестов, индекс строгости и другие.

Предложенный метод обладает высоким потенциалом для получения информации о том, как COVID представляется в СМИ и какой тип статистических данных способствует активности СМИ. Например, было выявлено, что СМИ в России и Казахстане склонны фокусироваться на абсолютных значениях новых случаев/смертей в день, в то время как более информативные показатели, такие как частота положительных тестов и частота репродукции вируса, не освещаются и не показывают значительной корреляции с активностью публикаций.

Кроме того, метод может быть применен для оценки того, как серьезность ограничений отражается в СМИ, выявления тем, которые могут указывать на причины ухудшения эпидемиологической ситуации,

Направления дальнейших исследований включают:

- Провести анализ настроений в новостях и сравнить их с данными COVID.
- Попытаться выявить возможные статистические неточности официальных показателей COVID-19, используя данные СМИ.

- Построить и проанализировать тематический профиль пандемии COVID-19 и то, как он менялся во времени, чтобы попытаться оценить его влияние на экономику, образование, политику, туризм и т.д.

Благодарности

Данное исследование финансировалось Комитетом по науке Министерства образования и науки Республики Казахстан (грант № IRN AP09259587 "Разработка методов и алгоритмов интеллектуальной ГИС для многокритериального анализа данных здравоохранения").

Данная работа была частично поддержана Словацким агентством по исследованиям и развитию, грант № APVV PP-COVID. APVV PP-COVID-20-0013 "Разработка методов оценки риска и надежности системы здравоохранения в условиях вспышки коронавируса".

Литература

1. Назарбаев Н.А. Послание Президента Республики Казахстан Н.Назарбаева народу Казахстана. 31 января 2017 г. - https://www.akorda.kz/ru/addresses/addresses_of_president/poslanie-prezidenta-respubliki-kazahstan-nnazarbaeva-narodu-kazahstana-31-yanvarya-2017-g (20.08.2021).
2. Atun R. Transitioning health systems for multimorbidity //The Lancet. – 2015. – Т. 386. – №. 9995. – С. 721-722.
3. Baldwin R., Di Mauro B. W. Economics in the time of COVID-19: A new eBook //VOX CEPR Policy Portal. – 2020. – С. 2-3.
4. Орлов Е.М. Категория эффективности в системе здравоохранения //Фундаментальные исследования. – 2010. – №. 4..
5. Tasnim S., Hossain M. M., Mazumder H. Impact of rumors and misinformation on COVID-19 in social media //Journal of preventive medicine and public health. – 2020. – Т. 53. – №. 3. – С. 171-174.
6. Gao J. et al. “Mental health problems and social media exposure during COVID-19 outbreak,” Plos one, vol. 15, no. 4, p. e0231924, 2020.
7. Yakunin K. et al. KazNewsDataset: Single Country Overall Digital Mass Media Publication Corpus //Data. – 2021. – Т. 6. – №. 3. – С. 31.
8. Mukhamediev R. I. et al. Classification of Negative Information on Socially Significant Topics in Mass Media //Symmetry. – 2020. – Т. 12. – №. 12. – С. 1945.
9. Dong E., Du H., Gardner L. An interactive web-based dashboard to track COVID-19 in real time //The Lancet infectious diseases. – 2020. – Т. 20. – №. 5. – С. 533-534.
10. Воронцов К. В., Потапенко А. А. Регуляризация, робастность и разреженность вероятностных тематических моделей //Компьютерные исследования и моделирование. – 2012. – Т. 4. – №. 4. – С. 693-706.
11. Jelodar H. et al. Latent Dirichlet allocation (LDA) and topic modeling: models, applications, a survey //Multimedia Tools and Applications. – 2019. – Т. 78. – №. 11. – С. 15169-15211.
12. Vorontsov K. et al. Bigartm: Open source library for regularized multimodal topic modeling of large collections //International Conference on Analysis of Images, Social Networks and Texts. – Springer, Cham, 2015. – С. 370-381.

ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ ПРОЦЕССОМ АВТОМАТИЗАЦИИ ВЫПОЛНЕНИЯ СЛОЖНЫХ ОПЕРАЦИЙ В СОВОКУПНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ РОБОТОВ

Ускенбаева Р.К.[1], Куандыков А.А.[2], Кальпеева Ж.Б.[1], Рахметова П.М.[1], Сағынулы С.[1]
e-mail: uskenbaevar@gmail.com, abu.kuandykov@mail.ru, z.kalpeyeva@satbayev.university, p.rakhmetova@gmail.com, s.sagynuly@satbayev.university
[1]*Satbayev University, Алматы, Казахстан*
[2]*Международный университет информационных технологий, Алматы, Казахстан*

Аннотация. *Данная работа посвящена исследованию вопросов теории интеллектуальных роботов (ИР), которые представлены модулем программных или интеллектуальных агентов и модулем механотроники, в том числе из механических устройств. Подробно рассматриваются процессы декомпозиция сложных задач автоматизации на конечные задачи, организация объединения упрощенных конечных задач путем построения бизнес-процесса, организация совместной работы и взаимодействия между собой нескольких исполнителей – систем ИР, чтобы суммарная функциональность была достаточна для автоматизации процессов выполнения организованных конечных задач, сложность которых в составе бизнес-процесса высока для одиночных систем.*

Ключевые слова: *интеллектуальные роботы, бизнес-процессы, агенты, конечные задачи, автоматизация процессов.*

1. Введение

Процесс решения и выполнения некоторых сложных задач сводится к совокупности сложных операций или подпроцессов таких как:

- обладающих такими свойствами, как стационарность и подвижность;
- обладающими такими свойствами, как когнитивность и физичность (механически-подвижными свойствами) в микропространстве (рабочее пространство с одной позицией платформы и манипулятора) или в макропространстве (в разных позициях платформы и манипулятора), умственно-рутинность и физическо-рутинность.

Кроме того, пространство задач состоит из таких компонентов (в том числе систем) инфраструктуры, что для решения и выполнения таких сложных задач функциональность одиноких систем может быть недостаточной. Поэтому решение и выполнение таких задач может быть достигнута при объединении функциональности нескольких систем [1, 2]. Эти системы могут быть как стационарными, так и подвижными, а архитектура сильно-связанной и/или слабосвязанной. Функциональность слабосвязанных систем формируется из объединения функциональности сильно-связанных систем так, чтобы было достаточно для решения и выполнения сложных задач заданного пространства.

Объединение функциональности различных систем можно увеличить путем специальной организации (т.е. координации, согласования) по определенному методу. От метода организации сильно-связанных систем зависит уровень объединенной функциональности слабосвязанных систем, которые должны быть достаточными для автоматизированного выполнения задач и операций.

Отметим, что в качестве сильно-связанных систем выступают ИР на уровне модулей. С другой стороны, уменьшение уровня сложности задач достигается специальным организационным методом – декомпозицией и созданием бизнес-процессов, и повторной декомпозицией операций бизнес-процессов.

В целом, работа посвящена исследованию вопросов теории ИР, которые представлены модулями программных или интеллектуальных агентов и модулями механотроники, в том числе из механических устройств.

Изучение вопросов участия в процессе автоматизации сложных задач, исходя из психофизиологических особенностей человека в статье сознательно опускается, т.к. эти вопросы требуют отдельных исследований.

2. Постановка класса задач и процессов выполнения операций

Формулировка задачи, которая формализует выполняемые действия в задании с указанием ограничения осуществляется исходя из условий, поставленных перед системой, и из инфраструктуры.

Например, задания ИР могут быть следующего утверждения (состоящих из совокупности признаков):

«**Используя предметы, произвольным образом, находящиеся в районе «А» построить объект по заданному проекту в районе «В»**».

Для данного задания постановка задачи осуществляется при заданном пространстве, согласно которой составляется инфраструктура: *<задание, инфраструктура>→<задача>*.

Инфраструктура. Инфраструктура для формулируемой задачи имеет следующий вид.

Пусть задано трехмерное Евклидовое (горизонталь и вертикаль) пространство Ω. В зависимости от характера решаемой задачи, пространство представляется различным образом, например, нужны только горизонтальные или/и вертикальные размеры предметов.

Пространство Ω со стороны роботов может разбиваться таким образом. Пространство Ω для i-го робота, состоит из Ω^{MIi} – микропространства или рабочего пространства (пространство вытянутой манипулятором-руки робота) i-го робота, а также Ω^{MAi} – макропространство для i-го робота – это пространство деятельности данного робота. Полное пространство Ω^i для i-го робота. Для робота R_i, который выполняет задания $Зд_i$ пространство выполнения Ω^i может совпадать с полным пространством Ω всего робота [3].

Если роботы в пространстве Ω являются подвижными, то его микро-пространство Ω^{MIi} задается окрестностью предметов, с которыми робот работает.

В частности, для нашей задачи пространство разбито на ячейки в зависимости от необходимости решения задачи. Причем ячейки могут объединятся (группироваться) в районы A, B, C, и т.д.

Пусть, координаты ячейки (например, в ячейках Esh(X,Y)) района A пространства Ω (т.е. $Esh(X,Y) \in A \in \Omega$), задается/характеризуется значением координат, где X_0 и $У_0$ декартовые координаты центра ячейки, района. Любой район (например, A) может включать от одной ячейки до нескольких.

В ячейке (например, в районе A) пространство Ω может иметь конечное множество предметов или элементов,

$$Pr = \{Pr_i\},\ i = 1, I \quad (1)$$

где, Pr_i - i-ой предмет I ограничен ($Pr = \{Pr_i\}$, i = 1, I, где Pr_i - i-ой предмет),

Pr – множество объектов или предметов.

Каждый предмет (объект или элемент) имеет известные характеристики и характеризуется признаками объекта,

$$Pr_i \in Pr:\ \chi(Pr_i) = \{\chi_{ij}\},\ i = 1, I,\ j=1,J_i \quad (2)$$

Характеристики для предметов,

$$Pr_i \in Pr:\ \chi(Pr_i) = \{\chi_{ij}\},\ i = 1, I;\ j = 1, J_i \quad (3)$$

и для предмета,

$$Pr_k \in Pr:\ \chi(Pr_k) = \{\chi_{kh}\},\ k=1,K = I;\ h=1,H_k \quad (4)$$

таковы, что выполняется:

$$\exists \chi_{ij} \neq \chi_{kh} \quad (5)$$

Где,

χ_{ij} - j–ая характеристика i – предмета Pr_i;

χ_{kh} - h –ая характеристика k – предмета Pr_k.

Эти объекты или предметы могут быть как в микропространстве робота $\forall\omega_i \subseteq \Omega$ (т.е. рабочем пространстве робота или $\Omega = \cup\omega_i$), так и в макропространстве деятельности роботов Ω.

Причем, надо отметить, что значения характеристик этих предметов может оставаться постоянным на длительное время $t>\Delta T$.

Отметим, что формализация предметов, элементов или участников пространства могут задаваться пассфреймами, посфреймами, ортофреймами и унифреймами [4, 5], описания которых в работе сознательно опускаем.

Если Роботы в пространстве Ω являются подвижными, то для них микро-пространство Ω^{MIi} задается окрестностью предметов.

В задаче требуется выполнить следующее.

Пусть, из заданных предметов с определенными признаками Pr, $Pr = \{Pr_i\}$, i = 1, I′; $I' \leq I$ следует построить роботам проект (чертеж) объекта PrO из имеющихся предметов.

Требуется в ячейках (Esh) района B, пространства Ω построить объект согласно проекту PrO из предметов $Pr' = \{Pr_i\}$, i = 1, I′; $I' \leq I$.

Требуется взять предмет A(x,y) из адреса (x_1,y_1), перенести по адресу (x_2,y_2) с помощью одной или несколькими рук $\{P_1,P_2, P_3, \ldots, P_i, \ldots, P_n\}$. Характеристики рук будут заданы позже.

Требуется сначала построить алгоритм построения объекта из исходных объектов или предметов заданных районах A и других в Ω.

3. Основные особенности процесса решения задачи такого класса

Анализ показывает, что особенности исследуемого класса задач следующие:

Процесс решения задач состоит из операций (независимо от субъекта и/или системы выполнения) имеющих определенные сложности. Эти операции могут быть стационарными и подвижными, когнитивными, механическими и рутинно-умственными, и рутинно-физическими.

Кроме того, имеются такие задачи или их операции, в которых свойства когнитивность и физичность (микроопераций) в их составе не делимы при существующей инфраструктуре. Причем, для автоматизации и управления процессами выполнения этих операций функциональность одиночных систем недостаточна. Поэтому для автоматизации процессов выполнения таких операций возникает необходимость привлечения нескольких систем (т.е. ИР).

В связи с этим, предлагаем общий подход к решению проблем, для которых требуются методы и средства, позволяющие:

- уменьшить сложности автоматизируемых операции;
- координировать и согласовывать поведение и работы ИР, привлеченных для автоматизации выполнения операций задач между собой с целью максимизировать эффективность их суммарной функциональности.

4. Принципы автоматизации сложных задач с помощью ИР

Принцип упрощения и приспособления к процессам автоматизации выполнения классов задач должны осуществляться с двух сторон: как со стороны автоматизируемых операций, так и со стороны исполнителей.

Со стороны задач или операций, которые должны быть автоматизированы:

1) сложные задачи для выполнения автоматизации могут быть представлены в виде ряда простых задач при имеющей инфраструктуре;
2) простые задачи должны быть организованы между собой определенным образом, так чтобы сложность этих простых задач стали упрощеннее и приспособлены к автоматизированному выполнению.

Со стороны исполнителей автоматизация выполнения задач или операций описываются:

1) Некоторые операции после упрощения и организации могут быть усложнены тем, что функциональность одиночных сильно-связанных систем недостаточна (в частности ИР) для выполнения сложных операций. Поэтому для автоматизации процессов выполнения этих операций, требуется привлечение нескольких систем (сильно-связанных), суммарная функциональность которых была достаточна для автоматизации процессов выполнения этих операций.
2) Привлечение нескольких систем (сильно-связанных), обеспечивающих автоматизацию задач необходимо организовать определенным методом, а именно, обеспечить совместную работу и взаимодействие сильно-связанных систем исполнителей с слабо связанной системой. Данный метод должен обеспечить повышение суммарной функциональности слабосвязанной системы из сильно-связанных систем исполнителей, т.е. ИР.
3) Расширить круг сильно-связанных систем, создавая из них сеть слабосвязанной системы. Повышение функциональности слабосвязанных систем достигается путем организационного метода из совокупности слабосвязанных систем, какими являются ИР.

Тем самым, для исполнения сложных операций с совокупностью сильно-связанных систем, требуется сильно-связанные системы организовать в виде слабосвязанных систем.

5. Технологические основы процессов упрощения сложных задач

Процесс упрощения автоматизации состоит из следующих этапов:

1 этап. Сложные задачи могут быть в первую очередь декомпозированы (процесс декомпозиции может несколько раз повторяться) на ряд более простых подзадач, которые в сумме наследует свойства исходной задачи: когнитивные, физические (механические, подвижные), умственно-рутинные и физическо-рутинные операции.

2 этап. Процесс решения и выполнения декомпозированной задачи, в свою очередь, состоит из операций: когнитивных, физических (механические, подвижные), умственно-рутинных и физическо-рутинных. Поэтому нужны такие исполнители, которые обладают функциями и выполняют эти операции.

3 этап. Деление сложных операций на простые зависит от инфраструктуры их выполнения, и инфраструктуры или средств декомпозиций сложных операций на простые.

Таким образом, сложные задачи или операции сводятся на ряд декомпозированных, более простых, чем первоначальная постановка, т.е. «простым» задачам и их организации между собой. Эти простые задачи далее не декомпозируются при наличии существующих средств декомпозиции или инфраструктур, поэтому назовем их «конечными» задачами.

Суммарная сложность этих декомпозированных «конечных» задач такова, что их решения могут быть достигнуты при совместном (применений) выполнении как когнитивных, так и механических операций, при существующей инфраструктуре. Таким образом, не только первоначальные сложные задачи, но и конечные задачи в сумме содержат: когнитивные, механические и рутинные (умственные и физические) компоненты - операции.

В свою очередь эти «конечные» задачи являются трудными и сложными для автоматизации при наличии имеющихся средств (инфраструктуры) автоматизации.

После декомпозиции и упрощения первоначально сложных задач на «конечные», все еще остается функционально сложным выполнение одиночных сильно-связанных (т.е. ИР) систем.

Было отмечено, что в таких «конечных» задачах когнитивные свойства и физические свойства исходной сложности задач не теряются, они наследуются из исходной задачи. При выполнении таких «конечных» задач, возможно, не найдется система, функциональность которой достаточно для их выполнения. Поэтому следует упростить сложность этих «конечных» задач для автоматического (автоматизированного) выполнения.

Для упрощения сложности задач надо их организовать между собой и средствами их решения, в результате которого процессы их решения станут простыми.

Одним из таких методов организации упрощения процессов решения и выполнения «конечных» задач является построение бизнес-процесса (БП). Такой метод организации можно назвать методом упрощения «объединенной организации «конечных» задач», суть которой сводится к построению бизнес-процесса.

Бизнес-процессы позволяют организовать «конечные» задачи с ресурсами их решения, а также исполнителями этих задач в единый процесс. Однако, и после

построения бизнес-процесса некоторые операции, т.е. «конечные» задачи могут оказаться сложными с точки зрения их исполнения одними сильно-связанными (т.е. ИР) системами.

Исполнение некоторых операций БП для сильно-связанной системы может быть сложной и не выполнимой из-за недостаточности ее функциональности среди сильно-связанных систем, имеющихся в заданном пространстве. Решение таких операций БП или «конечных» задач могут быть достигнуты при объединении функциональности нескольких систем. Объединение функциональности (т.е. суммарная функциональность) систем должны быть достаточны для выполнения операций БП или «конечных» задач.

Одним из методов организации объединения сильно-связанных систем (т.е. ИР) является метод организации слабосвязанных систем из сильно-связанных систем (т.е. из совокупности ИР). Другими словами, объединением совокупности ИР в слабосвязанных системах с определенным методом организации, тем самым объединяем функциональность в общую функциональность.

Предполагается, что когнитивные операции могут выполняться как стационарными, так и подвижными системами сильно-связанного и слабосвязанного типа. Другими словами, когнитивные и умственно-рутинные операции могут быть выполнены системами как стационарного, так и подвижного типов, т.к. для выполнения этих операций достаточно удаленного режима через беспроводную связь.

Но если для выполнения когнитивных операций достаточно неконтактное, а удаленное взаимодействие различных систем, то для выполнения механических операций требуются обязательно контактные совмещения. Другими словами, для выполнения физических и рутинно-физических операций необходимы системы (сильно-связанными или слабосвязанными системами) подвижного типа, т.к. для выполнения этих операции необходим физический контакт, кроме удаленного режима через беспроводную связь.

Как сложные когнитивные, так и сложные физические операции могут выполняться одним и тем же типом - подвижными системами, которые являются как сильно-связанными типами по отдельности, так и слабосвязанными типами при их объединении для совместной деятельности.

Если в качестве систем принять ИР, то он может выполнить:

1) когнитивные операции/функции;
2) перемещение в пространстве (механические операции в макропространстве);
3) манипуляции в рабочем пространстве (в микропространстве).

Таким образом, ИР является системой, выполняющей все виды операций: когнитивные, физические.

В качестве сильно-связанных систем выступают одиночные интеллектуальные роботы (ИР), созданные по сильно-связанному модульному принципу.

Объединение сильно-связанных систем (т.е. ИР) в слабосвязанные происходит по методу организации на основе признаков для определенной цели (т.е. организация объединения ИР).

В качестве сильно-связанных систем выступает ИР, а в качестве слабосвязанных системы выступает объединение ИР по определенному методу организации.

Резюмируя, можно утверждать, что для решения вопросов автоматизации сложных задач или операций следует упростить сложность операций, особенно механических, т.к. для их выполнения требуется контакт систем-исполнителей. Для выполнения сложных когнитивных и механических задач (операции) применяют как стационарные, так и подвижные системы, но для выполнения сложных механических задач (операции) применяют только подвижные системы.

6. Концептуальный алгоритм решения и выполнения теоретической задачи ИР

Общий алгоритм заданного класса задач включает проектирование плана решения, программы исполнения его в едином информационном потоке и состоит из следующих этапов:

1. Постановка задачи;
2. Решение или составление плана решения задачи: план промежуточных целей для достижения глобальной цели;
3. Формирование логической модели БП решения задачи;
4. Формирование архитектуры БП для решения и выполнения задачи на макро-уровне, который является подуровнем исполнительного уровня;
5. Формирование компонентов и операторов БП;
6. Программирование процесса выполнения макро-операций на операциях БП;
7. Декомпозиция макро-операций на подоперации или микрооперации и далее насколько инфраструктура позволяет;
8. Оценка способности ИР: обладает ли универсальными свойствами для задач выполняемого класса или специализированными свойства;
9. Для выполнения макро-операций выбор ИР-исполнителей состоит из:

- назначение исполнителя для макро-операции. Если у макро-операции имеется микрооперации, то выбор ИР менеджера качества среди претендентов. Если макро-операция без декомпозиции, то необходимо выбрать для него ИР-исполнителя;
- оценка необходимого количества ИР для выполнения микрооперации;
- программирование исполнения микрооперации из действий k к количеству ИР;
- программирование каждого действия (последовательность и одновременное выполнение действий) ИР приводам;
- определение величины каждого действия приводами ИР;
- определение законов выполнения действий – определения законов выработки управляющих воздействий на привод (программирование для всех приводов), например, по законам: П, ПД, ПИ, ПИД;

10. Исполнение или выполнение действия привода по законам П, ПД, ПИ, ПИД;
11. Запоминание протоколов выполнения задания;
12. Обучение и завершение цикла решения задач.

Концептуальный алгоритм заданного класса задач может конкретизоваться исходя из параметров и характеристики экземпляра заданного класса задач и из особенности единого информационного пространства. В качестве единого информационного пространства для деятельности ИР могут выступить пространства с различными характеристиками, в частности пространства горного карьера, ландшафт района города, отделение больниц и т.д.

Заключение

В работе изложены некоторые теоретические положения интеллектуальных роботов. Понятие интеллектуального робота в работе сознательно не приводятся, хотя оно формально является интеграцией агентов и механических модулей.

Приведена формулировка задачи, которую надо выполнить одному или множеству ИР в заданном пространстве Ω. Разные сферы человеко-машинной деятельности по разному формулируются и конкретизируются в зависимости от параметров (характеристик) задачи, инфраструктуры и окружающей среды в Ω.

Исходя из возможности инфраструктуры в Ω, одним из составляющих которого выступает множества ИР, формируется алгоритм решения поставленной задачи. Причем, приведена только структура алгоритма, а не процедура.

Литература

1. Kuandykov, A.A. The formalization of problem area, implementation and maintance of and service of business-process by group of unmanned vehicles / A.A. Kuandykov. // IJCTA, 2013. – P. 79-82.

2. Uskenbayeva, R.K., Kuandykov, A.A., Cho, Young Im, Kalpeyeva, Zh.B., Kozhamzharova, D.K. Organization of computing processes in the large heterogeneous distributed systems / R.K. Uskenbayeva, A.A. Kuandykov, Young Im Cho, Zh.B. Kalpeyeva, D.K. Kozhamzharova // 44th International Symposium on Digital Object Identifier: 10.1109/ISR.2013.6695697, 2013. - P. 1- 4.

3. Uskenbayeva R.K., Kuandykov A.A, Cho Young Im, Kozhamzharova D.K., Kalpeyeva Zh.B. Models and Methods of Joint Work Management of Group of Unmanned Vehicles / R.K. Uskenbayeva, A.A. Kuandykov, Young Im Cho, D.K. Kozhamzharova, Zh.B. Kalpeyeva // 13th International Conference on Control, Automation and Systems (ICCAS 2013), 2013.

4. Kuandykov A.A. Fundamentals of the axiomatic theory of situational management of complex objects / A.A. Kuandykov // Astana: Vestnik ENU, 2009. №2, P. 57-63.

5. Kuandykov A.A. Axiomatic foundations of a formal system of managing complex objects / A.A. Kuandykov // Proceedings National Academy of Sciences of RK series of Physics and Mathematics, 2009. – Vol. 5, - P. 12-15.

6. Kuandykov A.A., Kozhamzharova D.Kh., Karimzhan N.B., Baimuratov O.A. Design and construction a model of remote control software mobile robot for MAS / A.A. Kuandykov, D.Kh. Kozhamzharova, N.B. Karimzhan, O.A. Baimuratov // 2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), 2014. – P. 1- 5.

ОТ КЛАССИЧЕСКОГО МАШИННОГО ОБУЧЕНИЯ К ГЛУБОКОМУ. ОСНОВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

Мухамедиев Р.И., Сымагулов А., Кучин Я., Якунин К., Елис М.
e-mail: ravil.muhamedyev@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан
Satbayev University, Казахстан

Аннотация. *Существуют многообещающие перспективы на пути к широкому использованию ИИ, а также проблемы, которые необходимо преодолеть для адаптации технологий AI&ML в отраслях промышленности. В статье систематизированы разделы ИИ и рассчитана динамика изменения количества научных статей в разделах машинного обучения по данным Google Scholar. Использован метод расчета динамических показателей изменения публикационной активности: темпа роста (D1) и ускорения роста (D2) научных публикаций. Анализ публикационной активности, в частности, показал высокий интерес к современным моделям трансформеров, развитие наборов данных для некоторых отраслей промышленности, а также резкий рост интереса к методам объясняющего машинного обучения. Относительно небольшие исследовательские области получают все больше внимания, о чем свидетельствует отрицательная корреляция между количеством статей и оценками D1 и D2.*

В статье представлены результаты по более чем 400 поисковым запросам, связанным с классифицированными областями исследований и применением моделей машинного обучения в отраслях.

Работа представляет собой сокращенный авторский перевод статьи [Mukhamediev R. I. et al. From Classical Machine Learning to Deep Neural Networks: A Simplified Scientometric Review //Applied Sciences. – 2021. – Т. 11. – №. 12. – С. 5541.]

Результаты расчетов и программное обеспечение можно скачать https://www.dropbox.com/sh/fkfw3a1hkf0suvc/AACRZ7v9qympen_ht00jeiF6a?dl=0.

Ключевые слова. Искусственный интеллект; машинное обучение; глубокое обучение; объясняемое машинное обучение; трансферное обучение; сверточные нейронные сети; рекуррентные нейронные сети; трансформеры; наукометрия; библиометрические показатели.

1. Введение

Для успешного экономически обоснованного развития традиционных и новых производств, увеличения объемов производства и производительности труда необходимы новые технологии, связанные не только с технологиями добычи, переработки и производства, но и со сбором, обработкой и анализом данных, сопровождающих эти процессы. Безусловно, одним из наиболее перспективных инструментов в этой области развития является искусственный интеллект (ИИ). ИИ уже приносит значительные экономические выгоды в здравоохранении [1], торговле, транспорте, логистике, автоматизированном производстве, банковском деле и т.д. [2]. Многие страны разрабатывают или уже приняли свои стратегии по использованию и развитию ИИ [3]. В то же время на пути к широкому использованию ИИ есть как многообещающие перспективы, так и некоторые

препятствия, преодоление которых означает новый виток технологического развития ИИ и расширение сферы его применения.

Эволюция каждого научного направления, в том числе и ИИ, сопровождается повышением или понижением интереса исследователей, что отражается в изменении библиометрических показателей. Выявление "горячих" областей, в которых эти показатели более весомы, позволяет лучше понять ситуацию в науке и, по возможности, сконцентрировать усилия на прорывных направлениях.

Область машинного обучения (МО) и ИИ характеризуется широким спектром методов и задач, некоторые из которых уже имеют приемлемые решения, реализованные в виде программного обеспечения, а другие требуют интенсивных исследований.

Для выявления логики изменений в публикационной активности в [4] предложены дифференциальные индикаторы.

На наш взгляд, использование динамических показателей наряду с полнотекстовым анализом позволяет более точно оценить потенциал исследовательских областей.

В данной работе в качестве анализируемых показателей рассматривается количество публикаций статей с выбранными ключевыми терминами. Дифференциальные метрики позволяют оценить динамику изменений в использовании выбранных ключевых терминов авторами научных публикаций, что косвенно свидетельствует о росте или снижении интереса исследователей к научной области, обозначенной данным термином.

Задачи исследования:

1. Систематизация разделов ИИ и МО по литературным данным;

2. Оценка изменений в публикационной активности в ИИ исМО с использованием дифференциальных показателей для выявления быстрорастущих и "угасающих" исследовательских областей.

Данная статья представляет в сокращенном авторском переводе материалы статьи [Mukhamediev R. I. et al. From Classical Machine Learning to Deep Neural Networks: A Simplified Scientometric Review //Applied Sciences. – 2021. – Т. 11. – №. 12. – С. 5541.]

2. Метод

Детали метода изложены в работе в упомянутой работе [22.]

3. Результаты и обсуждение

Общее количество публикаций ИИ и МО и изменения в некоторых областях, сокращающихся и растущих в 2015-2020 годах, показаны на рисунке 1. Видно, что общее количество статей, достигшее пика в 674 тысячи в 2019 году, значительно снизилось в 2020 году (594 тысячи). На графике видно замедление общего роста с 2018 года. Причиной этого является снижение с 2017 года количества статей с ключевыми словами Robotics, Expert Systems и т.д., которое не могло быть компенсировано ростом разделов глубокого обучения.

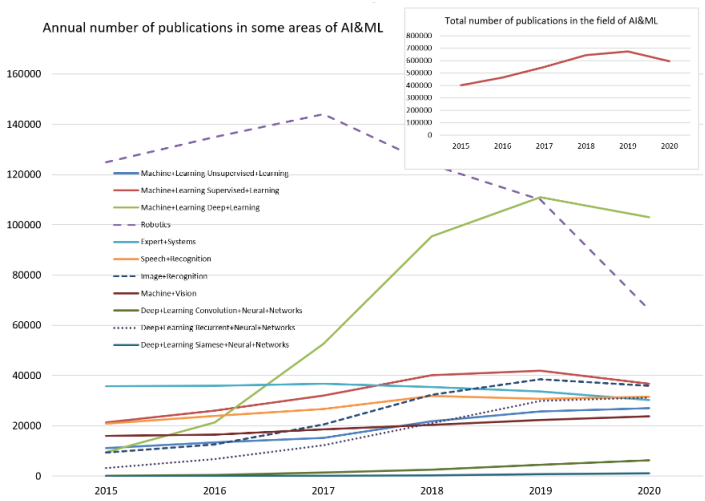


Рисунок 1. Ежегодное количество публикаций в области ИИиМО

Показатели D1 и D2 расчитаны основных разделов ИИ (рис. 2), популярности основных моделей машинного обучения и глубокого обучения (рис. 3, 4), публикационной активности, связанной с объяснительными приложениями ИИ и современными моделями МО в экономике (см. [22]).

Интерпретация значений индикаторов D1 и D2, следующая:

- Когда оба значения (D1, D2) положительны, это указывает на ускоренный рост количества статей в данной области;
- Когда D1 отрицательно, а D2 положительно, это указывает на уменьшение числа статей;
- Когда D1 положителен, а D2 отрицателен, это указывает на замедление роста числа статей;
- Когда оба значения отрицательны, это указывает на ускоренное снижение количества статей.

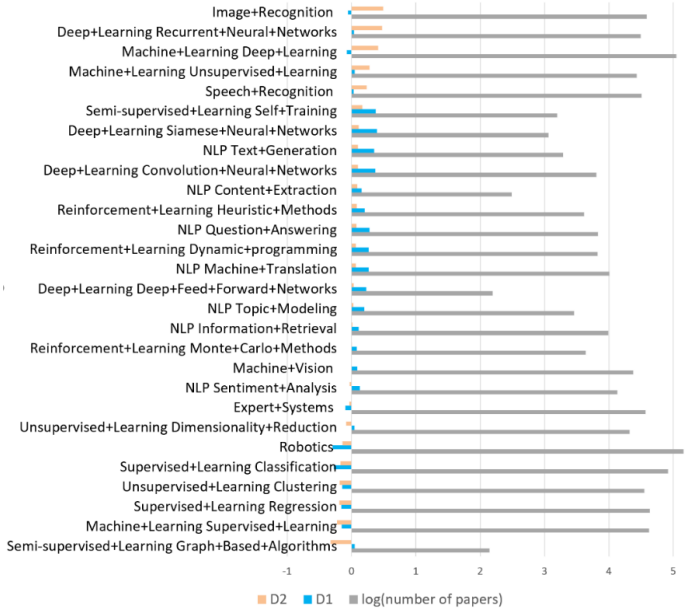


Рисунок 2. Популярность разделов ИИ. Серым цветом показано количество статей в логарифмической шкале. В бирюзовом цвете D1, в оранжевом D2.

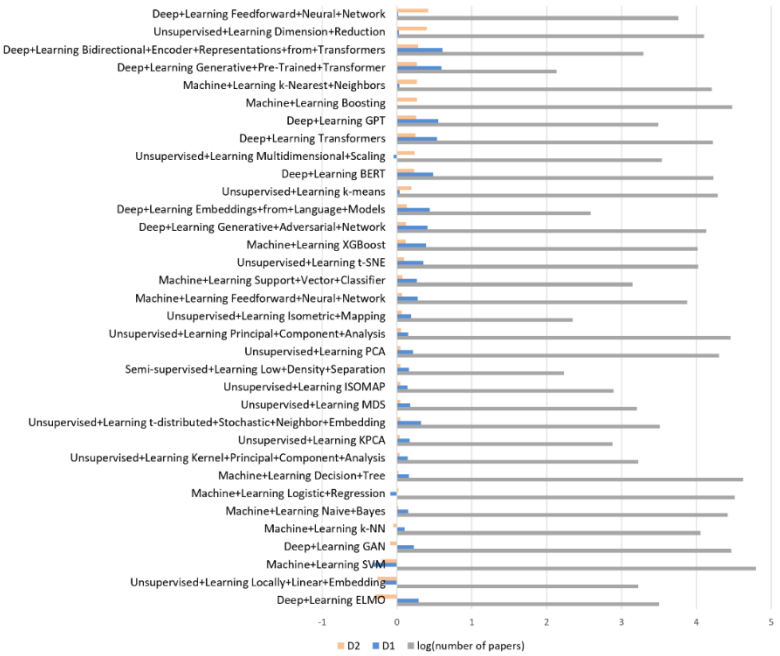


Рисунок 3. Использование популярных моделей обучения без учителя (Unsupervised Learning), машинного обучения (MO), глубокого обучения (DL). Серым цветом показано количество статей в логарифмической шкале. В бирюзовом цвете D1, в оранжевом D2.

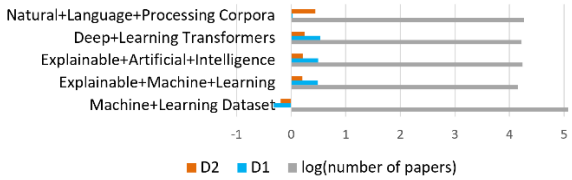


Рисунок 4. Интерес исследователей к методам объяснительного машинного обучения и разработке наборов данных и корпусов текстов. Серым цветом показано количество статей в логарифмической шкале. В бирюзовом цвете D1, в оранжевом D2.

Поскольку некоторые домены не имеют большого количества публикаций, на графиках показано максимальное количество статей (мкс) в домене за период анализа в логарифмическом масштабе - log_{10}(мкс).

Рисунок 3 показывает значительное увеличение публикационной активности в области глубокого обучения, что было ожидаемо. Зрелость и актуальность научной области можно оценить по количеству обзорных статей. Мы провели такой анализ для разделов машинного обучения, подсчитав статьи, содержащие в названии термины review/overview/survey. Наибольшее количество таких обзоров приходится на область глубокого обучения (852 за 2020 год, увеличение более чем в 20 раз с 2015 года), обучение с подкреплением (101 статья за 2020 год, увеличение более чем в 10 раз с 2015 года) и обучения с учителем (38 статей за 2020 год, увеличение с 2015 года более чем в семь раз). Объяснение результатов моделей машинного обучения является серьезной проблемой, препятствующей широкому использованию ИИ в здравоохранении [5], банковском деле и многих других областях [6]. Рисунок 3

показывает значительный и ускоряющийся рост публикационной активности в области объяснимого машинного обучения и применения трансформеров.

В области применения МО наблюдается значительный рост числа публикаций, связанных с терминами "набор данных", "точное сельское хозяйство", "точное земледелие" и т.д. Действительно, в области глубокого обучения решение многих задач зависит от объема и качества наборов данных. Проблема нехватки данных в компьютерном зрении преодолевается с помощью синтетических наборов, созданных в графических редакторах 3D [10], игровых движках и средах [11-14]. Такие наборы данных, в частности, использовались для обучения беспилотных автомобилей [15] и в других областях [16]. В последнее время для их генерации также используются генеративные состязательные сети [17,18].

Активность в публикациях позволяет оценить, какие именные группы алгоритмов наиболее востребованы на практике. В частности, в [19] было выявлено, что технологии глубокого обучения демонстрируют высокий рост публикационной активности применительно к здравоохранению. Текущий анализ подтверждает, что здравоохранение является одной из популярных областей применения глубокого обучения. Например, модели трансформеров (BERT) и генеративные состязательные сети демонстрируют очень высокие показатели D1 и D2 в сочетании с термином здравоохранение. BERT применительно ко многим отраслям (разработка, производство, связь, электроэнергетика, цепочки поставок и т. д.) демонстрирует высокие темпы роста публикаций. В то же время выборка для поисковых терминов Electricity Deep + Learning, Social + Services Deep + Learning показывает резкое замедление роста публикаций. Это явление можно интерпретировать как возможное изменение интереса исследователей к новым терминам, описывающим современные модели глубокого обучения.

Основываясь на значениях D1 и D2, можно сделать следующие предположения:

- В целом, количество публикаций в области ИИ&МО будет уменьшаться.
- Новые области, такие как применение трансформеров и объяснимое машинное обучение, будут быстро развиваться.
- Классические модели машинного обучения, такие как SVM, k-NN, логистическая регрессия, будут привлекать меньше внимания исследователей.
- Количество статей о кластерных моделях продолжит расти.

4. Выводы

Мир ИИ огромен. Самой быстрорастущей областью исследований является машинное обучение, а в его рамках - модели глубокого обучения. Практически ежедневно появляются новые результаты, а также приложения ранее предложенных сетей. Эта область исследований и приложений включает в себя большое семейство сетей для распознавания текста, речи и почерка, сети для преобразования и стилизации изображений, а также сети для обработки временных последовательностей.

В работе [22] мы систематизировали разделы ИИ и оценили динамику изменения количества научных статей в доменах машинного обучения по данным Google Scholar. Результаты показывают, что, во-первых, можно определить быстрорастущие и "угасающие" научные домены для любого "разумного" числа статей (>100), а во-вторых, предсказание публикационной активности возможно в краткосрочной перспективе с достаточной для практики точностью.

Использованный нами метод имеет некоторые ограничения, в частности:

1. При всей глубине неформального анализа набор терминов все равно задается человеком. Следовательно, некоторые статьи, входящие в исследуемый раздел, могут быть пропущены, и, наоборот, некоторые публикации могут быть ошибочно отнесены к рассматриваемой теме. Мы также не можем гарантировать исчерпывающую полноту и последовательность проведенного эмпирического обзора;

2. Данный анализ не учитывает тот факт, что значимость конкретной научной темы определяется не только количеством статей, но и объемом цитирования, "весом" индивидуальных характеристик авторов, качеством журналов и так далее;

3. Метод не оценивает процессы смены терминов и семантическую близость научных областей.

Полученные оценки, несмотря на описанные ограничения примененного подхода, соответствуют эмпирическим наблюдениям, связанным с ростом применения моделей глубокого обучения, построением объяснимых систем искусственного интеллекта, увеличением количества и разнообразия наборов данных для многих приложений машинного обучения. Анализ показывает, что усилия научного сообщества направлены на преодоление технологических ограничений МО. В частности, уже разработаны и в некоторых случаях успешно применяются методы генерации наборов данных, объяснение результатов работы систем машинного обучения и ускорения обучения. Однако для преодоления описанных ограничений для большинства приложений ИИ необходимы новые решения. Как только это произойдет, мы станем свидетелями нового этапа в развитии приложений ИИ.

Будущие исследования могут быть сосредоточены на использовании преимуществ тематического моделирования и анализа текстов. Мы планируем использовать классическое тематическое моделирование [20] и Embedded Topic Model [21] для автоматической кластеризации корпуса научных публикаций и выявления связанных терминов. Кроме того, более продвинутый скрапер будет предоставлять данные о количестве цитирований статей и качестве научных журналов.

Литература

1. Социально-экономическое влияние ИИ в здравоохранении. – https://www.medtecheurope.org/wp-content/uploads/2020/10/mte-ai_impact-in-healthcare_oct2020_report.pdf (дата обращения: 10 мая 2021 года).

2. Haseeb M. et al. Economic impact of artificial intelligence: new look for the macroeconomic assessment in Asia-Pacific region //International Journal of Computational Intelligence Systems. – 2019. – Т. 12. – №. 2. – С. 1295-1310.

3. Van Roy V. et al. AI Watch-National strategies on Artificial Intelligence: A European perspective in 2019. – Joint Research Centre (Seville site), 2020. – №. JRC119974.

4. Muhamedyev R. I. et al. New bibliometric indicators for prospectivity estimation of research fields. Annals of Library and Information Studies (ALIS). – 2018. – Т. 65. – №. 1. – С. 62-69.

5. Davenport T., Kalakota R. The potential for artificial intelligence in healthcare //Future healthcare journal. – 2019. – Т. 6. – №. 2. – С. 94.

6. Arrieta A. B. et al. Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI //Information Fusion. – 2020. – Т. 58. – С. 82-115.

7. ImageNet. – http://image-net.org/index (дата обращения: 10 мая 2021 года).
8. Open Images Dataset M5+ Extensions. – https://storage.googleapis.com/openimages/web/index.html (дата обращения: 10 мая 2021 года).
9. COCO dataset. – http://cocodataset.org/#home (дата обращения: 10 мая 2021 года).
10. Wong M. Z. et al. Synthetic dataset generation for object-to-model deep learning in industrial applications //PeerJ Computer Science. – 2019. – Т. 5. – С. e222.
11. Ros G. et al. The synthia dataset: A large collection of synthetic images for semantic segmentation of urban scenes //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2016. – С. 3234-3243.
12. Sooyoung C. et al. How to Generate Image Dataset based on 3D Model and Deep Learning Method. International Journal of Engineering and Technology(UAE). – 2018. – Т. 7. – С. 221-225.
13. Müller M. et al. Sim4cv: A photo-realistic simulator for computer vision applications //International Journal of Computer Vision. – 2018. – Т. 126. – №. 9. – С. 902-919.
14. Doan A. D. et al. G2D: from GTA to Data //arXiv preprint arXiv:1806.07381. – 2018.
15. Dosovitskiy A. et al. CARLA: An open urban driving simulator //Conference on robot learning. – PMLR, 2017. – С. 1-16.
16. Kuchin Y. I., Mukhamediev R. I., Yakunin K. O. One method of generating synthetic data to assess the upper limit of machine learning algorithms performance //Cogent Engineering. – 2020. – Т. 7. – №. 1. – С. 1718821.
17. Arvanitis T. N. et al. A Method for Machine Learning Generation of Realistic Synthetic Datasets for Validating Healthcare Applications //medRxiv. – 2021.
18. Nikolenko S.I. Synthetic data for deep learning. arXiv preprint arXiv:1909.11512 2019.
19. Mukhamedyev R. I. et al. Assessment of the dynamics of publication activity in the field of natural language processing and deep learning //International Conference on Digital Transformation and Global Society. – Springer, Cham, 2019. – С. 744-753.
20. Blei D. M., Ng A. Y., Jordan M. I. Latent dirichlet allocation //the Journal of machine Learning research. – 2003. – Т. 3. – С. 993-1022.
21. Dieng A. B., Ruiz F. J. R., Blei D. M. Topic modeling in embedding spaces //Transactions of the Association for Computational Linguistics. – 2020. – Т. 8. – С. 439-453.
22. Mukhamediev R. I. et al. From Classical Machine Learning to Deep Neural Networks: A Simplified Scientometric Review //Applied Sciences. – 2021. – Т. 11. – №. 12. – С. 5541.

СЕКЦИЯ 4

Деректерді қорғау және ақпараттық қауіпсіздік. Ақпаратты қорғаудың бағдарламалық-техникалық құралдары. Күрделі жүйелердің ақпараттық қауіпсіздігін камтамассыз етудің математикалық әдістері.

Информационная безопасность и защита данных. Программно-технические средства защиты информации. Математические методы обеспечения информационной безопасности сложных систем

Information security and data protection. Software and hardware for information protection. Mathematical methods of ensuring information security of complex systems

ЗАЩИТА ЛИНИЙ СВЯЗИ НА ФИЗИЧЕСКОМ УРОВНЕ

Луценко Г.В.
e-mail: lucenco@mail.ru
Академия Комитета национальной безопасности Республики Казахстан.

***Аннотация**. В данном докладе, рассматриваются нестандартные схемы соединения оборудования с пространственным распределением соединительных линий, который позволит передавать каналы приёма и передачи данных по разным кабелям, прокладываемым по разным маршрутам. Тем самым повышается уровень информационной безопасности, а применение сетевого ключа ускоряет процесс переключения проводов линий передачи сигналов.*

Надёжная, безопасная и защищённая связь является неотъемлемой частью современного бизнеса. Степень безопасности этой связи определяется её защищённостью, что позволяет работникам организации вести конфиденциальные переговоры и обмениваться информацией.

Используемые каналы передачи информации не всегда гарантируют защиту передаваемых данных. Большие корпорации используют методы криптографической защиты операционных систем и других методов шифрования включая аппаратные средства. Такой метод защиты информации в некоторых случаях получается дорогостоящим и не всегда применим.

Анализ фактического состояния функционирования защищённой связи свидетельствует о проявлении проблем, не позволяющих в полной мере гарантировать её безопасную работу. Применение стандартных методов применения каналообразующего оборудования предполагает наличие уязвимости технических каналов передачи информации с ограниченным доступом через линии связи, электропитания и заземления. Одной из угроз является способ съёма информации через параллельное подключение ноутбука со специальным программным обеспечением, описанного в журнале «Хакер» [1]. Данный способ легко реализуем при стандартном подключении к линии связи. Поэтому необходимо рассмотреть возможности нестандартных соединений технических средств канала, что позволит минимизировать риски по утечке информации. Нестандартные соединения линий связи позволят усложнить способ получения информации и заставят злоумышленника отказаться от съёма информации методом параллельного подключения к линии связи и искать другие пути перехвата данных.

Для изучения возможности съёма и защиты информации на фрагменте вычислительной сети от маршрутизатора до рабочих компьютеров оперативных работников рассмотрим структурную схему организации связи с удалёнными объектами (Рисунок 1), которая построена по технологии сети Ethernet.

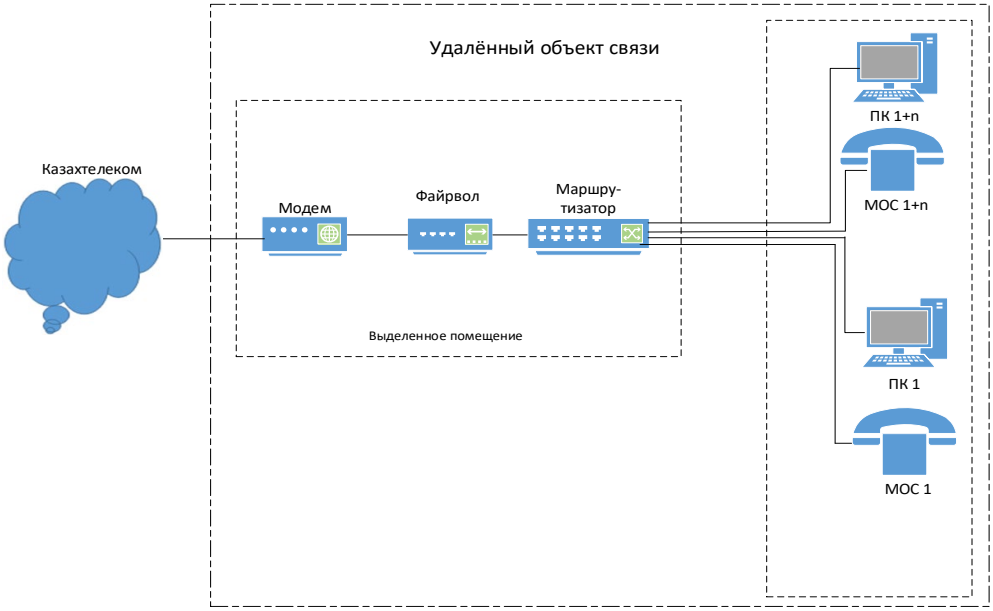


Рис. 1. Схема организации связи с удалёнными объектами

Проблемам защищенности каналов передачи данных и способам перехвата информации с них посвящено немалое количество статей и книг. Доктор технических наук, профессор, заведующий кафедрой информационной безопасности Московского института электронной техники Хорев А.А. является специалистом в области противодействия техническим разведкам и технической защиты информации и большое внимание в своих работах уделял вопросам эффективности защиты средств вычислительной техники от утечки информации по техническим каналам [2], [3].

В своём учебном пособии Хорев А.А. [4] описывает процесс перехвата данных с помощью специального программного обеспечения со съёмником, который подключается в разрыв линии вычислительной сети. При использовании такого съёмника не исключено пропадание связи между клиентами локально-вычислительной сети, которые сделают заявку на проверку и ремонт канала передачи данных. Работники провайдера связи при обследовании канала передачи данных, могут обнаружить разрыв жил кабеля и инициировать мероприятия по выяснению причин выхода его из строя.

В учебном пособии «Методы и средства инженерно-технической защиты информации», составленном под редакцией доктора технических наук, профессора Аверчинкова В.И., описаны методы защиты информации в каналах связи, основанные на предохранении линии от электромагнитных наводок посредством уменьшения магнитной и электрической связи, то есть снизить напряжение источника сигнала или тока, уменьшить площадь петли, передавать сигналы постоянным током или на низких частотах, и т.п. [5].

В интернет-издании журнала Хакер [1] подробно описан процесс съёма информации с витой пары[9] методом параллельного подключения. Имея в арсенале канцелярский нож, ноутбук с программным обеспечением для снифинга (прослушивания канала передачи данных), скачанное с интернет сети, можно

[9] Витая пара – вид кабеля связи. Представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с наибольшим числом витков на единицу длинны), покрытых пластиковой оболочкой.

осуществлять съём информации с сети передачи данных. Для этого надрезается оболочка сетевого кабеля, отыскиваются либо к оранжевый (оранжево-белой) (схема А), либо к зеленый (зелено-белой) паре (схема В) согласно инструкции по обжиму сетевого кабеля [6]. Оба варианта обжима сетевого кабеля представлены на рисунке 2. Согласно инструкции обжима сетевого кабеля и задач прослушивания трафика (приём 3-ий и 6-ой контакт или передача осуществляется по 1-му и 2-му контакту) выбираются соответствующие цвета проводов для подключения. Доверять монтажникам не стоит, поэтому надо попробовать 2 варианта: оранжевую и зеленую пару (в редких случаях цвета могут быть совсем перепутаны). Схема присоединения проста: плюс к плюсу, минус к минусу. То есть одноцветный провод к одноцветному, полосатый к полосатому. Все это также придется делать с оглядкой на инструкцию по обжиму: положительный провод - полосатый, отрицательный - однотонный. Если монтажники не соблюдали инструкцию, то определить, какой из них какой, без сложной и громоздкой аппаратуры не представляется возможным – только перебор [1]. Перебор проводов кабеля, состоящего из 8ми жил требует определения необходимых комбинаций подключения.

Необходимо отметить, что в статье [1] акцентируется внимание читателя на том, что найти необходимые провода без сложной и громоздкой аппаратуры не представляется возможным, а для определения необходимых жил кабеля методом перебора может уйти около 20 минут. Если ещё учесть время на разделку кабеля и снятие изоляции с жил кабеля, то время на подключение может дойти до 1 часа, а то и более. Это при условии, что злоумышленник будет перебирать именно тот кабель, который нужен, а если этот кабель находится в пучке кабелей, то время перебора и подключения увеличится во много раз.

В этой связи, для защиты информации, передаваемой по линиям передачи данных, предлагается рассмотреть возможности нестандартных соединений технических средств канала связи, что позволит минимизировать риски по утечке информации.

Как уже говорилось ранее существуют стандарты по обжиму кабеля. Эти стандарты пришли к нам вместе с технологиями по построению вычислительных сетей. Для полной ясности рассмотрим электрическую схему обжима проводов, соединяющих аппаратуру локально-вычислительной сети рисунок 2. Чаще всего используется подключение по стандарту Т568В. Кабель состоит из витых пар показанных на рисунке 3.

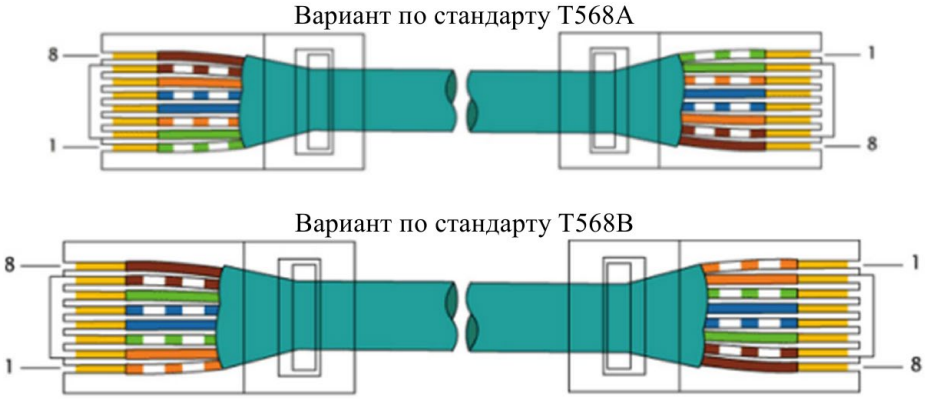


Рис. 2. Цветовая схема обжима сетевого кабеля

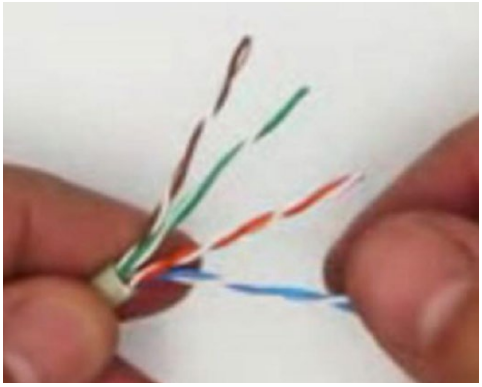


Рис. 3. Витые пары сетевого кабеля

Если посмотреть на попарную схему обжима сетевого кабеля, то можно заметить, что при обжиме кабеля разбивается только 1 пара жил кабеля в коннекторе RJ-45 (рисунок 4). Так как толщина жил, и их изоляция в кабеле витой пары одинаковы, а также нет никакой привязки к цветам кабеля, то эту схему можно использовать в любых цветовых комбинациях. Главное, чтобы разбивка жил в витых парах осуществлялась согласно схеме рисунка 4.

Как раз это свойство обжима сетевого кабеля можно использовать при монтаже оборудования связи. В этом случае нужно создать внутреннюю инструкцию по обжиму сетевого кабеля в которой оговорить свои цветовые схемы обжима кабеля для каждого подразделения или использовать схему защиты, которая является своего рода паролем для подключения оборудования сети. Такая схема безопасности будет переключать стандартное подключение на специальное, разработанное сотрудниками связи для каждого подразделения. Нестандартный способ разбивки пар кабеля витой пары может существенно усложнить процесс снятия информации с канала передачи данных. В качестве дополнительной защиты линии связи можно рассмотреть пространственное распределение жил передачи информации.

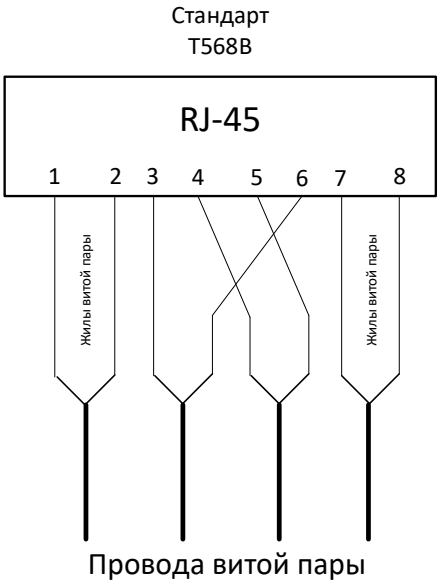


Рис. 4. Схема обжима сетевого кабеля.

Как известно, для организации связи между департаментами используется вычислительная сеть типа Ethernet. В качестве соединительных проводов

используется кабель витой пары, который состоит из 8-ми парных жил (рисунок 3). Для передачи информации в сети типа Ethernet задействованы только 4 жилы, жилы 3 и 6 на приём, жилы 1 и 2 на передачу. Если 8 жил кабеля разделить на 2 части по 4 жилы в каждой (например, жилы, подключенные к 1, 2, 4, 5 контактам в одной части и к 3, 6, 7, 8 контактам в другой части), то пары приёма и передачи окажутся в разных частях, что дает возможность эти части пустить по разным кабелям, которые в свою очередь пустить по разным маршрутам (трассам) прокладки. А если кабели идут еще и в пучке с другими кабелями, то найти необходимый канал практически будет невозможно. Не исключено, что разбить кабель можно по такой схеме, где жилы приёма и передачи тоже могут быть разделены по разным кабелям и маршрутам их прокладки, но этот способ разбивки кабеля требует отдельного исследования.

Для того, чтобы проще было разобраться с маршрутами или трассами прокладки кабеля рассмотрим рисунок 5.

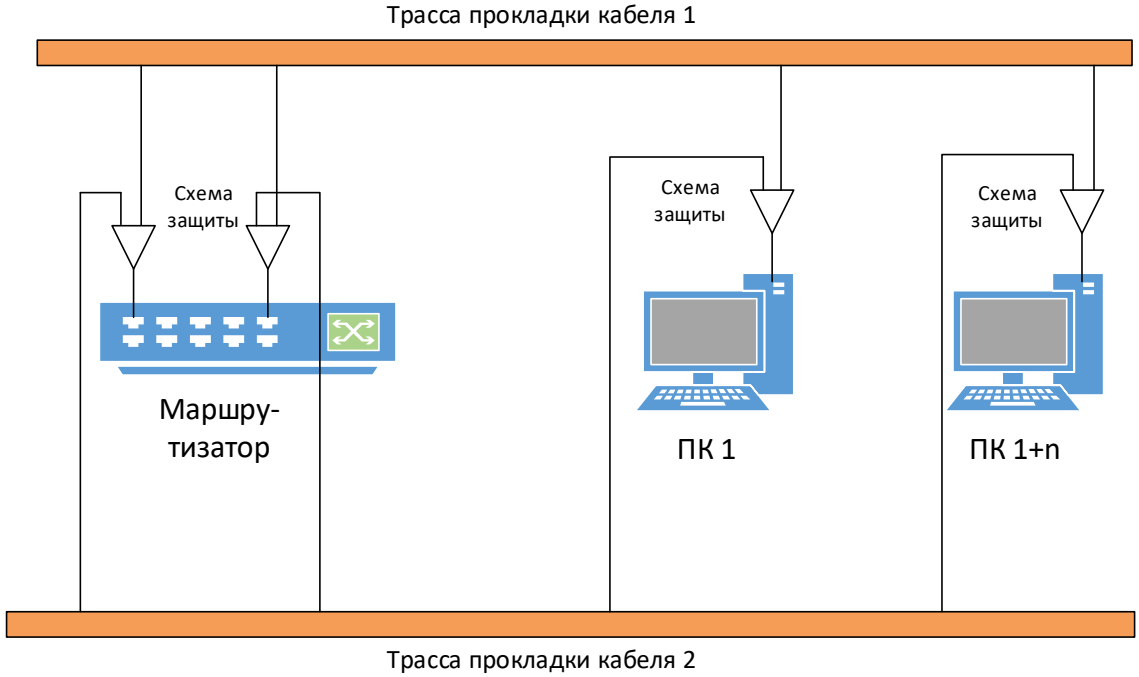


Рис. 5. Схема пространственного разделения канала связи.

На рисунке 5 видно, что каждый компьютер подключается к маршрутизатору двумя кабелями. Каждый кабель подводится к компьютеру разными трассами прокладки. При такой схеме подключения обжим кабелей можно использовать стандартный. Распределение жил будет осуществляться в схеме защиты (рис. 6б), которая может быть разработана непосредственно для каждого подразделения индивидуально и держаться в секрете. Если расстояние между маршрутизатором и компьютерами работниками организации имеет расстояние более 50 метров, то разбивку жил кабеля необходимо производить согласно рисунка 6б что позволит сохранить скорость передачи данных.

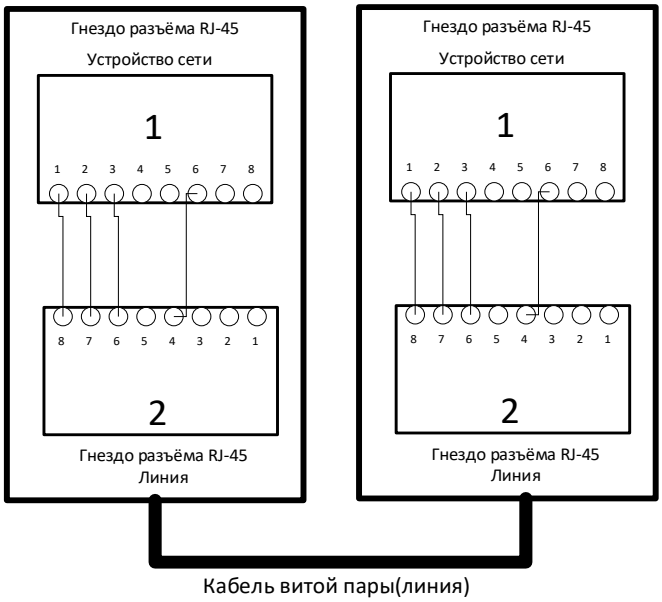


Рис. 6а. Электрическая схема защиты для одного кабеля витой пары

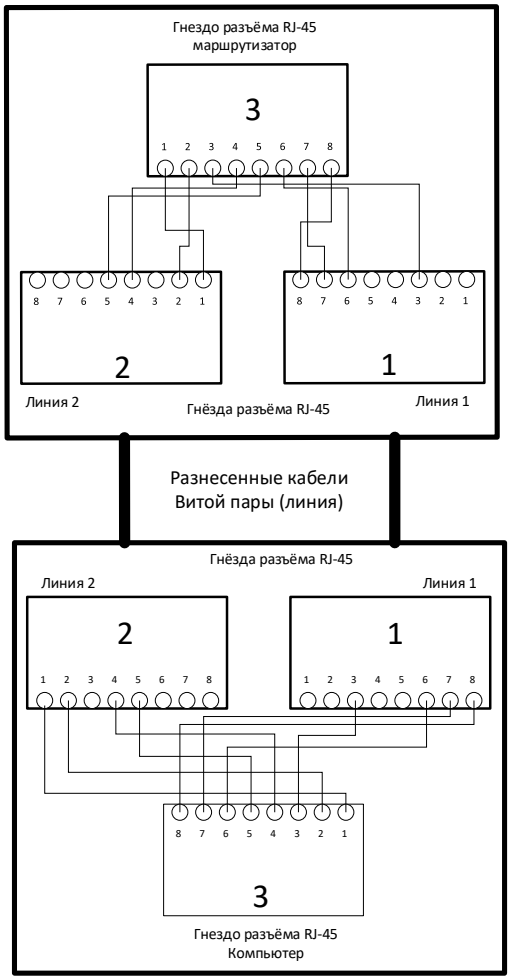


Рис. 6б. Электрическая схема защиты для двух кабелей витой пары

Такое подключение компьютеров существенно усложнит съём информации на физическом уровне. А если учесть, что необходимый кабель будет находиться в пучке кабелей то количество времени на перебор может уйти довольно много.

Таким образом, в результате проведенного исследования рассмотрены некоторые способы съёма информации с линии передачи информации. Все они основываются на физическом подключении к каналу передачи данных. Стандартное подключение технических средств позволяет с лёгкостью производить подключение к каналу передачи информации.

Предложенный автором метод защиты канала связи позволит повысить уровень информационной безопасности, а использование схемы защиты ускорит процесс переключения проводов линии передачи сигналов.

Следующим шагом необходимо изучить возможность разбивки линии связи по жилам кабеля витой пары, что однозначно увеличит число комбинаций подключения инсайдеров к каналу и тем самым усложнит процесс съёма информации. При этом следует отметить, что разбивка жил кабеля может вызвать понижение скорости передачи информации канала связи. И чтобы выявить дополнительные возможности применения схемы защиты необходимо исследовать его внедрение в телефонии.

Литературы

1. Журнал хакер, Витой снифер: как прослушать витую пару, 16. 11. 2007. [В Интернете]. Available: https://xaker.ru/2007/11/16/41146/?aimp. [Дата обращения: 21. 11. 2020].
2. Хорев А.А., Основные задачи защиты информации//Защита информации., С. Петербург: Инсайд, 2010.
3. Хорев А.А., Оценка эффективности защиты средств вычислительной техники от утечки информации по техническим каналам. Часть 2//Специальная техника., Москва, 2007.
4. Хорев А.А., Техническая защита информации: учебное пособие для студентов, Москва: НПЦ Аналитика, 2008.
5. Аверчинков В.И., Методы и средства инженерно-технической защиты информации: учебное пособие., Москва: Издательство Флинта, 2010.
6. «Инструкция по обжиму витой пары» Блог сисадмина, 1. 03. 2013. [В Интернете]. Available: http://blogsisadmina.ru/wp-content/uploads/2013/03/1.jpg. [Дата обращения: 24. 11. 2020.].

SP ЖЕЛІСІ НЕГІЗІНДЕ ҚҰРЫЛҒАН ЖАҢА AL02 БЛОКТЫ ШИФРЛАУ АЛГОРИТМІНІҢ ҚҰРЫЛЫМЫ

Д.С. Дюсенбаев[1,2], Н.А.Капалова[1]., К.Т. Алғазы[1], А.Хомпыш[1,2]
email: dimash_dds@mail.ru
[1]ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты»
Алматы, Қазақстан,
[2]әл-Фараби атындағы ҚазҰУ Алматы, Қазақстан

Аңдатпа. *Мақалада қазіргі ақпараттану кезеңіндегі мәліметтерді құпиялығын қамтамасыз ету үшін қолданылатын симметриялық блокты шифрлардың маңыздылығы, ерекшеліктері және пайдалану аумағы жайлы айтылады. Сонымен қатар жаңадан құрылған AL02 симметриялы блокты шифрлау алгоритмі құрылымы, сондай-ақ раундтық кілттерді жасау механизмі толықтай көрсетілген. Жаңадан құрылған алгоритм бағдарламалық жүзеге асырылды және шифрлау жылдамдығы тексеріліп жылдам жұмыс жасайтындығы анықталды.*

Кіріспе

Криптографиялық қорғау әдістерінің ішінде симметриялық блокты шифрлау алгоритмдері қазіргі уақытта заманауи ақпараттық және телекоммуникациялық жүйелерде ақпаратты өңдеу барысында құпиялылықты қамтамасыз етудің негізгі құралы болып табылады[1]. Тәжірибеде блокты шифрлар олардың жоғары криптоберіктілігіне байланысты, басқа шифрлардан қарағанда жиі қолданылады.

Америка және Ресей шифрлау алгоритмдері дәл осы блоктық шифрлардың класына негізделген. Қазіргі шифрлау алгоритмдері Киркхоффс принципіне негізделеген, оған сәйкес шифрдың құпиялылығы шифрлау алгоритмінің құпиялығымен емес, кілттің құпиялығымен қамтамасыз етілуі керек [2-4]. Сонымен қатар заманауи блокты шифрлау алгоритмдеріне жоғары талаптар (деректерді түрлендіру жылдамдығы, криптоталдау әдістеріне беріктілігі және т.б.) қойылатынын ескерсек, онда блокты шифрлау алгоритміне қойылатын жоғарғы талаптарды қанағаттандыратын отандық ақпаратты криптографиялық қорғау құралдарын құру, оның ішінде шифрлау алгоритмдерін құру бойынша зерттеулер жүргізу өзекті және қажетті болып табылады[5].

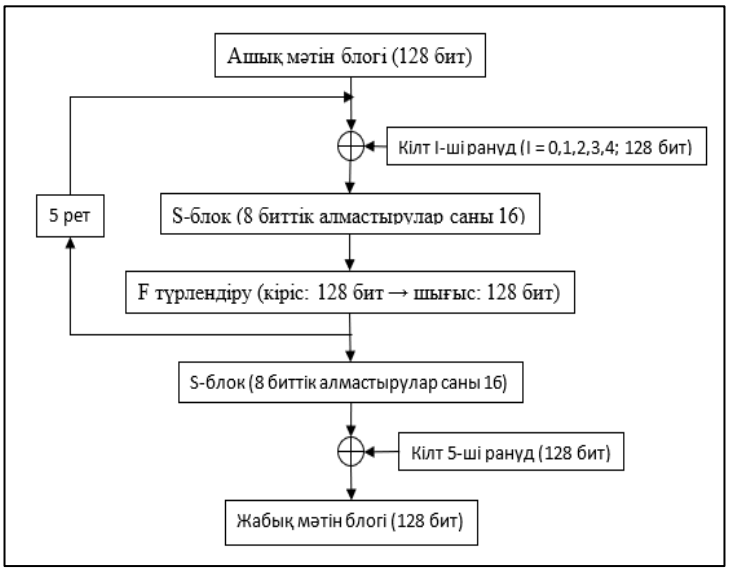
Стандартталған криптоалгоритм қауіпсіздіктің жоғары деңгейін қамтамасыз етуі, қажетті жылдамдыққа ие болуы және әр түрлі есептеу платформаларында тиімді жұмыс істеуі қажет. Қолданыстағы көптеген симметриялы блокты алгоритмдердің құрылымы сызықты және сызықты емес түйіндерден тұратыны белгілі. Нақтылағанда, оның құрамындағы сызықты түрлендірулер – ашықмәтін мәндерін ішінара араластыру үшін, ал сызықты емес түйіндер болса ашық мәтін мен шифр мәтін арасында сызықты емес байланысты күрделендіру үшін қолданады[6]. Сызықты емес түйін мәселесін шешкенде қазіргі таңда S-блок ауыстырулары пайдаланылуда[7-8].

Шифрлау алгоритмін құру барысында заманауи технологияның даму қарқыны мен криптоталдау әдістерінің ерекшеліктері мен мүмкіндіктерін ескере кеткен жөн. Сондай-ақ жұмыс барысында құрылатын симметриялы блокты шифрлау алгоритмдеріне қойылатын негізгі талаптар мен ұсыныстар басшылыққа алу – негізгі ұстаным болды[9]. Жоғарыда көрсетілген мәселелерді ескере отырып жаңа

AL02 симметриялық блокты шифрлау алгоримі және кілт жасау алгоритмі құрылды. Енді сол алгоритмнің құрылымын және әрбір түрлендірулеріне жеке жеке тоқталып өтейік.

AL02 алгоритмінің құрылысы

Ұсынылатын алгоритмнің негізгі параметрлері келесідей: шифрлау блогінің, негізгі және раундтық кілттер ұзындығы 128 бит, раундтың саны – 5. Алгоритмге сызықтық емес функция ретінде қатысатын S-блоктің өлшемінің кіріс және шығыс биттерінің көлемі 8 бит. Қолданылатын негізгі түрлендірулер «модуль 2 бойынша қосу» (⊕ XOR операциясы), S-блок алмастыруы және осы екі түрлендірудің негізінде құрастырылған F түрлендіруінен тұрады. Алгоритмнің жалпылама сұлбасы 1-суретте көрсетілген. Сонымен қатар мақалада шифрлау алгоритмінің раундтық кілттерді жасау алгоритмі де қарастырылған. Бұл жерде де кіріс және шығыс деректер ұзындығы 128 бит. Раундтар саны – 5. Әдеттегідей, негізгі кілтті раундтық кілттің ең алғашқысы, яғни K_0 деп белгілейміз. Ескере кететіні, бастапқы K_0-ді жасауда псевдакездейсоқ әдіс қолданылатын болады. Ал, раундтық кілттерді K_1, K_2, K_3, K_4, K_5 есептеулер барысында аламыз.



1-Сурет. AL02 алгоритмінің жалпылама сұлбасы

Енді шифрлау процесін толығырақ тоқталасақ. 128 бит ұзындықтағы кіріс мәтінді 16 байт түрінде қарастыратын боламыз. Яғни,

$A = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15})$ түрінде жұмыс істейміз.

Кіріс мәтінді байттық жазбасын екі өлшемді квадрат матрица ретінде, яғни 4×4 түріндегі квадрат матрица болады:

$$A = \begin{pmatrix} a_0, a_1, a_2, a_3 \\ a_4, a_5, a_6, a_7 \\ a_8, a_9, a_{10}, a_{11} \\ a_{12}, a_{13}, a_{14}, a_{15} \end{pmatrix} = \begin{pmatrix} a_{0,0}, a_{0,1}, a_{0,2}, a_{0,3} \\ a_{1,0}, a_{1,1}, a_{1,2}, a_{1,3} \\ a_{2,0}, a_{2,1}, a_{2,2}, a_{2,3} \\ a_{3,0}, a_{3,1}, a_{3,2}, a_{3,3} \end{pmatrix} \quad (1)$$

Шифрлау алгоритмінің сұлбасында көрсетілгендей, әр раунд төмендегідей операциялардан тұрады. Оған ашық мәтінге раундтық кілт қосу, S-блок алмастыру және F түрлендіру қатысады. Енді осы түрлендіруге жеке-жеке тоқталайық.

Блокқа жүргізілетін F түрлендіру:

A матрицасының әрбір жолына сәйкес b_i аралық мән болатын төрт санды төмендегідей формула бойынша бірінші элементтің өзін, екінші элементтің S-блоктан өткен мәнін, үшінші мен төртінші элементтердің биттік қосындысының (XOR операциясы) S-блоктағы мәнін алып және олардың биттік қосындыларын есептейміз:

$$b_i = a_{i,0} \oplus S(a_{i,1}) \oplus S(a_{i,2} \oplus a_{i,3}) = a_{4i} \oplus S(a_{4i+1}) \oplus S(a_{4i+2} \oplus a_{4i+3}), i = 0,1,2,3. \quad (2)$$

Алынған b_i төрт мәнді өзара биттік қосып, қосындының S-блоктағы мәнін алып, оны түрлендіруден кейінгі матрицаның бірінші жолының бірінші элементі ретінде қабылдаймыз:

$$c_{0,0} = S(b_0 \oplus b_1 \oplus b_2 \oplus b_3). \quad (3)$$

Түрлендірілген матрицаның қалған элементерін, түрлендірілген матрицаның сол жолдағы алдыңғы элементімен түрлендіруден өтпеген матрицаның сол орындағы элементін өзара биттік қосу оперциясын қолданып, қосындыдан S-блоктің мәнін аламыз:

$$c_{i,j+1} = S(c_{i,j} \oplus a_{i,j+1}), i = 0,1,2,3; j = 0,1,2 \quad (4)$$

(4) формуладағы келесі жолдарының бірінші элементін, яғни $c_{i,0}$ алу үшін сол жолдың алдындағы жолдың соңғы элементімен түрлендіруден өтпеген матрицаның сол орындағы элементін өзара биттік қосқандығы қосындының S-блоктағы мәнін аламыз:

$$c_{i,0} = S(c_{i-1,3} \oplus a_{i,0}), i = 1,2,3 \quad (5)$$

Осы (2)-(5) формулалар арқылы түрлендіруден өткен матрицаның барлық элементтерін есептеп аламыз.

Осы аталған үш түрлендіруді бес рет қайталап, нәтижеге ақырғы рет S-блок алмастыру мен соңғы раундтық кілтті қосу операциясын орындап, шифрланған мәтін блогін аламыз.

Дешифрлау процесі: әдеттегідей шифрмәтіннен ретімен 16 байттан кесіп алынып, блок ретінде блокті дешифрлаудағы жүргіземіз. Қарастыратын 16 байтты 16 көлемдегі вектор немесе 4×4 түріндегі квадрат матрица бойынша қарастырамыз:

$$\mathrm{C} = (\mathrm{c}_0, \mathrm{c}_1, \mathrm{c}_2, \mathrm{c}_3, \mathrm{c}_4, \mathrm{c}_5, \mathrm{c}_6, \mathrm{c}_7, \mathrm{c}_8, \mathrm{c}_9, \mathrm{c}_{10}, \mathrm{c}_{11}, \mathrm{c}_{12}, \mathrm{c}_{13}, \mathrm{c}_{14}, \mathrm{c}_{15})$$

немесе

$$C = \begin{pmatrix} c_0, c_1, c_2, c_3 \\ c_4, c_5, c_6, c_7 \\ c_8, c_9, c_{10}, c_{11} \\ c_{12}, c_{13}, c_{14}, c_{15} \end{pmatrix} = \begin{pmatrix} c_{0,0}, c_{0,1}, c_{0,2}, c_{0,3} \\ c_{1,0}, c_{1,1}, c_{1,2}, c_{1,3} \\ c_{2,0}, c_{2,1}, c_{2,2}, c_{2,3} \\ c_{3,0}, c_{3,1}, c_{3,2}, c_{3,3} \end{pmatrix} \quad (6)$$

Раундтық кілттер қолданылуы раунд реті бойынша кері тәртіппен орындалады. S-блок алмастыру кестесіне кері S-блок алмастыру түрлендіруі (S^{-1}), ал F түрлендіруіне кері F^{-1} түрлендіруі қолданылады. Енді осы F^{-1} кері түрлендіруіне жекелей тоқталсақ.

F^{-1} кері түрлендіруі: Берілген матрицаға кері түрлендіруді қолдану арқылы жаңа матрица аламыз. Кері түрлендіруден кейінгі матрицаның элементтерін төмендегідей анықтаймыз. Кері түрлендіруде есептеуді бірінші жолдың екінші элементінен бастап жүргіземіз. Сондықтан, әрбір жол үшін берілген матрицаның элементінен кері S-блоктың мәнін алып, оны сол жолдағы алдыңғы элементпен өзара биттік қосып, кері түрлендіруден кейінгі сол орындағы элементті аламыз:

$$a_{i,j} = S^{-1}(c_{i,j}) \oplus c_{i,j-1}, i = 0,1,2,3; j = 1,2,3 \quad (7)$$

Екінші жолдан бастап әл жолдағы бірінші элементті есептеуде кері түрлендіруге дейінгі сол орындағы матрицаның элементінен кері S-блоктың мәнін алып және алдыңғы жолдың соңғы элементін биттік қосу арқылы аламыз:

$$a_{i,0} = S^{-1}(c_{i0}) \oplus c_{i-1,3}, i = 1,2,3 \quad (8)$$

(7)-(8) формулалары арқылы F^{-1} кері түрлендірудегі матрицаның бірінші жолдағы бірінші элементінен басқа матрицаның барлық элементтері аламыз. Бірінші жолдың бірінші элементін алу үшін келесі қадамдарды орындаймыз. Екінші жолдан бастап аралық үш мәнді (2-ші, 3-ші, 4-ші аралық мәндер немесе b_i-лер) келесі жолмен, бірінші элементтің өзін, екінші элементтің S-блогінің мәнін, үшінші мен төртінші элементердің биттік қосындысының S-блоктағы мәнін алып және олардың биттік қосындыларын есептейміз:

$$b_i = a_{i0} \oplus S(a_{i1}) \oplus S(a_{i2} \oplus a_{i3}), i = 1,2,3 \quad (9)$$

Түрлендірудің кірісі ретінде алынған матрицаның бірінші жолы мен бірінші бағанының қиылысындағы элементтінен (бірінші жолдың бірінші элементінен) кері S-блок мәнін алып және аралық үш мәндердің барлығының биттік қосындысын есептеу арқылы бірінші аралық төртінші мәнді b_0 –ді (10) формула арқылы табамыз.

$$b_0 = S^{-1}(c_{0,0}) \oplus b_1 \oplus b_2 \oplus b_3 \quad (10)$$

Кері түрлендірілген матрицаның бірінші жолының бірінші элементі $a_{0,0}$-ді табу үшін осы бірінші аралық мәнді, бірінші жолдың екінші элементін кері S-блоктан өткізіп, екінші мен үшінші элементердің биттік қосындысын кері S-блоктан өткізіп және олардың барлығының биттік қосындысын (11) формуламен есептейміз:

$$a_{0,0} = b_0 \oplus S^{-1}(a_{0,1}) \oplus S^{-1}(a_{0,2} \oplus a_{0,3}) \quad (11)$$

Дешифрлауды жүргізгенде 1-суреттегі бүкіл процесті кері қарай, яғни соңынан басына дейін жүргізетін боламыз. Раундтарға қатысты операцияларды раунд санына байланысты бес рет қайталау арқылы жүргізіп, ақырында ашық блокқа қол жеткіземіз.

Кілтті және раундтық кілттерді алу алгоритмдері

Кілт жасаудағы бастапқы мән уақыт (күні, айы, жылы, сағат, минут, секунд) пен тышқанның орынына (жазықтықтағы координатасы) қатысты таңдалып есептеліп, алынған мәнге кілт жасау түрлендіруі жүргізіліп, негізгі кілт (құпия кілт) алынады.

Кілтке осы түрлендірудің әрбір қайталауына қатысты раундтық кілттер алынады. Алынған уақыт мәні координатаның абсисасының мәніне көбейтіліп, ординатасының мәніне қосылады. Осы алынған мән кілт жасау түрлендіруінің кірісі ретінде таңдалады.

Кілт жасау түрлендіруі: Түрлендірудің кірісі мен шығысы 128 биттен тұрады, сондықтан кірісінің ұзындығы 128-ден кем болса, онда аяғы нөлдермен толықтырылады. Ал егер артық болса, алғашқы қажетті ұзындық таңдалады. 16 байтты кірісі 16 көлемдегі вектор немесе 4×4 түріндегі квадрат матрица бойынша енгізіледі:

$$A = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15})$$

немесе

$$A = \begin{pmatrix} a_0\ , a_1\ , a_2\ , a_3 \\ a_4\ , a_5\ , a_6\ , a_7 \\ a_8\ , a_9\ , a_{10}, a_{11} \\ a_{12}, a_{13}, a_{14}, a_{15} \end{pmatrix} = \begin{pmatrix} a_{0,0}, a_{0,1}, a_{0,2}, a_{0,3} \\ a_{1,0}, a_{1,1}, a_{1,2}, a_{1,3} \\ a_{2,0}, a_{2,1}, a_{2,2}, a_{2,3} \\ a_{3,0}, a_{3,1}, a_{3,2}, a_{3,3} \end{pmatrix}$$

Матрицаның бірінші жолдың бірінші элементінің өзін, екінші элементтің S-блогінің мәнін, үшінші мен төртінші элементерінің биттік қосындысының S-блоктағы мәнін алып, осылардың биттік қосындыларын S-блоктан өткендегі мәні аралық мән b_0 алынады:

$$b_0 = S\left(a_{0,0} \oplus S(a_{0,1}) \oplus S(a_{0,2} \oplus a_{0,3})\right) = S(a_0 \oplus S(a_1) \oplus S(a_2 \oplus a_3)) \qquad (12)$$

Алынған аралық мәнді екінші жолдың бірінші элементінің өзіне, екінші элементінің S-блогінің мәніне, үшінші мен төртінші элементтерінің биттік қосындысының S-блоктағы мәнін алып және олардың биттік қосындыларын есептеп, оны S-блоктан өткіземіз, осылай екінші аралық мәнді аламыз:

$$b_1 = S(b_0 \oplus a_{0,0} \oplus S(a_{0,1}) \oplus S(a_{0,2} \oplus a_{0,3})) = S(b_0 \oplus a_4 \oplus S(a_5) \oplus S(a_6 \oplus a_7)) \quad (13)$$

Дәл осылай алынған мәнді үшінші және төртінші жолдар үшін де қайталаймыз:

$$b_i = S(b_{i-1} \oplus a_{i,0} \oplus S(a_{i,1}) \oplus S(a_{i,2} \oplus a_{i,3})) = S(b_{i-1} \oplus a_{4i} \oplus S(a_{4i+1}) \oplus S\ (a_{4i+2} \oplus a_{4i+3})), \quad i=2,3. \qquad (14)$$

Егер тізбекті 128 бит арқылы өрнектеген болсақ, онда солға циклдік жылжыту арқылы алынған тізбекті ретімен 8 бит бойынша S-блоктан өткізіп, түрлендірілген жаңа 128 биттік тізбек аламыз.

Осы айтылған тірлендіруді берілген байттық матрицада келесідей орындаймыз:

$$\begin{pmatrix} a_{0,0}, a_{0,1}, a_{0,2}, a_{0,3} \\ a_{1,0}, a_{1,1}, a_{1,2}, a_{1,3} \\ a_{2,0}, a_{2,1}, a_{2,2}, a_{2,3} \\ a_{3,0}, a_{3,1}, a_{3,2}, a_{3,3} \end{pmatrix} \xrightarrow{\text{солға 3 қадамға циклдік жылжыту және S−блоктан өткізу}} \begin{pmatrix} a'_{0,0}, a'_{0,1}, a'_{0,2}, a'_{0,3} \\ a'_{1,0}, a'_{1,1}, a'_{1,2}, a'_{1,3} \\ a'_{2,0}, a'_{2,1}, a'_{2,2}, a'_{2,3} \\ a'_{3,0}, a'_{3,1}, a'_{3,2}, a'_{3,3} \end{pmatrix}$$

Мұндағы $a'_{i,j}$ матрицаның элементтері төмендегідей өрнектеледі:

$$a'_{i,j} = S\Big(\big((a_{i,j} \times 8)mod256\big) \oplus \big((a_{i,(j+1)mod4} \times 8)mod256\big) \oplus \big((a_{i,(j+1)mod4} \times 8)mod257\big)\Big), i = 0,1,2,3; j = 0,1,2. \quad (15)$$

$$a'_{i,3} = S\Big(\big((a_{i,3} \times 8)mod256\big) \oplus \big((a_{(i+1)mod4,0} \times 8)mod256\big) \oplus \big((a_{(i+1)mod4,0} \times 8)mod257\big)\Big), i = 0,1,2,3. \quad (16)$$

Кілт жасау түрлендіруден кейінгі матрицаның бірінші жолының бірінші элементі ретінде b_3 пен $a'_{0,0}$ мәндерін биттік қосындысының S-блоктан өткен мәнін қабылдаймыз:

$$c_{0,0} = S(b_3 \oplus a'_{0,0}) \quad (17)$$

Түрлендірілген матрицаның қалған элементерін, түрлендірілген матрицаның сол жолдағы алдыңғы элементімен түрлендіруден өтпеген матрицаның сол орындағы элементін өзара биттік қосып, қосындыдан S-блоктің мәні алынады:

$$c_{i,j+1} = S\big(c_{i,j} \oplus a_{i,j+1}\big), i = 0,1,2,3; j = 0,1,2 \quad (18)$$

Жолдың бірінші элементтің алу үшін алдыңғы жолдың соңғы элементімен түрлендіруден өтпеген матрицаның сол орындағы элементін өзара биттік қосқандығы қосындының S-блоктағы мәнін аламыз:

$$c_{i,0} = S\big(c_{i-1,3} \oplus a_{i,0}\big), i = 1,2,3 \quad (19)$$

Осындай түрлендіруден өткен матрицаның барлық элементтерін есептеп аламыз. Кілт жасау алгоритмі үшін кілт жасау түрлендіруі бес рет композициялық түрде қайталанады. Раундтық кілттерді жасауда әрбір кілт жасау түрлендіруінен

өткен қадамдағы матрица раундтық кілт ретінде қабылданады. Біздің жағдайда рауд саны 5 болғандықтан, түрлендіру 5 рет орындалады.

Көрсетілген алгоритм бойынша мысал ретінде төмендегідей негізгі кілттер мен раундтық кілттерді көрсете кетейік.

Уақыт пен координатаға сәйкес алынған негізгі кілттер:
20.06.2021 17:48:17 - 5249284099403484404 - 48d93413960d0cf4
K=5a9c49f22488dd6619c3d95a0ad75471
20.06.2021 17:49:14 - 5249284099970006938 - 48d93413b7d17f9a
K=304aa5dbf5fc5abb54e19a772d06c859
20.06.2021 17:50:18 - 5249284100609752684 - 48d93413ddf33e6c
K=c8446cd4286bea53535c451936612fea
Төменде раундтық кілттер:
K_1=b565075cc81bf687d2f654a03e4c3ff7
K_2=af0147a13c8e2b7046d6d91703498aa4
K_3=e9e11bc4dbb5ba89960a4dda94b1c00b
K_4=5da65f498361d84471320d93788ae99f
K_5=286869763b81ffdcdf86eb5336feb7fa

AL02 алгоритмінің бағдарламалық іске асырылуы

Көрсетілген шифрлау алгоритмі бағдарламалық іске асыру жағынан жұмыстар жүргізілді, бағдарламасы құрылып, нәтижелері шифрлау алгоритмінің негізгі сипаттамалары жан-жақты зерделенді. Бағдарламаның көмегімен алгоритмнің жұмыс істеу өнімділігі қарастырылды. Жекелей алғанда, 326 Мб видео файлды 13 және 130 Мб pdf форматтағы файлды 6,5 секундта шифрлады. Кері шифрауға да тура осындай уақыт жұмсалады.

Қорытынды

Ұсынылып отырған мақалада блоктық шифлау алгоритмдерінің негізгі талаптарын қанағаттандыратын жаңа AL02 симметриялық блокты шифрлау алгоритмі құрылды. Алгоритмнің құрамындағы сызықты және сызықты емес түрлендіру әдістеріне жеке жеке тоқталынып, алгоритмнің жұмыс құрылымы түсіндірілді.

Сонымен қатар құрылған алгоритмде қолданылатын раундық кілттерді алуға арналған алгоримінің жұмыс істеу процессі көрсетілген. Құрылған алгоритмнің жылдамдығын тексеру үшін бағдарламасы C# тілінде жасалынып. Бағдарлама көмегімен әр түрлі өлшемдегі, кеңейтуі әртүрлі файлдарды алып шифрлап, шифрлау жылдамдығы жылдам жасайтындығы анықталды. Алдағы жұмыстарда алгоритмнің криптоберіктілігін анықтау үшін әртүрлі криптоәдістер арқылы талдаулар жүргізілетін болады.

Қолданылған әдебиеттер тізімі

1. В. Столлингс Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. – М.:Вильямс, 2001.

2. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.

3. Зензин О.С., Иванов М.А. Стандарт криптографической защиты - AES. Конечные поля. – М.: КУДИЦ-ОБРАЗ, 2002. – 176 с.

4. Варфоломеев А.А., Варфоломеев А.А., Жуков А.Е. Блочные криптосистемы. Основные свойства и методы анализа стойкости. – М.: МИФИ, 1998. – 247 с.

5. Kapalova N., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform. // Cogent engineering. – 2020. – Vol.7(178829). – ISSN 2331-1916. – P. 1-12.

6. Д.С. Дюсенбаев, К.Т. Алғазы, Қ.С. Сақан. Симметриялы шифрларда қолданылатын сызықты емес түйіндерді зерттеу // Матер. межд. науч.-практ. конф. «Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020». – Алматы, 2020. – Б.34-39.

7. А.А. Кузнецов, И.Н. Белозерцев, А.В. Андрушкевич. Анализ и сравнительные исследования нелинейных узлов замены современных блочных симметричных шифров, Прикладная радиоэлектроника, том 14, №4, 2015, с.343-350.

8. L.O. Connor, An analysis of a class of algorithms for S-box construction. Journal of Cryptology,7(1):133-151,1994.

9. Biyashev R. G., Smolartz A., Algazy K.T., Khompysh A. Encryption algorithm ‘’Qamal NPNS’’ based on a nonpositional polynomial notation // Journal of Mathematics, Mechanics and Computer Science, «Хабаршы» ҚазҰУ. – Алматы, 2020. –Vol. №1 (105). – P. 198-207.

ХЕШТЕУ АЛГОРИТМДЕРІН ЖАСАУДАҒЫ БЛОКТЫ ШИФРЛАУ АЛГОРИТМДЕРІН ҚОЛДАНУ ЕРЕКШЕЛІКТЕРІ

С.Нысанбаева, Қ. Сақан
e-mail: sultasha1@mail.ru, kairat_sks@mail.ru
Ақпараттық және есептеуіш технологиялар институты ҚР БҒМ ҒК, Қазақстан

Аңдатпа. *Мақалада қазіргі ақпараттану кезеңіндегі мәліметтерді хештеудің маңыздылығы, ерекшеліктері және пайдалану аумағы жайлы айтылады. Хештеу алгоритмдерінің жасау процесінде симметриялық блоктық шифрлеу алгоритмін негізге алу, пайдалану мүмкіндіктері, құрылымдық қасиеттері, ерекшеліктері, сондай-ақ олардың осал және басым тұстары көрсетілген. Жұмыс нәтижесі арқылы шифрлау алгоритмнің пайдалануына қойылатын талаптер мен ұсыныстар баяндалған.*

Кіріспе

Қазіргі таңда сандық технологияның шарықтап даму кезеңіндегі заманауи қауіпсіз хэш алгоритмдері көптеген компьютерлік жүйелердегі ақпарат пен деректердің тұтастығы мен жарияланбауы үшін өте маңызды екендігі белгілі. Ақпараттық қауіпсіздіктің бұл талаптарын қамтамасыз ету мақсатында «хештеу» термині, осыған сәйкес хештеу алгоритмдері қолданылады, яғни ол ассоциативті массивтерді құру кезінде, деректер қорында көшірмелерді іздеу кезінде, деректер қоры үшін бірегей идентификаторларды құру кезінде, деректерді сақтау және/немесе беру кезінде туындайтын кездейсоқ немесе қасақана жасалынған өзгертулердің бар-жоғын, қауіпсіздік жүйелеріндегі парольдерді хеш ретінде сақтаған кезде, электрондық құжаттарға электрондық цифрлық қолтаңбаны жасау кезінде пайдаланылады.

Хештеу (hash - араластыру, араластыру, араластыру) – бұл кіріс хабарламалар массивін тұрақты ұзындықтағы мәліметке дейін түрлендіру (хеш, хеш-код немесе дайджест деп аталады). Хештің ерекшелігі – ұзындығы бастапқы берілген дерекке қарағанда едәуір қысқа болып келеді және бастапқы дерек пен оның хеші арасында жоғарғы ықтималдықпен екеуара өзара сәйкестіктің болуы. Өзара сәйкестікті қамтамасыз ету мақсатында қолданылатын математикалық түрлендіру хеш-функциялар (криптографиялық хеш-функциялар) көмегімен жүргізіледі. Уақыт өте келе ең кеңінен қолданылатын криптографиялық хеш функциялардың өздерінен айтарлықтай кемшіліктері анықталуда [1, 2].

Ақпаратты хештеу функцияларына қойылатын негізгі талаптарды айқындау

Жалпы жағдайда, бастапқы деректер мен оның хеші арасында өзара бірге-бір сәйкестік бола бермейді, яғни коллизиялардың (соқтығысулардың) бар болуы. Бірдей хеш беретін әртүрлі деректер жиынтығы бар болуы мүмкін, осындай сәйкестіктердің бар болуы ықтималдығын азайту – хеш-функцияға қойылатын негізгі талап болып саналады. Сондықтан, түпнұсқалықты қамтамасыз ету үшін хештеу алгоритмін қиындату немесе барынша жақсару заманауи хеш-алгортмдер жасауға негіз болып отыр. Осыған сәйкес жасалынатын криптографиялық хеш-функция төмендегідей негізгі сипаттамаларға ие болуы міндетті:

- кез-келген ұзындықтағы деректерді белгіленген ұзындықтағы хешке түрлендіру орындай алуы керек;
- үлкен есептеу ресурстарын қажет етпеуі керек және жылдам орындалуы керек;
- хеш-функцияның криптографиялық тұрақтылығын зерттеу үшін оның алгоритмі ашық болуы керек;
- хештеу процесі (түрлендіруі) бір жақты болуы керек, яғни хеш бойынша бастапқы деректерді анықтауға математикалық мүмкіндік болмауы керек;
- ол коллизияларға «қарсы» болуы керек, яғни әртүрлі деректерге сәйкес бірдей хеш табу есептеулер күрделілігі жағынан мүмкін болмау керек;
- деректердің шамалы өзгеруіне сәйкес хеш айтарлықтай өзгеруі керек (лавиндік эффект).

Бұдан әрі, осы сипаттамалар негізінде жасалған криптографиялық хэш функциясы криптоталдау шабуылдардың барлық белгілі түрлеріне төтеп бере алуы керек. Теориялық криптографияда хеш функциясының қауіпсіздік деңгейі келесі қасиеттерді қолдана отырып анықталады:

- соқтығысуға (коллизияға) төзімділік,
- алғашқы бейнеге қарсылық (прообразға төзімділік),
- екінші алғашқы бейнеге қарсылық (екінші прообразға төзімділік).

Хеш функциялары жұмысы істеу тәртібін қарастырғанда, M хабарламаны хештеудің ең ыңғайлы әдісі: алдымен оны бірнеше бірдей бөліктерге (блоктарға) бөліп, содан кейін осы бөліктерді итеративті және жүйелі түрде өңдеу екені белгілі. Бүгінгі таңда параллель процессорлардың көмегімен бұл итеративті түрде тізбектеп хеш алу хэш әдісі тіпті кеңінен қолданылады.

Жалпы жағдайда, кез-келген хеш-функция болмаса хештеу алгоритмі екі компоненттен тұрады: f сығу функциясы және H конструкциясы. Сығу функциясы – бұл бекітілмеген үлкен өлшемдегі кірісті бекітілген аз өлшемдегі шығысқа сәйкес келтіретін $f : \{1, 0\}^m \rightarrow \{1, 0\}^n$ функция, мұндағы $m > n$. Конструкция – бұл M хабарламасын $M_1, M_2, \ldots, M_t$ бөлліктерге бөліп, оларды өңдеу үшін f қысу функциясын бірнеше рет жұмыс жасату (шақыру) тәсілі.

Хештеу алгоритмдерін жасаудағы блокты шифрлау алгоритмдерін қолдану жолдары

Хештеу алгоритмдерінде f сығу функциясы ретінде қандай да бір симметриялы блоктық шифрлау алгоритмін қолдануға болады. Мысалы, Ресейде ГОСТ Р 34.11-94 хештеу стандарты ресейлік ГОСТ 28147—89 криптографиялық шифрлау стандарты негізінде жасалған. Ал, қазіргі ГОСТ Р 34.10-12 («Стрибог» хештеу алгоритмі) стандарты да XSPL шифры негізіндегі ГОСТ Р 34.11-2012 стандартындағы блок шифры алынды. Көбінесе, шифрлау алгоритмі жолымен хештеу алгоритмдерінде белгілі Меркл-Дамгард конструкциясы пайдаланады. Коллизияға төзімділікті жоғарлатып, хеш функция қауіпсіздігін қамтамасыз ету мақсатында Меркл-Дамгард конструкциясының жаңа модификациялары бар. Соның бірі – Стефан Лакс ұсынған wide-pipe конструкциясы [3]. Бұл әдіс ұзындықты ұзарту шабуылына (“length extension” attack) ұшыраған Меркл-Дамгардтағы кемшіліктерді жою үшін ұсынылды. wide-pipe конструкциясы хешті есептеу үшін екі f және g қысу функциясынан тұрады. Еркін ұзындықтағы хабарлама толтырылғаннан кейін f функциясы кезекті b-биттік хабарлама бөлігін итеративті өңдеу үшін және нәтижесінде w-биттік аралық хештер алу үшін қолданылады. Хабарлама толықтай өңдегеннен кейін, g функциясы w-биттік соңғы аралық хешті қабылдап, одан n

биттік ақырғы хешті алу үшін қолданады: $f: \{1, 0\}^w \times \{1, 0\}^b \rightarrow \{1, 0\}^w$, $g: \{1, 0\}^w \rightarrow \{1, 0\}^w$, мұнда $w \geq n$.

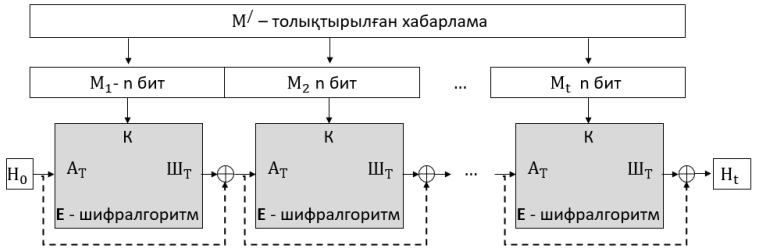
Қауіпсіздікті қамтамасыз ету үшін кілт ретінде берілген итерацияда хэштеуге арналған хабарламалар бөлігін, ал сығу функциясының алдыңғы шақырылымдағы нәтижесі кіріс ретінде, болмаса, кірістерін керісінше еті те алуға болады. Содан кейін соңғы итерацияның нәтижесі алгоритмнің шығысы, яғни ақырғы нәтижесі хеш болып есептелінеді [4]. Бұл жағдайда хеш фукциядағы сығу функциясы рөлін шифрлау алгоритмі орындайды. хеш функциясының қауіпсіздігі қолданылатын алгоритмнің қауіпсіздігіне негізделген. Осы процестің жалпы нұсқасын төмендегі сурет-1-ден көруге болады.

Сурет-1 – Блоктық шифрлау алгоритмі негізіндегі хеш функциясының жалпылама сұлбасы

Меркл-Дамгард конструкциясын негізге алып, ондағы f сығу функциясы ретінде E блоктық шифрын қолдану – аталған конструкцияның әрі қарай жетілдіруге келді [3]. Себебі, қолданылатын E блоктық шифрына біржақтылықты (односторонность) қамтамасыз ету керек. Біржақты функция – кез-келген кіріс мәні үшін оңай есептелетін математикалық функция, бірақ кері қарай, яғни, алынған мән арқылы функцияның аргументін табу қиын. Осыған сәйкес Пренель, Говертс және Вандевалль (Preneel, Govaerts and Vandewalle) $E: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ блоктық шифры негізінде жасалатын f хеш-функцияның 64 түрлі әдісін қарастырды [5]. Кейде бұл осы 64 схеманың қауіпсіздігін зерттеу үшін шабуылдарға негізделген талдау әдістерін қарастырған осы авторлардың аты-жөндерімен байланыстырып, PGV схемалары деп атаған. Алдымен 12 PGV схеманың қауіпсіз екендігі, яғни коллизияларға төзімді екендігі дәлелденді, кейін тағы 8-і қосылды [6].

Бірқатар схемаларда аралық хеш мәні мәтін блогымен модуль 2 бойынша қосылу операциясы пайдаланылады. Бұл жағдайда шифрдағы кілт пен блоктың ұзындықтары бірдей болады. Шифрдегі кілт пен блоктың ұзындықтары сәйкес келген жағдайда тәжірибеде кең таралған ең қарапайым схема жайлы тоқталайық. Ескере кететіні, осы схемаларда бастапқы $H_0 = IV$ ретінде қарастырылады, мұндағы: IV – бастапқы вектор, ол көп жағдайларда нөлдік вектор деп алу енгізілген.

Дэвис-Мейер схемасы мына тәртіпте жұмыс істейді: $H_i = f(H_{i-1}, M_i) \oplus H_{i-1}$, $i = 1,2, \dots, t$, мұнда қысу функциясы ретінде E шифрлау алгоритмі, K кілт ретінде кезекті M_i хабарлама бөлігі, A_T ашық мәтін ретінде алдыңғы итерация мәні H_{i-1}, ал $Ш_T$ шығыс ретінде H_i аралық хеш мәні болады. Е шифрлау алгоритмі нәтижесі H_{i-1} – алдыңғы итерация мәнімен XOR операциясы арқылы біріктіріліп, соңында жаңа H_i – аралық хеш мәнді алатын боламыз. Бұл схема негізінен Рабин схемасын қайталайды, тек «Орта ақпарат» («Сведения в середину») шабуылынан қорғау үшін пайдаланады, схеманың графиктік бейнесі сурет-2 көрсетілген.



Сурет-2 - Дэвис-Мейер схемасы жұмыс тәртібі

Хештеу алгоритмдерін жасаудағы блокты шифрлау алгоритмдерін қолдану ерекшеліктері мен талаптары

f сығу функциясы негізін блоктық шифрлау алгоритмі ретінде қарастырғанда, хеш функцияның криптографиялық қауіпсіздігі қолданылатын шифрлау алгоритмнің қауіпсіздігіне негізделген болады [4]. Сондықтан, хештеу алгоритміндегі f сығу функциясы ретінде шифрлау алгоритмін пайдаланғанда, шифрлау алгоритмдерде төмендегідей талаптарды ескеру керек:

- күштік шабуылдарға криптографиялық беріктілік (аралық және қосымша нәтижелерді сақтау үшін және уақытша өлшем бойынша талап етілетін жадтың қажетті ең аз көлемі бойынша);
- ашық, жабық және шифрлау кілті (біздің жағдайда алдыңғы итерациядағы аралық хеш мән, кілт ретінде алынатын хабарлама бөлігі және осы итерациядан алынған аралық хеш мән, сәйкесінше) арасындағы өзара байланысты сипаттайтын алгебралық (логикалық) теңдеулер жүйесін табу және шешу тәсілдерінің болмауы;
- алгоритмге белгілі аналитикалық криптошабуылдарды іске асырудың практикалық қол жетімсіздігі немесе олардың жоғары есептеу күрделілігі;
- заманауи инновациялық-технологиялық дамудың қарқынын ескере отырып, алгоритмнің оңтайлы «криптографиялық беріктілік қорының» болуы;
- алгоритмнің жеңілдетілген нұсқасының криптографиялық беріктілігі, ондағы кейбір опцияның операцияларын қарапайым нұсқалармен алмастырыла алуы немесе жеңілдетіле алуы;
- шифрдың шығыс мәтінінің (аралық хеш мәнінің) статистикалық көрсеткіштері шынайы кездейсоқ тізбектің көрсеткіштеріне ұмтылуы тиіс.

Сонымен қатар, хеш алгоритмдері үшін пайдаланатын блоктық симметриялы алгоритмдерді жобалау мен талдау кезеңінде төмендегідей тәсілдерді ескеру ұсынылады [7]:

- «консервативті дизайн», яғни тек бірнеше рет тексерілген, яғни сенімді құрылымдарды, криптографиялық примитивтер мен кепілдендірілген қауіпсіздік әдістері пайдалану керек;
- барлық белгілі криптоталдаулық шабуылдарға беріктілік;
- алгоритмді жобалаудың қолжетімді және қарапайым құрылымы мен қағидаттары;
- алгоритмнің оңтайлы «төзімділік қорын» қалыптастыру, есептеу техникасы құралдарының ықтимал криптоталдаулық шабуылдарының пайда болуын ескеріп, алгоритмді одан әрі қауіпсіз пайдалану мүмкіндігі болуы;
- алгоритмнің барлық ықтимал осалдықтарынан қорғауды қамтамасыз ету;
- үздік әлемдік көрсеткіштерге жақын жоғары өнімділікті және беріктілікті қамтамасыз ету.

Қорытынды

Блоктық шифлау алгоритмдері негізінде хеш алгоритмдерін жасау барысында оған қойылатын алғышарттар, талаптар мен ұсыныстар нақтыланды. Соның негізінде алдағы уақытта біржақтылықты қамтамасыз ете алатын блоктық шифрлау алгоритмі жасалынып және Меркл-Дамгард конструкциясының wide-pipe модификациясын пайдаланып, параллельдік есептеуіштерде жұмыс істеуге мүмкіндік беретін хештеу конструкциясы құрылуда. Негізгі басымдық хеш функцияның негізгі үш қасиетіне ие болатын, сондай-ақ жұмыс өнімділігі бойынша заманауи әлемдік көрсеткіштерге сай хештеу алгоритмі жасалуда.

Алғыс

Ғылыми зерттеу жұмысы Ақпараттық және есептеуіш технологиялар институтында орындалып жатқан «Электрондық цифрлы қолтаңба үшін еркін ұзындықтағы хэштеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау» бағдарламалық-нысаналы қаржыландыру жобасы аясында орындалды.

Әдебиеттер

1. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, "Finding collisions in the full SHA-1," in Proceeding of CRYPTO'05, vol. 3621, 2005, pp. 17-36.

2. Marc Bevand, "MD5 Chosen-prefix collisions on GPUs," in Black Hat USA, Las Vegas, 2009.

3. Hirose, S. Some plausible constructions of double-blocklength hash functions. Fast Software Encryption, LNCS, Springer-Verlag, 2006, 4047, 210-225

4. Авезова Я.Э. Современные подходы к построению хеш-функций на примере финалистов конкурса SHA-3 // Вопросы кибербезопасности. 2015. №3 (11). URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-postroeniyu-hesh-funktsiy-na-primere-finalistov-konkursa-sha-3 (дата обращения: 10.08.2021).

5. Thomas Ristenpart and Thomas Shrimpton. How to build a hash function from any collision-resistant function. In Asiacrypt’07, vol. 4833, pp. 147-163. Springer-Verlag, 2007.

6. John Black, Phillip Rogaway, and Thomas Shrimpton. Black-box fnalysis of the block-cipher-based hash-function constructions from PGV. In Crypto’02, vol. 2442, pp. 320-335. Springer-Verlag, 2002.

7. Горбенко И.Д., Долгов И.В., Олейников Р.В., Руженцев В.И., Михайленко М.С., Горбенко Ю.И. Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования // Известия ЮФУ. Технические науки. 2007. №1. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (3.11.2020).

«AL02» ШИФРЛЕУ АЛГОРИТМІНІҢ ҚАСИЕТТЕРІН ЗЕРТТЕУ

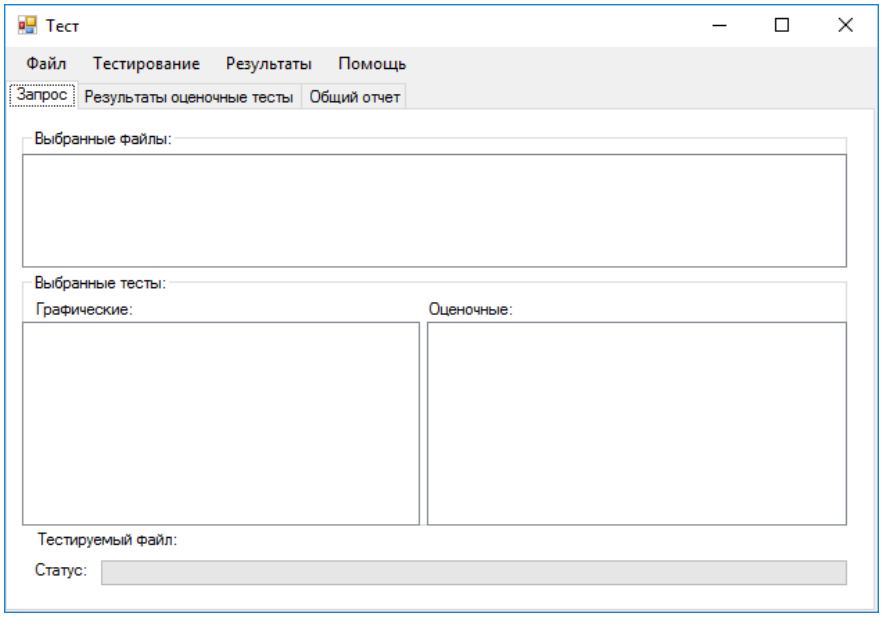
Самрат С.М.
e-mail: sanzhar.samrat@gmail.com
ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты», Қазақстан

Аңдатпа. *Бұл мақалада статистикалық тесттер жинағын қолдана отырып «AL02» шифрлеу алгоритмінің статистикалық қасиеттеріне зерттеу, талдау жасалды және сапасы бағаланды.*

Бүгінгі таңда жүргізіліп жатқан зерттеу жұмыстарының негізгі мақсаты «AL02» шифрлеу алгоритмінің статистикалық қауіпсіздігін бағалау. «AL02» шифрлеу алгоритмі бес раундтан тұрады. Бұл алгоритмде шифрлау блогының ұзындығы негізгі кілт ұзындығына тең және 128 битті құрайды. Алгоритмде сызықты емес функция ретінде қатысатын S-блок мөлшері – 8 бит. Қолданылатын негізгі модификациялар: 2 модуль бойынша қосу, S-блокты алмастыру және осы екі түрлендіруге негізделген F-түрлендіру.

Ұсынылатын криптоалгоритмге қойылатын талаптардың бірі, псевдокездейсоқ тізбек генераторы ретінде пайдалану жарамдылығы болып табылады. Ол үшін шифрмәтіндерді (алынған тізбектерді) статистикалық тесттерден өткізіп, нәтижелерін талдау керек. Тест үшін 20 түрлі файлды 5 түрлі кілттер тобымен шифрлеп, 100 шифрмәтін алынды.

Алынған 100 тізбектің статистикалық қауіпсіздігін зерттеу үшін «Д.Кнуттың статистикалық тесттерді және графикалық тесттерді таңдаудың автоматтандырылған жүйесі» (Автоматизированная система подборки статистических тестов Д.Кнута и графических тестов) бағдарламасы қолданылады.



1-сурет. «Д.Кнуттың статистикалық тесттерді және графикалық тесстерді таңдаудың автоматтандырылған жүйесі» бағдарламасының басты терезесі

Псевдокездейсоқ тізбекті зерттеу үшін, екі тест тобы қолданылады [1-3].

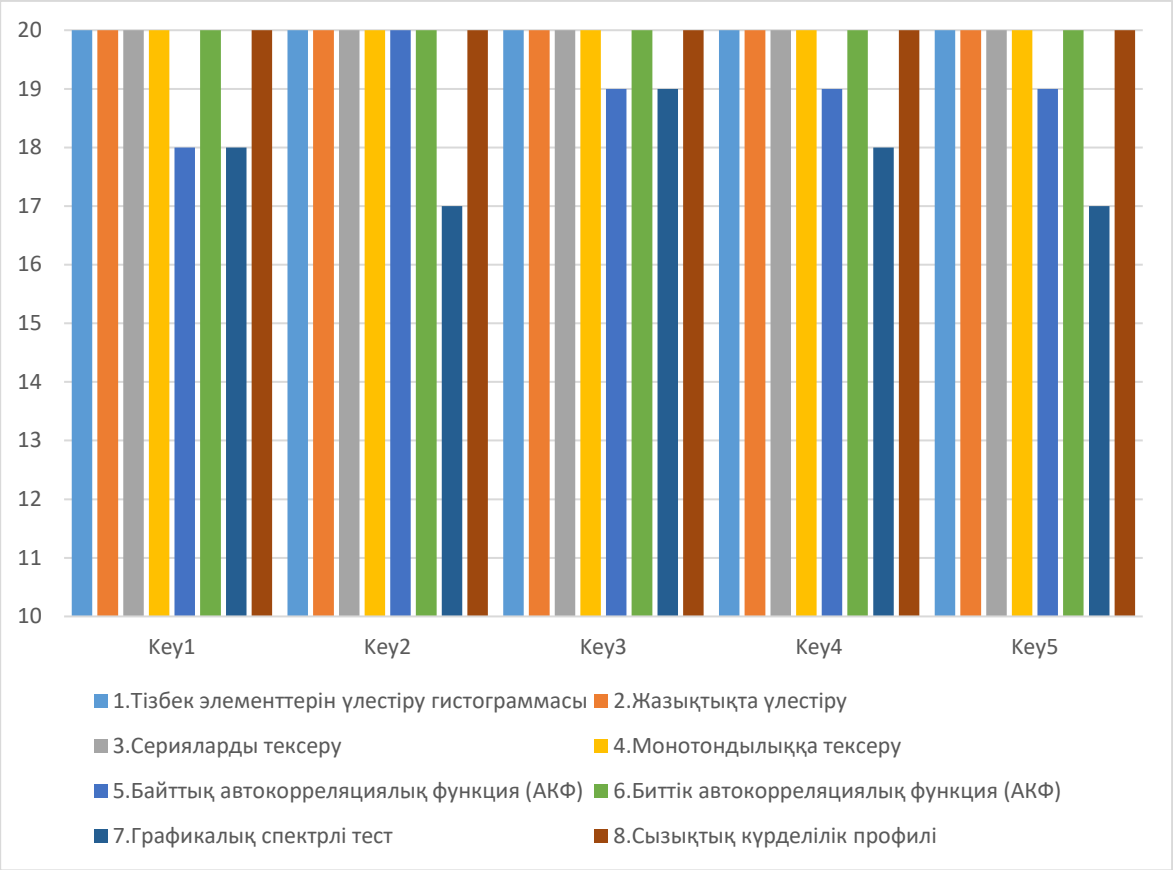
- **Графикалық тесттер.** Тізбектің статистикалық қасиеттері графикалық тәуелділік түрінде көрсетіледі. Графикке қарап зерттелетін тізбек қасиеттеріне қорытынды жасалады. Графикалық тесттер: тізбек элементтерін үлестіру гистограммасы; жазықтықта үлестіру; серияларды тексеру; монотондылыққа тексеру; автокорреляциялық функция (АКФ), графикалық спектрлі тест, сызықтық күрделілік профилі.
- **Бағалау тесттері.** Тізбектің статистикалық қасиеттері сандық сипаттамалармен анықталады. Бағалау тесттері беретін сандық сипаттама арқылы тесттен өткенін немесе өтпегенін нақты айтуға болады. Бағалау тесттері: 0 мен 1-ге тексеру, байланыссыз серияларды тексеру, символ бойынша тексеру, интервалдарды тексеру, комбинацияларды тексеру, купондарды жинаушының тесті, орын ауыстыруларды тексеру, корреляцияны тексеру.

1-кесте. Шифрмәтіндерді зерттеу нәтижелері

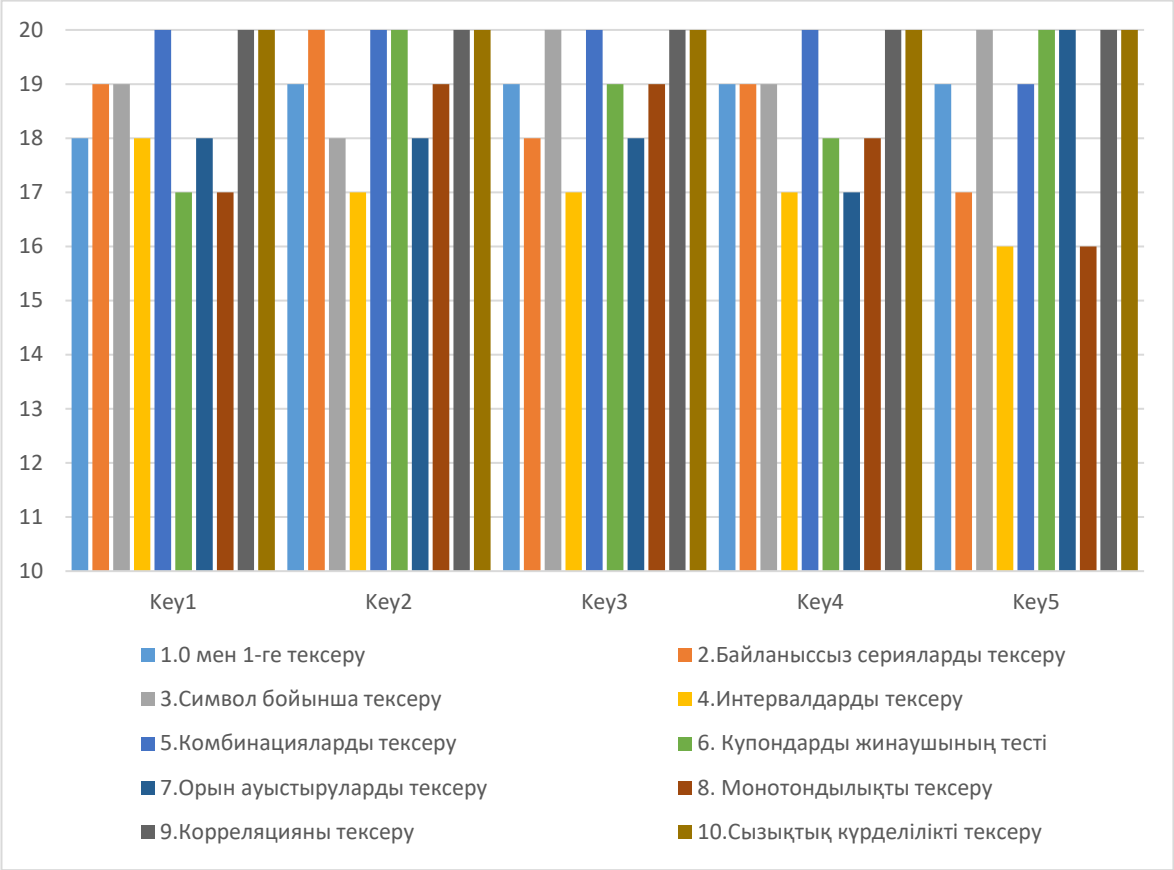
Тест түрі	Тесттер	Key1	Key2	Key3	Key4	Key5
Графикалық тесттер	1.Тізбек элементтерін үлестіру гистограммасы	20	20	20	20	20
	2.Жазықтықта үлестіру	20	20	20	20	20
	3.Серияларды тексеру	20	20	20	20	20
	4.Монотондылыққа тексеру	20	20	20	20	20
	5.Байттық автокорреляциялық функция (АКФ)	18	20	19	19	19
	6.Биттік автокорреляциялық функция (АКФ)	20	20	20	20	20
	7.Графикалық спектрлі тест	18	17	19	18	17
	8.Сызықтық күрделілік профилі	20	20	20	20	20
Бағалау тесттері	1.0 мен 1-ге тексеру	18	19	19	19	19
	2.Байланыссыз серияларды тексеру	19	20	18	19	17
	3.Символ бойынша тексеру	19	18	20	19	20
	4.Интервалдарды тексеру	18	17	17	17	16
	5.Комбинацияларды тексеру	20	20	20	20	19
	6. Купондарды жинаушының тесті	17	20	19	18	20
	7.Орын ауыстыруларды тексеру	18	18	18	17	20
	8. Монотондылықты тексеру	17	19	19	18	16
	9.Корреляцияны тексеру	20	20	20	20	20

	10.Сызықтық күрделілікті тексеру	20	20	20	20	20

1-кестеде әр тесттен сәтті өткен тізбектер саны көрсетілген. 2 және 3-суретте графикалық және бағалау тесттер нәтижелері көрсетілген.



2-сурет. Графикалық тесттер нәтижелері



3-сурет. Бағалау тесттер нәтижелері

Графикалық және бағалау статистикалық тесттерінен алынған тізбектің статистикалық сипаттамаларын талдау нәтижелері алынды.

Графикалық тесттер нәтижелері 2-сурете көрсетілген. Жалпы тест нәтижелері – жақсы. Нәтижелер шифрленетін файл түріне байланысты болады. Графикалық спектрлі тест пен байттық автокорреляциялық функция тесттерінен орташа алғанда 18 файл өтті. Қалған графикалық тесттерден барлық 20 файл сәтті өтті.

Бағалау тесттер нәтижелері 3-сурете көрсетілген. Комбинацияларды тексеру, корреляцияны тексеру, сызықтық күрделілікті тексеру тесттерінен барлық 20 файл өтті. Қалған бағалау тесттерінен орташа 18-19 файл сәтті өтті, және бұд нәтиже – жаман емес. Бұл тесттерде дәлірек нәтиже алу үшін тізбек ұзындығын және файлдар санын көбейтіп, қосымша тестілеу жасауға болады.

Әдебиеттер

1. Нысанбаева С.Е., Капалова Н.А., Дюсенбаев Д.С., Алгазы К.Т. Исследования статистических свойств разработанного генератора псевдослучайных последовательностей // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2018. – С. 210-217.

2. Капалова Н.А., Алгазы К.Т., Самрат С.М. Криптоалгоритмдердің статистикалық қауіпсіздігін зерттеу // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий (29-30 июня 2017 г.)». – Алматы, 2017. – С. 108-113.

3. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: «КУДИЦ-ОБРАЗ», 2003. – 240 с.

4. Дюсенбаев Д., Сақан Қ. «AL01» шифрлау алгоритміне криптографиялық талдау // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» (Часть II). – Алматы, 2019. – с. 561-569.

5. Бияшев Р.Г., Алгазы К.Т., Дюсенбаев Д.С., Ержанов Е.Б. Результаты проверки «лавинного эффекта» алгоритма «AL01» // Материалы IV международной научно-практической конференции «Информатика и прикладная математика» (Часть II). – Алматы, 2019. – с. 602-607.

КРИПТОГРАФИЯ ЖӘНЕ СТЕГАНОГРАФИЯ АЛГОРИТМДЕРІН ҚОЛДАНА ОТЫРЫП, ШИФРЛАУДЫҢ ЖӘНЕ ДЕКОДТАУДЫҢ ЖАҢА ТӘСІЛДЕРІ.

Аяшова А.М.
e-mail: ayashova.a@mail.ru
Казахский Национальный Университет имени Аль-Фараби,
Факультет Информационных технологий

Аңдатпа*. Бұл мақалада желілік ортада деректердің қауіпсіздігін арттыру үшін аффинді шифрлау алгоритмі бар Hash Least Significant bit (H-LSB) алгоритмі ұсынылды.*
Түйін сөздер: Криптография, стеганография, құпия хабарлама, хэш негізіндегі LSB, аффинді шифр, шифрлау процесі, дешифрлау.

Қазіргі уақытта желі деректерді көзден тағайындалған жерге дәл және жылдам жеткізуде маңызды рөл атқарады. Деректер құпиялылықтың жоғары деңгейімен беру үшін жеткілікті қауіпсіз емес. Ақпараттық қауіпсіздік компьютерлік желі арқылы деректерді беру кезінде ресурстарды бөлісудің негізгі мәселелерінің бірі болады. Криптография және стеганография - ашық арна желісі арқылы беру кезінде деректерді зиянкестерден қорғаудың екі әдісі болып табылады. Криптография - бұл деректерді шифрлау әдісі, ал стеганография - мұқабадағы құпия хабарламаны жасырудың өнері мен ғылымы.

Алдымен біз деректерді жаңа криптографиялық алгоритммен шифрлаймыз, содан кейін кескінге енгіземіз. Құпия хабарламаның сегіз биті 3, 3, 2 болып бөлінеді және сәйкесінше мұқабаның RGB пиксель мәндеріне енеді. LSB биттеріндегі кірістірудің нақты орнын таңдау үшін хэш функциясы қолданылады. Бұл жүйе хабарлама жіберушіге кескінге енгізбестен бұрын құпия хабарламаны шифрлау кілттерін таңдауға мүмкіндік береді, ал алушы хабарламаны шифрлау үшін кілттерді пайдаланады. Алушы шифрланған хабарламаны дұрыс емес кілттермен, бірақ бастапқы хабарламадан басқа нысанда шеше алады. Бұл жүйе құпия хабарламаны желілік ортада бір ұшынан екінші ұшына беру кезінде қауіпсіздікті жақсартуға қабілетті.

Телекоммуникация саласы өскен сайын желілер арқылы желілік сандық суреттердің әртүрлі түрлері беріледі. Қазіргі әлемнің әр дамып келе жатқан саласының негізгі қажеттілігі - байланыс. Барлығы ақпараттың құпия және қауіпсіз болуын қалайды. Интернеттің өсуі, ақпараттық технологиялар мен коммуникацияның маңызды факторлары ақпараттың қауіпсіздігі болады [1].

Күнделікті өмірде біз телефон арқылы немесе интернет арқылы ақпарат алмасу және беру үшін көптеген қауіпті жолдарды қолданамыз. Алайда, белгілі бір деңгейде бұл қауіпті. Криптография және стеганография - бұл ақпаратты өз өмірін шифрлау немесе жасыру үшін пайдаланатын екі әдіс. Оларды ақпаратты жасырын түрде бөлісу және беру үшін пайдалануға болады. Криптография - бұл байланыс құпиялығын қамтамасыз ету үшін хабарламаны өзгертуді қамтитын әдіс [2]. Қазіргі уақытта хабарлама құпиясын қорғау үшін деректерді шифрлау және дешифрлау үшін көптеген түрлі әдістер қолданылады.

Криптография. Криптографияда аралық тұлғаға хабарлама тек жіберуші мен алушыға белгілі шифрлау кілтімен шифрланғаны туралы түсінікті. Шифрлау кілтін

пайдаланбай хабарламаға қол жеткізу мүмкін емес. Алайда, бұл әдістер хабарлама құпиясының мазмұнын қорғау үшін жеткіліксіз. Өйткені криптографияда стеганография деп аталатын басқа әдіс қолданылады [3].

Стеганография - бұл хабарламаны көрінбейтін түрде беру өнері мен ғылымы, ал құпия хабарлама оны мұқабада жасыру үшін жасалады және адам суретте жасырылған хабарламаны көре алмайды [4]. Мұқабаның құпия деректері бар суреті содан кейін алушыға беріледі. Алушы хабарламаны қабылдау процесі және жіберуші ұсынған құпия кілт арқылы ала алады.

Криптография - бұл хабарламаны рұқсат етілмеген пайдаланушылардың хабарламаларға қол жеткізуінен қорғау үшін құпия хабарламаларды кодтау және декодтау механизмі. Желілік ортада криптография жұмыс істейтін қосымшаларда деректерді қорғауда үлкен рөл атқарады. Грек тілінде криптография "жасырын құпия" дегенді білдіреді. Сонымен қатар, бұрын криптографияны барлау және қарулы күштердің саяси секторы қолданған. Ал қазіргі уақытта ол банкомат карталарында, электрондық коммерцияда, электрондық пошталарда, компьютерлік парольдерде және басқа қосымшаларда жиі қолданылады. Осы жылдар ішінде хабарламаны жіберуші мен алушыға белгілі шифрлау кілтімен өзгерту үшін әртүрлі алгоритмдер пайда болады [4].

Хабарламаны шифрлау кілтін пайдаланбай шифрлау мүмкін емес. Криптографиядан туындайтын мәселелердің бірі - бұл хабарлама әрдайым арадағы адамға түсінікті, өткені бұл хабарлама шифрланған. Бұл хабарлама жіберушінің бөтен адамның оқығанын қаламайтынын білдіреді. Бүгінгі таңда деректерді шифрлай алатын криптографияның көптеген әдістері бар. Ең көп таралған әдістердің бірі-аффиндік алгоритм. Аффиндік алгоритм ақпаратты шабуылдаушы үшін түсініксіз пішінге айналдыра алады.

Стеганография. Қазіргі уақытта пайдаланушылар арасында сандық кескінді бөлісу үшін әртүрлі желілер қолданылады. Компьютерлік желілердің түрлерінің көбеюімен сандық мәліметтердің үлкен көлемі желі арқылы жеткізіледі. Өйткені олардың көпшілігі құпия, жеке немесе екеуі де болуы мүмкін. Бұл деректерді зиянкестерден қорғау үшін шифрлаудың сенімді әдістеріне қажеттілік артады [5].

Стеганография - құпия хабарламаны кескінге енгізу үшін қолданылатын маңызды әдістердің бірі [6]. Бұл әдіс қолданушыға кескін ішіндегі ақпаратты жасыруға мүмкіндік беретін тамаша шифрлау қосымшасы болып табылады. Стеганография әдістері криптография арқылы құпия хабарламаны қосымша қорғауды қамтамасыз ете алады, осылайша ақпарат екі есе қорғалады [7].

Стеганография кескіннің ішіндегі ақпаратты жасырады, сондықтан кескіннің ішінде ешқандай ақпарат жасырмайтын сияқты болып тұрады. Осылайша, пайдаланушылар құпия ақпаратты қорғалмаған арна арқылы, мысалы, Интернет арқылы жібере алады. Стеганографияның әртүрлі әдістері қолданылады. Бұл мақалада біз кескінге құпия хабарламаны енгізу үшін ең аз маңызды бит (LSB) әдісін қолдандық.

Шифрлау. Бірінші кезеңде деректер жүйесіне кіру үшін пайдаланушыларға пайдаланушы аты мен пароль қажет. Жүйеге кіргеннен кейін пайдаланушы құпия кілттермен деректерді шифрлау үшін хабарлама жаза алады. Біздің жүйеде құпия ақпаратты шифрлау үшін Афина алгоритмін қолданамыз. Афина алгоритмі - деректерді шифрлау үшін қолданылатын алгоритмдердің бірі. Бұл процесте алфавиттегі әр әріп оның сандық эквивалентімен салыстырылады, математикалық функцияны қолдана отырып шифрланады және қайтадан әріпке айналады.

Пайдаланылған формула әр әріп бір әріпке және артқа шифрланғанын білдіреді. Яғни шифр дегеніміз - бұл стандартты ауыстыру шифры, ол қай әріпке қалай жүретінін анықтайды.

Бұл әдіс деректерді пайдаланушыны желі арқылы рұқсатсыз кіруден қорғау үшін қауіпсіздікті қамтамасыз етеді. Сондықтан деректерді алушының кілтінсіз алу оңай болмайды. Қарапайым мәтінді шифрланған мәтінге айналдырғаннан кейін афина алгоритмнің көмегімен біз жоғары қауіпсіздікті қамтамасыз ету үшін шифр мәтінін алып, әр әріпті екілік кодтарға айналдырдық. Бұл ұсынылған әдіс шабуылдаушылардың оларды алуға тырысқанда нақты деректерді алуына жол бермеу үшін қолданылады. Бұл шифрланған деректер бастапқы кескіннің нөлдік бұрмалануымен кескінге енеді.

Мысалы:
Мәтін: Казахстан
Шифрланған мәтін: мигиузких
Бұл жерде әріптер А әрпінен Я әрпіне дейін алынған.

Шифрланатын ашық мәтінмен «Казахстан» алынды. Әр әріптің сандық мәндері үшін және әр әріпті шифрлау үшін келесі функция қолданылды:

$$E(x) = (ax + b) \bmod m \quad (1)$$

мұндағы:
x: ашық мәтіндегі әріптің сандық мәні.
m: ашық мәтін әліпбиіндегі әріптер саны.
a және b - жіберуші мен алушы арасындағы құпия сандар.
E (x): түрлендіру нәтижесі.

Кесте 1 - X мәнін анықтау

мәтін	К	а	з	а	х	с	т	а	н
X	11	1	8	1	22	18	19	1	14

Енді әр x мәнін алып, теңдеудің бірінші бөлігін орындаймыз (3x + 6). Әр таңба үшін (3x + 6) мәнін тапқаннан кейін нәтижені (3x + 6) 26-ға бөлген кезде қалдықты аламыз. Келесі кестеде шифрлау процесінің алғашқы төрт қадамы көрсетілген:

Кесте 2 – Мәтінді шифрлау

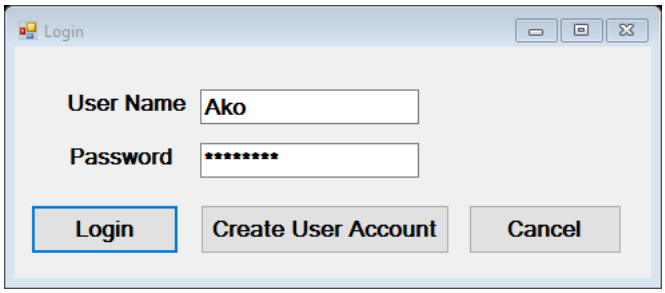
мәтін	К	а	з	а	х	с	т	а	н
X	11	1	8	1	22	18	19	1	14
(3x + 6)	39	9	30	9	72	60	63	9	48
(3x + 6)mod26	13	9	4	9	20	8	11	9	22
Шифрленген мәтін	м	и	г	и	у	з	к	и	х

Сандарды екілік түрінде көрсету үшін 6 екілік бит қажет, өйткені орыс алфавитінде 33 әріп қолданылады. Сондықтан бастапқы мәтін келесідей болады: 001101, 001001, 000100, 001001, 010100, 001000, 001011, 001001, 010110

Құпия хабарламаны шифрлағаннан кейін шифрланған хабарламаны кескінге ендіру әдісін қолдануға болады. Бұл процесс кіші мәнді битті алмастыратын хэш негізіндегі ең аз мәнді битті (HLSB) қолдану арқылы жүзеге асырылады. LSB-деректерді кескін файлына ендірудің ең танымал стеганография әдісі. Бұл әдіс

суреттегі шифрланған хабарламаны жасыру үшін қолданылады, содан кейін суретті алушыға жібереді. Бірінші кезеңде біздің жүйеде пайдаланушылар логин мен парольді алу үшін тіркелгі жасауы керек. Тіркелгенде пайдаланушылар барлық өрістерді толтыруы керек.

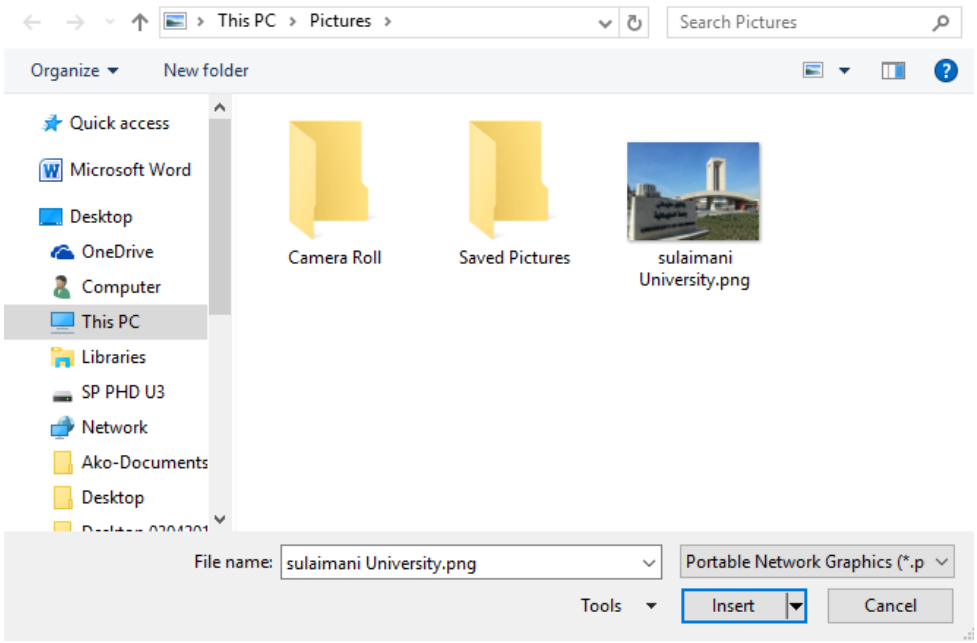
Құпия хабарламаны шифрлағаннан кейін шифрланған хабарламаны кескінге ендіру әдісін қолдануға болады. Бұл процесс кіші мәнді битті алмастыратын хэш негізіндегі ең аз мәнді битті (HLSB) қолдану арқылы жүзеге асырылады. LSB-деректерді кескін файлына ендірудің ең танымал стеганография әдісі. Бұл әдіс суреттегі шифрланған хабарламаны жасыру үшін қолданылады, содан кейін суретті алушыға жібереді. Бірінші кезеңде біздің жүйеде пайдаланушылар логин мен парольді алу үшін тіркелуге жазылу керек. Жүйеге тіркелгеннен соң, пайдаланушылар 1-суретте көрсетілгендей кіру үшін логин мен парольді қолдана алады.



Сурет 1- Жүйеге кіру

Жүйеге кіргеннен кейін жүйелік пайдаланушылар екі қойындыны көре алады: біреуі - шифрлау деректерін кескінге шифрлау және ендіру үшін "деректерді кодтау", екіншісі - кескін ішіндегі деректерді шығару үшін "деректерді декодтау". Кескін туралы ақпарат, мысалы: сөздердің саны, кескіннің ішінде кодтауға болатын максималды өлшем. Суреттің өлшемі, биіктігі мен ені жоғарғы оң жақ панельде көрсетіледі. Сонымен қатар, кодтау қойындысындағы жоғарғы жолақта бізде бір мәтін өрісі бар. Ал батырма кескінді компьютердегі кез-келген жерден жүктеу үшін қолданылады.

Файлды ашудағы диалог терезесі келесідей көрсетіледі: пайдаланушы құпия суретті жасыру үшін кескін файлын таңдап, 2-суретте көрсетілгендей "ашу" түймесін басуы керек.

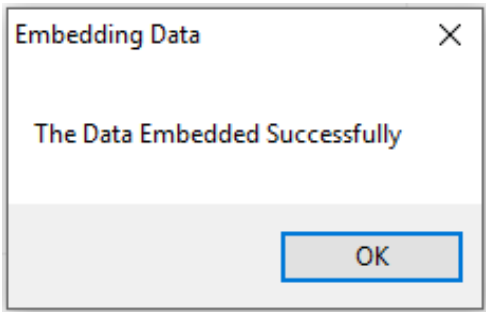


Сурет 2 - Суретті таңдау

Кодтау қойындысында үш мәтін өрісі бар: біріншісі - пайдаланушылар кескінде кодтағысы келетін құпия хабарлама жазуға арналған құпия хабарлама, екіншісі - хабарламаны шифрлау. Бұл мәтін өрісінде пайдаланушы шифрланған хабарламаны тікелей көре алады. Ал үшінші мәтін өрісі кескінді енгізбестен бұрын түрлендірілген шифрланған хабарламаны ASCII кодына көрсету үшін қолданылады.

Сонымен қатар, шифрланған хабарламаны кескін ішінде жасыру және қауіпсіздік үшін пароль қажет. Тексеру үшін парольді екі рет енгізу керек. Пайдаланушының паролі үшін алты таңбаны пайдалану керек. Бұл деректер паролі кескінге де енеді. Құпия хабарламаны шифрлау үшін пайдаланушыларға Affine cipher key таңдау керек.

Шифрланған деректерді енгізгеннен кейін пайдаланушылар 3-суретте көрсетілгендей шифрланған деректердің сәтті енгізілгеніне көз жеткізу үшін хабарлама терезесін алады.



Сурет 3 - Деректерді ендіру

Шифрланған деректерді сәтті енгізгеннен кейін жаңа stego_image дерекқорда сақталады. Сонымен қатар, пайдаланушылар stego_image-ді тікелей Интернет арқылы немесе мақсатты пайдаланушыларға электрондық пошта арқылы кескіннің

ішіндегі құпия деректерді ашпай-ақ жібере алады. Бұл жүйеде деректерді шифрлау немесе алу үшін екінші қойынды қолданылады. Бұл қойынды жолағы екі мәтін өрісінен, кескін көрінісінен, екі тізім өрісінен және түймелерден тұрады. Алушы дерекқордан суретті сұрау үшін пароль енгізу үшін бірінші мәтін өрісін пайдаланады.

Дұрыс парольді енгізіп, "суретті қайтару" түймесін басқаннан кейін, кескін шифрлау жолағына бірден оралады. Бірақ алушылар a = 3 және b = 6 сияқты екі тізім өрісі арқылы аффиндік шифрлау кілттері дұрыс таңдалғанға дейін кескінге енгізілген деректерді шығарып, шеше алмайды. Бұл деректердің тұтастығы мен құпиялылығын қамтамасыз ету үшін қажет. Қате құпия кілтті кез-келген таңдау арқылы алушы мағынасыз хабарламаны қайтарады. Бұл желілік ортадағы зиянкестерге қарсы деректердің қауіпсіздігіне кепілдік береді.

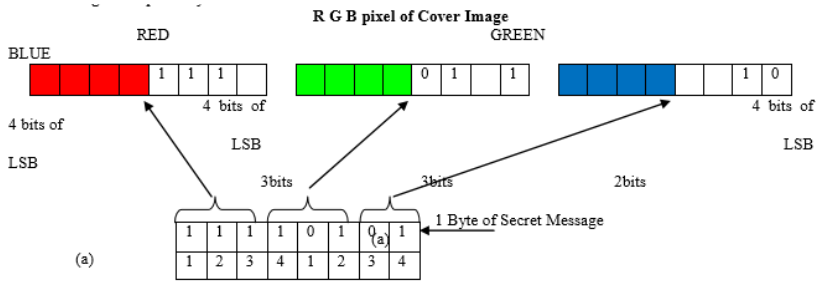
Бұл мақалада көп деңгейлі қауіпсіздік әдістерін қолдана отырып, деректерді зиянкестерден қорғаудың жақсы қауіпсіздігін қамтамасыз ету үшін криптография және стеганография әдістері ұсынылған. Осы екі әдістің үйлесімі пайдаланушылар ашық арна арқылы деректерді беру кезінде басқалардан қорғағысы келетін кейбір маңызды деректердің арқасында деректерді енгізу қауіпсіздігін арттырады.

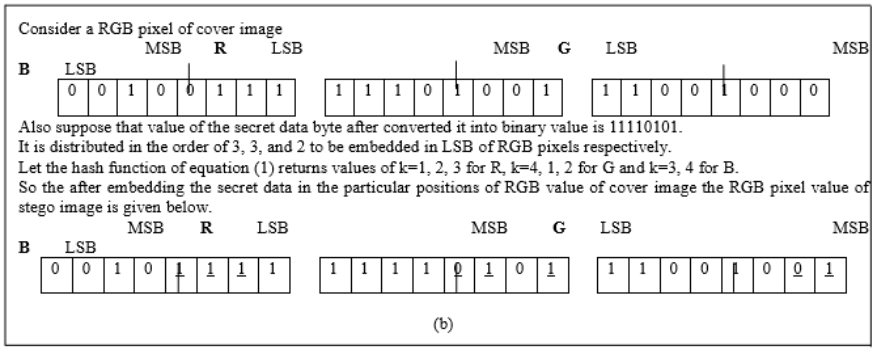
Бұл процестің басында шифрланған хабарлама алынады, ол мұқабаның кескініне енеді. Кез-келген шабуылдаушыға оны алушының жеке кілтінсіз шифрлау қиын болады. Содан кейін хэш функциясы позицияларды таңдау үшін қолданылады және ұсынылған әдіс сегіз бит алынады, құпия деректер сәйкесінше 3, 3, 2 ретпен LSB пиксель мәндеріне (қызыл, жасыл және көк) енеді. Әдістерге сәйкес, кескінге құпия деректерді енгізу үшін қызыл пиксельдің LSB-ге үш бит, жасыл пикселье үш бит және көк пикселдердің LSB-ге 2 бит біріктірілген.

Бұл сегіз бит келесі ретпен енгізілген, өйткені көк түстің адам көзіне хроматикалық әсері қызыл және жасыл түстерге қарағанда үлкен. Сондықтан үлестіру үлгісі көк пиксельде жасырылатын 2 битті таңдайды. Осылайша, сурет сапасы жойылмайды. Бұл процесс барлық биттік хабарлама мұқаба кескініне енгенге дейін жалғасады. Әрбір RGB мұқаба кескінінің LSB-де деректерді жасыру позициясын анықтау үшін келесі формула қолданылады:

$$K = p \,\%\, n \ldots\ldots\ldots (1) \qquad (2)$$

мұндағы K – пиксельдегі кіші бит позициясы, P – жасырын кескіндегі әр пиксельдің орны, ал n - LSB бит саны, біздің жағдайда ол - 4.





Сурет 4 (a) және (b). RGB пиксель мәнінің кіші екілік разрядын табу үшін хэштеу процесі

Қорытынды

Бұл мақалада желілік ортада деректердің қауіпсіздігін қамтамасыз ету үшін криптография және стеганография әдістері ұсынылған. Біз ұсынатын жүйенің көмегімен деректерді жіберуші мен алушы арасында қорғалмаған желілік орта арқылы жіберуге болады. Желілік ортада бұл жүйе шабуылдаушылардан хабарлама құпиясын жасырудың ең жақсы тәсілдерінің бірі екені анық.

Мақалада қауіпсіздіктің қосымша функциялары бар жүйені дамытуға баса назар аударылады. Криптография әдісі, яғни аффиндік шифрлау алгоритмі құпия хабарламаны шифрлау үшін жүзеге асырылды және екілік кодқа түрленді. Сондықтан шабуылдаушыға кілтсіз және парольсіз шифрлауды бұзу оңай болмады.

Әдебиеттер

1. Р. Пурнима и Исвария Р.Дж. «Обзор стеганографии цифровых изображений». Международный журнал компьютерных наук и инженерии 4.1 (2013): 23-31.

2. А. Анагоу и В. Шринивасарао. Модифицированный метод шифрования RSA на основе нескольких открытых ключей. Международный журнал инновационных исследований в области компьютерной и коммуникационной техники, Vol. 1, выпуск 4, июнь (2013): 859-864

3. Рашид, Акса, Малик Миссен и Надим Саламат. «Анализ методов стеганографии с использованием наименее значимого бит в изображениях в оттенках серого и его расширение на цветные изображения» Журнал научных исследований и отчетов (JSRR) 9.3 (2016): 1-14.

4. Ахмед Ласкар, Шамим. «Скрытие данных большой емкости с использованием стеганографии и шифрования LSB», Международный журнал систем управления базами данных (IJDMS) 4.6 (2012): 57-68.

5. Анил Кумар и Рохини Шарма. Защищенная стеганография изображений на основе алгоритма RSA и метода Hash-LSB. Международный журнал перспективных исследований в области компьютерных наук и программной инженерии. Том 3, выпуск 7, июль (2013): 363-372.

6. Романец Ю. В. Защита информации в компьютерных системах и сетях. /Под ред. В.Ф. Шаньгина. – М: Радио и связь 1999

7. Петраков А.В. Основы практической защиты информации. 2-е издание Учебн. Пособие. – М: Радио и связь 2010

OVERVIEW OF TYPICAL ATTACKS ON CRYPTOGRAPHIC PROTOCOLS FOR EXCHANGING KEY DATA.

Ospanov Zh.Zh.[1], Gorlov L.V.[1], Ibrayev R.B.[2], Kiyashko I.V., Itemirov R.S.
Almaty, Republic of Kazakhstan, [1] Al-Farabi Kazakh National University,
[2] Satbayev University.
tbegeldin@yandex.kz

Abstract: *This article discusses typical attacks on cryptographic key exchange protocols and also discusses potential vulnerabilities that are possible in the architecture of the protocol with methods of protection against specifically presented threats.*

Keywords: *Key exchange protocol, cryptographic protocol, cryptography, protocol attack.*

Introduction

The modern world economy is based on data exchange information systems. Recent events related to the pandemic have led to the digitalization of new spheres of human activity and have shown an even greater dependence of a person on information systems. The list of processes gradually flowing into digital format is constantly growing.

The prevalence of information systems creates positive dynamics in the IT field, which in turn increases the interest of attackers, as well as their number. The ever increasing capitalization associated with these processes indicates the need to ensure a high level of protection of confidential information. New areas of application of old technologies are emerging, which in turn creates prerequisites for the synthesis and use of new vulnerabilities. The constant fight against intruders leads to a permanent evolutionary process of information systems protection mechanisms. The transition from fat clients to lighter and more cross-platform solutions creates even more fertile conditions for crimes in this area and creates the preconditions for a new round of development of security systems.

To date, the existing practice in the construction of information systems in which confidential user data circulate implies the use of cryptographic protection methods, which in turn is not possible without a secure system of distribution and exchange of key information. The Kirchhoff principle, according to which the stability of the algorithm is provided only by the fact that the attacker does not know the key information, sets a high bar for the requirements for the distribution system of key information. In other words, the security of a cryptographic system with a properly developed mathematical apparatus has only one possible vulnerability - the keys on which the transmitted information is encrypted.

1. Basic concepts

Protocol - a description of an algorithm in which at least two participants sequentially perform certain actions and to ensure communication.

Participants (in other words - subjects, parties) of the protocol are the actors performing actions according to the protocol.

It is understood that all participants will take an active part in it, and passive observers are not participants in the protocol. The concepts of cycle, step, role and session are directly related to the protocol concept.

The sequence of steps in the protocol (request from A, request from B, response from A, etc.) is grouped into cycles.

Round is a time interval in which only one of the participants is active.

The cycle (transition) ends with the formation and sending of a message, followed by the transition of the active participant to the waiting state and the transfer of activity to another participant, in the asynchronous case the concept of a cycle is conditional.

A protocol step (protocol action) is a specific completed action performed by a participant (protocol) during one cycle (pass) of the protocol.

A session is a private process of performing protocol actions with specific participants.

Cryptographic protocol - a protocol with the performance of the functions of a cryptographic system.

Cryptographic system - a system for protecting information using cryptographic methods.

The main functions of a cryptographic system are confidentiality, integrity, authentication, non-repudiation, and non-traceability.

As subsystems, it can include encryption systems, identification systems, imitation security systems, digital signature systems, as well as a key distribution system.

Authentication is the process of verifying the identity of a protocol participant using the built-in functions of protocol methods to ensure that non-repudiation cannot be guaranteed during a communication session.

Message Authentication — A verification process performed during a communication session between parties to ensure that messages from an authenticated protocol party match. This mechanism must ensure that the received messages are not tampered with or distorted, created by an authenticated protocol participant in a legitimate time period, but not guaranteeing the timeliness of receiving messages.

Replay protection is a protocol mechanism that protects against threats exploiting vulnerabilities at the expense of time. In other words, the mechanism ensures that the received messages:

- have not been received earlier;
- generated during the current communication session;
- and was generated at a known time interval.

An attack on a protocol is an attempt to exploit a potential vulnerability embedded or not provided for in the protocol architecture in order to substitute, alter, or obtain unauthorized access to information circulating between protocol participants or other possible compromise. An attack is considered successful if at least one of the declared properties that characterize the security of the protocol are violated.

2. Major attacks on key distribution protocols.

For the most part, the classification of attacks is as follows:

- by the method of exposure (direct or indirect exposure);
- by the object of influence (on which of the elements of the protocol the attack is carried out);
- by the type of protocol;
- by the tools of influence (using the attacks presented below);
- by the resources required (what is the amount of required computing resources for the successful implementation of the attack);
- by the presence of additional information (knowledge of the complete architecture of the protocol, only partial information, features of service data, etc.).[1,2,3]

The list of the main types of attacks is as follows:

1. Substitution (impersonation).

A type of attack when an attacker acts on behalf of a legitimate user. The essence of the attack is that the attacker completely repeats and emulates the actions of the attacked person according to the protocol algorithm. It is one of the middle attack implementations.

The main ways to counter this method are:

- use of user identification marks;
- in the process of establishing communication, the use of various types of service messages;
- use of third party user authentication.
- keeping (if possible) in secret the algorithm for establishing communication between legitimate users.

2. Replaying the message (replayattack)[4].

These are attacks based on duplicate messages from a legitimate user of the system by an attacker in order to establish the same type of connection as the attacked object, as well as the ability to obtain an identical key. This type of attack differs from spoofing in that the attacker does not act as an intermediate link in the communication session, but has identical rights and capabilities of the attacked object. To implement this type of attack, service packets and data are used that were used earlier in the same session or in the previous protocol communication session.

In the protocols of transmission and exchange of key data, this type of attack can be used to reuse the key used in the previous session. This, in turn, allows you to compromise the system or the communication session as a whole.

Effective protection tools are:

- formation and attachment to each message of "conditional" time stamps containing information about the start time of the session, allowing you to track whether the message was received earlier, as well as metrics to determine the connection session. For example, using a pseudo-random number generator, which, according to a certain rule, will attach the above "conditional" timestamp.
- use of staged messaging in the architecture of connection establishment. Providing an increase in the complexity of using the accumulated data for the implementation of this method.

3. There is a type of message re-intrusion attack, where the data received from it is repeated to the attacked object and is called the reflection attack.[7]

To protect against this kind of attacks, the protocol architecture should contain non-symmetric overhead that allows tracing the initiator of the communication session.

4. There is also a type of re-enforcing attack, the essence of which is based on the re-sending of messages after a long time interval (forced delay), due to which the counters for receiving messages as well as time constraints may lose their meaning, and the attacked object, having received the message, will consider it legitimate to establish a new communication session.

To protect against such attacks, it is necessary to use the time stamp of the allowed time of message receipt in the protocol, in other words, for each time stamp, its own receiving and sending corridor is established.

5. Combined attack (interleavingattack).

This attack consists in the use of several simultaneously or sequentially applied attacks to compromise one user or gain unauthorized access to protected data.

Protection consists in the implementation of metrics and control labels that provide protection or inform about the violation of the integrity of the protocol stages to the participants in the communication session.

6. Another type of attacks presented above is the creation of simultaneous concurrent user authentication sessions with the attacked object to use messages from one sen in another. At one time, such an attack was successfully used against the Needham-Schroeder protocol, which was later improved and taken as the basis for the first versions of the Kerberos protocol.

The main method of protection against this type of attacks is the use of methods for controlling the integrity of the entire communication session.[6]

7. Attack by requests.

The essence of the presented attack lies in the use of specially selected requests by an attacker. As a result, the attacker obtains information about the long-term key. It is important to note that the attacked object acts as a slave in the protocol, in other words, the attacker appears to be a trusted party seeking to authorize the user.

The attacker in this case must:

- carry out the necessary manipulations with specially selected texts (encrypt, sign, calculate the checksum);
- to decrypt some previously intercepted text cipher.

Protection against this kind of attacks is based on the methods presented above:

- use of non-symmetric architecture;
- use of timestamps and metrics;
- use of methods for checking the integrity of protocol stages;
- creation of a complex hierarchical structure.

8. One of the resource-intensive methods is an attack based on providing an attacker with an environment for distributing and exchanging data. In other words, the classic attack Man in the middle. An attacker is capable of completely spoofing messages for both legitimate representatives of the protocol. The attack itself is based on the fact that the attack tool is the data transmission medium. In this case, the attacker is able to use additional other types of attacks presented. [12]

Protection against attacks of this kind is based on the use of:

- time stamps;
- message integrity labels;
- marks for checking the correctness of the protocol stage;
- It should be noted separately the method of labels and metrics of third parties. This method is used in modern protocols for using secure communication with a site, where a third party is a certification center that creates an additional connection with both communication members and carries out their identification.

9. Attack based on a known session key. [9]

The task of the attacker is to obtain data about a long-term key or other information that allows him to recover other session keys used in the protocol.

Protection against this kind of attacks is based on:

- a special architecture for generating keys, where the recovery of a certain key does not provide information about other session or long-term protocol keys;
- using a special mechanism that allows you to jointly generate a new session key.

10. Another type of middle attack is the unknown shared key attack. The essence of the attack is as follows[1]:

A third party acts between two legitimate participants in the protocol session, which opens two sessions with both participants. As a result of the attack, a situation arises in which a shared key is formed between the first and second parties, however, the first party will consider that it has formed a shared key with the second party, and the second party will consider that it has formed a shared key with a third party, which may not know the

shared key. An example of such an attack has been successfully implemented against the STS protocol.

Protection against the presented attack is implemented by using the following tools:

- use of checksums of protocol messages;
- use of digital signatures of subscribers;
- the use of tools for checking individual stages of the protocol;

11. Attack on implementation error.

This type of attack examines specific software implementations of algorithms and searches for potential vulnerabilities in them with their exploitation. Consideration of detailed attacks of this kind is not rational, but it is worth noting that protection against such attacks is built by other organizational and technical methods. Aimed at eliminating errors of this kind.

12. Attacks on linked keys.

Attacks of this kind are used in asymmetric systems, where an attacker replaces the public key of the attacked object with a previously known secret part. This allows you to completely duplicate the attacked object in the network with the ensuing consequences.

Protection against such attacks is based on the creation of a special infrastructure for the distribution of public / private keys, with a center that periodically checks, reviews, and issues new pairs.

Conclusion

The constant development of technology leads to an inevitable process of obsolescence of existing solutions. The safety margin set by the developers in relation to the computing power of their systems poses for the attackers the task of finding imperfections in the mathematical apparatus or the authentication architecture itself.

The attacks and threats shown above have shown that the use of cryptographic protection methods is not a panacea for communication security. The development of protection systems against existing threats has led to a natural process of evolution of data exchange protocols using cryptographic protection methods.

Literature

1. Cheryomushkin A.V. Cryptographic protocols. Basic properties and vulnerabilities: a tutorial. Moscow: Ed. Center "Academy", 2009.272 p.

2. Index of the security protocols repository (SPORE) // Laboratorie Sp'ecification et V'erification. http://www.lsv.ens-cachan.fr/spore/table.html.

3. Clark J., Jacob J. A Survey of Authentication Protocol Literature: Version 1.0. 17 Nov. 1997.http: //www.cs.york.ac.uk/ jac / papers / drareview.ps.gz, 1997.

4. Shannon K. A Mathematical Theory of Cryptography // Bell System Technical Memo MM 45-110-02, 1945

5. Shannon K. Communication Theory of Secrecy Systems // Bell System Technical Journal, 1949.

6. Panasenko S.P. Encryption algorithms. Special reference // BHV-Petersburg, 2009

7. Logachev OV, Salnikov A.A., Yashchenko V.V. "Cryptographic properties of discrete functions" // Proceedings of the conference "Moscow University and the development of cryptography in Russia". - M .: MCNMO. 2003 .-- S. 174-199

8. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography. Boca Raton, New York, London, Tokyo: CRC Press, 1997.780 p.

9. Cremers C. J. F., Lafourcade P. Comparing State Spaces in Automatic Security Protocol Verification. ETH Technical Report. 2007. No. 558.26 p.

10. Internet resource: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-022.

11. Venbo Mao. Modern Cryptography: Theory and Practice. - Publishing House "Williams", 2005. - ISBN 5-8459-0847-7.

12. Boyd C., Mathuria A. 5.3 MTI Protocols // Protocols for Authentication and Key Establishment — Springer-Verlag, 2003. — P. 147—155. — 321 p. — (Information Security and Cryptography) — ISBN 978-3-540-43107-7 — ISSN 1619-7100 — doi:10.1007/978-3-662-09527-0

СОВРЕМЕННЫЕ МЕТОДЫ СКРАПИНГА ИНФОРМАЦИИ С ВЕБ-САЙТОВ

Бобровский П.А.
email: p.bobrovskiy@aues.kz
Институт информационных технологий Алматинского университета энергетики и связи имени Гумарбека Даукеева, Казахстан

Аннотация. *В данной статье представлено описание такого понятия, как «веб-скрапинг», содержится информация о современных методы скрапинга информации с веб-ресурсов, а также будут приведены и проанализированы статистические данные на сегодняшний день.*

В данной статье будет описано само понятие «веб-скрапинг», современные методы скрапинга информации с веб-ресурсов, а также будут приведены и проанализированы статистические данные на сегодняшний день.

В широком смысле, термин «веб-скрапинг» можно объяснить, как технологию получения данных из сети Интернет путем извлечения их со страниц веб-ресурсов. Сбор информации с помощью любых средств, кроме программ, использующих API, или человека, использующего веб-браузер, является скрапингом. Общий принцип работы любого веб-скрапера можно описать следующим образом: вначале, с помощью автоматизированного кода выполняются GET-запросы на нужный сайт и получают ответы, затем происходит парсинг информации с документа HTML, и, в самом конце, происходит преобразование искомой информации в нужный формат. Данный процесс изображен в графическом виде на рисунке 1.

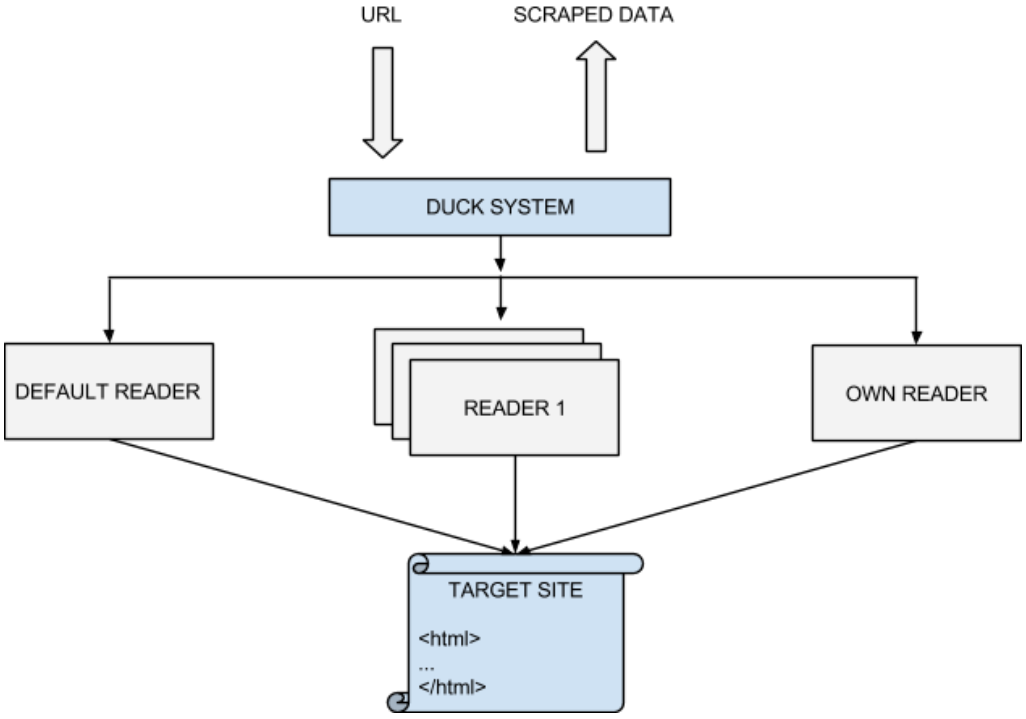


Рис. 1 Общий принцип работы веб-скрапера

Методы скрапинга можно разделить на 2 группы (рисунок 2): ручной (manual) и автоматизированный (automated).

Ручной веб-скрапинг подразумевает обычное копирование нужной информации со страниц сайта и последующая вставка и использование полученной информации. С одной стороны это трудозатратный процесс, требующий много усилий и частое повторение, но с другой стороны, если защитные механизмы сайта настроены только на обнаружение автоматизированных веб-скраперов, то в этом случае ручной скрапинг будет очень эффективным. Однако ручной веб-скрапинг на практике применяется очень редко, ввиду своей трудозатратности по времени и ресурсам.

Автоматизированные веб-скраперы представляют собой автоматизированный код, выполняющий парсинг веб-ресурса.

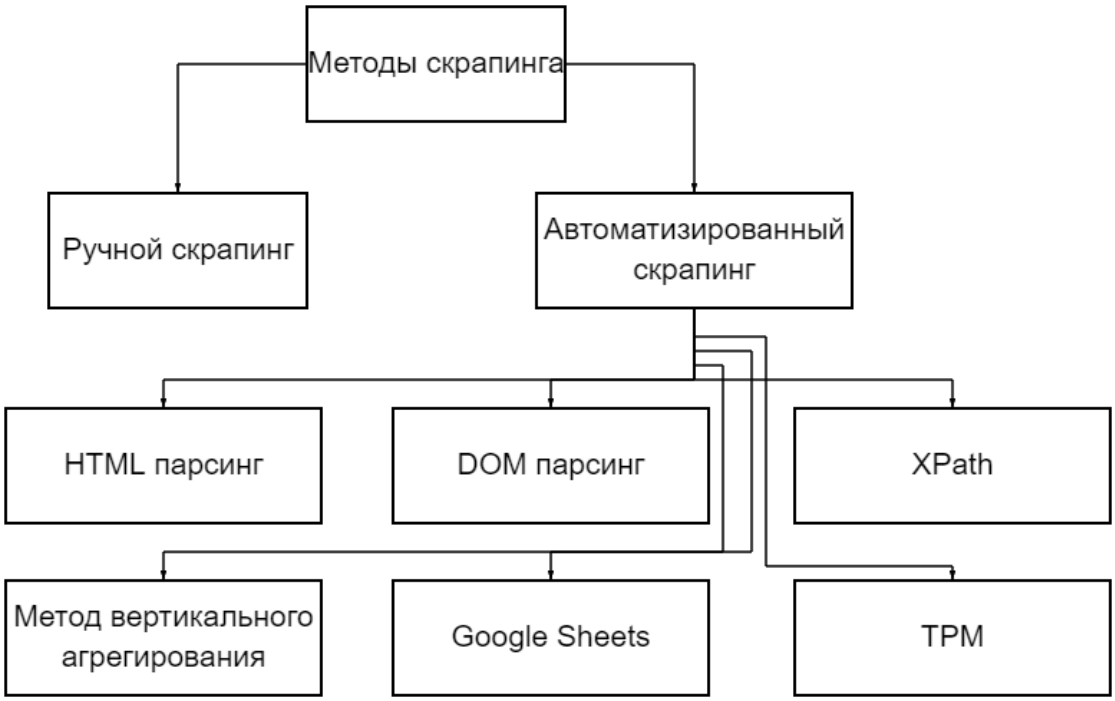


Рис. 2 Методы скрапинга

HTML парсинг выполняется с помощью JavaScript-кода и предназначен для линейных и/или вложенных HTML страниц.

DOM (Document Object Model) парсинг может определить стиль, структуру и содержимое в файлах XML. С помощью данного метода парсинга можно получить подробное представление о структуре веб-страницы. Метод DOM используется во многих браузерах, например в Internet Explorer или Firefox, для извлечения всей веб-страницы или только ее частей, даже если страница создана динамически.

Платформы, использующие метод вертикального агрегирования, создаются многими компаниями, которые имеют крупномасштабные вычислительные мощности. Также они используют данные платформы для сбора облачных данных. Эти платформы могут создавать и наблюдать за веб-роботами практически без вмешательства человека, их эффективность измеряется качеством извлеченных данных для определенной вертикали.

Следующая технология извлечения данных с веб-ресурсов называется XPath (XML Path Language). XPath это язык запросов, который работает с XML-документами. Ввиду древовидной структуры XML документов, XPath можно использовать для навигации по дереву, выбирая узлы на основе множества параметров. Немаловажным фактом является то, что XPath можно использовать вместе с DOM парсингом для извлечения всей веб-страницы и последующей публикации ее на целевом веб-сайте.

Google Sheets (Google страницы) также можно использовать для парсинга, и для этих целей это довольно популярный инструмент. Скрапинг данных происходит за счет одной единственной функции IMPORTXML(,). Также с помощью данной функции можно проверить любой сайт на защиту от кражи данных.

TPM (Text Pattern Matching – сопоставление текстового шаблона) – это метод сопоставления регулярных выражений, который использует команды UNIX grep. Данные команды широко применяются в автоматизированных веб-скраперах, написанных на таких языках программирования, как Python или Perl.

Если же говорить об общей статистике по веб-сайтам, подвергшимся различным веб-атакам злоумышленников, то их число растет с каждым годом. На рисунке 3 изображен график, показывающий нанесенный ущерб (в млн. долларов) от этих атак с 2009 по 2018 гг.

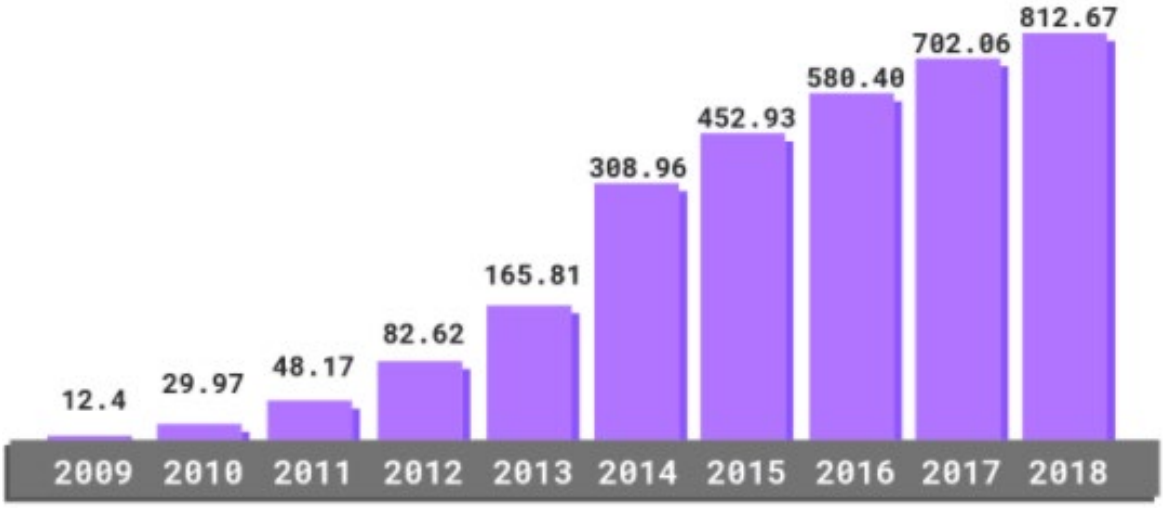


Рис. 3 Статистические данные по убыткам

Из-за такого быстрого роста появляется необходимость в развитии и финансировании области кибербезопасности во всем мире, что влечет за собой постоянно растущие ежегодные расходы в этой области. Данные тенденции представлены на графике, который изображен на рисунке 4.

Рис. 4 Статистические данные по финансированию в области кибербезопасности

Но несмотря на такое обилие методов парсинга и веб-скраперов, существует достаточное количество методов и утилит, предотвращающих сбор информации злоумышленниками. Ниже будут описаны самые действенные из них.

Использование CSRF токенов. CSRF токен – это уникальный идентификатор, отправляемый клиенту (браузеру) через веб-сервер. Клиент же в свою очередь должен обратно отправить этот токен во время следующего обращения к веб-серверу, а веб-сервер не будет отвечать на запросы, в которых отсутствует правильный CSRF токен. Это является очень эффективной защитой для любого веб-ресурса.

Использование специального программного обеспечения также является эффективным способом избежать кражи данных. Данное ПО использует методы машинного обучения для определения активности веб-скраперов путем измерения скорости, с которой пользователь заполняет поля и формы, то, как перемещается курсор по странице и с какой скоростью и частотой открываются определенные разделы веб-ресурса, кратко говоря, любая нечеловеческая деятельность будет заблокирована.

Также эффективным способом является ограничение количества запросов на страницах. Обычно эти ограничения делаются на количество запросов и загрузок по IP адресу.

Подводя итог всему вышенаписанному, можно с уверенностью сказать, что веб-скрапинг представляет ощутимую угрозу, не только для компаний-гигантов, малого и среднего бизнеса, но и для обычных пользователей. Т.к. под угрозу ставится самая ценная на сегодняшний день вещь – информация.

Литература

1. *Митчел Р.* Скрапинг веб-сайтов с помощью Python. - М.: ДМК Пресс, 2016. - 280 с.: ил.

2. *Митчел Р.* Современный скрапинг веб-сайтов с помощью Python. 2-е межд. издание. - СПб.: Питер, 2021. - 336 с.

3. *Aydin O.* R Web Scraping Quick Start Guide. 2018. – 114 с.

4. *О'Нил К., Шатт Р.*: Data Science. Инсайдерская информация для новичков. Включая язык R. – СПб.: Питер-Трейд, 2018. – 368 с.

АНАЛИЗ АТАК НА WEB-РЕСУРСЫ

Смагулов Р.Б.; Усатова О.А., PhD,
e-mail: yorozuya667@gmail.com, uoa_Olga@mail.ru.
Казахский национальный университет им. аль-Фараби, Казахстан, Алматы

Аннотация

В данной статье рассматриваются наиболее распространенные виды сетевых атак. Производится аналитическое исследование процентного соотношения целей сетевых атак и атак на web-ресурсы

Ключевые слова: сетевые атаки, виды атак, защита информации, цели сетевых атак.

Введение

XXI век – век бурного развития информационных технологий. Но не все сферы информационных технологий развиваются одинаково и синхронно. Зачастую, некоторые компоненты информационных систем не поспевают за другими. В данном случае речь идет о компоненте, отвечающим за безопасность программного обеспечения и связанных с ним ресурсов.

Вместе с развитием IT-технологий, и следующее с ним распространение web-ресурсов порождает множество проблем, которые связаны с ними:

1. Сама структура Сети, конечно, является крайне удобной для приема-передачи информации, но, вместе с тем, удобна и для передачи файлов, представляющих опасность с точки зрения информационной безопасности. Скорость развития сетевых коммуникаций только помогает злоумышленникам быстрее распространить зараженные файлы и прочее вредоносное программное обеспечение. Последствия могут быть катастрофичны, ценные данные могут быть украдены, искажены, заблокированы или вовсе уничтожены. Также подобного рода вредоносные файлы могут препятствовать работе рабочих машин и иных станций или привести к полной потери работоспособности последних.
2. Сеть представляет собой один из главных каналов утечки конфиденциальных данных, коммерческой тайны и иных данных, не допускающих бесконтрольного распространения и доступа для третьих лиц. Один из простейших примеров – почтовая система с недостаточной или полностью отсутствующей защитой от атак. Заражение данной системы может не только дать возможность взломщику доступ к данным на компьютере-клиенте, но и распространить вирусное программное обеспечение по всей системе. Заражение почтового сервера будет еще более сильным ударом по системе информационной безопасности. Стоит только ознакомиться со статистикой использования почты сотрудниками, например, в обычном офисе.
3. Невозможно найти современное программное обеспечение или программно-аппаратный комплекс, не имеющие недостатков с точки зрения информационной безопасности, простыми словами, нет систем без уязвимостей. Причины появления подобного рода уязвимостей различны. Начиная от ошибок при разработке, к примеру, программного обеспечения, а именно на этапе его проектирования, реализации кода, заканчивая банальными ненадежными паролями

и прочими ошибками, допущенными пользователями и разработчиками. Кроме того, уязвимости могут появиться и на более поздних этапах не только разработки ПО, но и при дальнейшем использовании и обновлении. А использование специальных программных средств может создать уязвимость, при отказе системы защиты или иных причин, понижающих степень защищенности системы.

4. Хоть эксплуатация web-ресурсов несет за собой риски, на данный момент не представляется возможным отказаться от использования этих ресурсов, потому как огромное количество данных создается, передается и используется при помощи вышеназванных ресурсов. В зависимости от типа, назначения и способа разработки web-ресурсов, разнятся и способы атаки на них. Для каждого типа основных атак существуют соответствующие способы защиты [9].

Цели сетевых атак и мотивы злоумышленников

Безусловно, различного рода информация имеет свою ценность. К особым видам информации принято относить закрытую информацию, а именно, конфиденциальные данные, коммерческая и государственная тайны и тому подобное.

Начиная с личных данных пользователей, заканчивая критически важной информации стратегического значения – вся информация может быть скомпрометирована, изъята, искажена или просто уничтожена. Шантаж личной информацией человека, кража чертежей новых разработок, раскрытие инсайдерской информации, касающейся финансовых структур, вмешательства политического характера, разведка на государственном уровне. Это, естественно, неполный список целей сетевых атак [5].

Более подробная статистическая информация в развернутом виде отразится в следующей главе. В этой же следует остановиться на мотивах злоумышленников. Мотивы имеют тесную связь с целями. Статистические данные взяты из Positive Technologies. Если взять для анализа предыдущий год, для удобства последний квартал, то можно заметить заявленную ранее тенденцию к увеличению доли атак на организации. Доля этого метода выросла на 6 процентных пунктов. 8 из 10 атак в прошлом квартале носили целенаправленный характер. В атаках на частных лиц замечен резкий всплеск социальной инженерии (доля выросла с 67% до 85%) [10]. Отдельно нужно будет отметить, что на данный тренд повлияла пандемия COVID-19, встревоженность части населения привела к менее разумной оценке некоторых потенциальных угроз в информационной сфере. Чем, конечно, воспользовались злоумышленники. По большей части это относится к социальной инженерии, но даже при данном способе получения или искажения, кражи информации, активно используются сетевые ресурсы как инструмент для подобного рода атак, или, по крайне мере, как среда для проведения атак.

Тем не менее, как и обычно, превалирующим мотивом у злоумышленников является получение данных. Неизменным спросом в атаках на организации пользуются персональные данные и коммерческая тайна. Атакуя частных лиц, злоумышленники чаще всего крадут сведения для аутентификации и персональные данные. Количество инцидентов в IV квартале 2020 года в сравнении с предыдущим кварталом увеличилось на 3,1%. По сравнению с аналогичным периодом 2019 года прирост составил 41,2% [9]. Как известно, скомпрометированные данные могут быть использованы в различных целях. В лучшем случае раскрытие закрытой информации может быть хулиганским актом с целью привлечения внимания или вымогательства, в худшем это может быть утечка критической информации, которая может быть крайне опасна для ее владельца. В обычных нежелательных ситуациях,

связанных с утечкой данных частных лиц, высока вероятность столкнутся с шантажом и вымогательством. На уровне организаций и предприятий среднего бизнеса существует риск утечки информации о транзакциях, клиентах, контрагентов вплоть до коммерческой тайны. На уровне транснациональных корпораций и государств раскрытие или искажение данных могут иметь не только тяжелые финансовые и политические последствия, но и могут стать причиной крупных кризисов различного рода. Стоит вспомнить раскрытие инсайдерской информации на рынке ценных бумаг или недавнее вмешательство в выборы президента США.

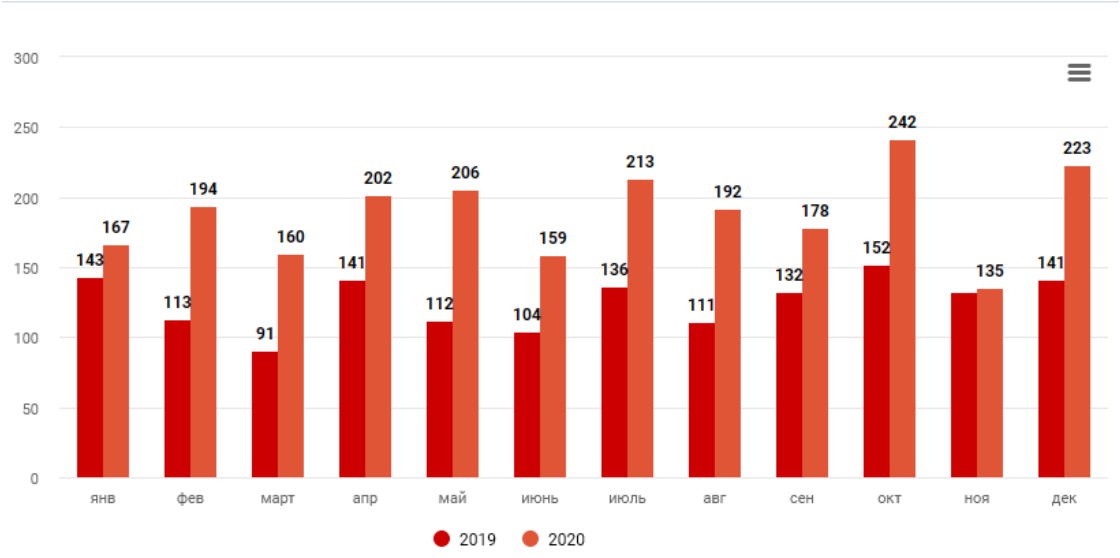


Рисунок 1 - Количество инцидентов в 2019 и 2020 годах (по месяцам)

Из Рис.1 видно, что общее количество атак увеличивается, то есть наблюдается четкая тенденция к росту. Рост наблюдается не только в атаках на организации, но также и на частные лица. Некоторые виды атак на организации можно зафиксировать во время отчетных периодов или иных отрезках времени, где собирается и упорядочивается самими организациями важная финансовая информация.

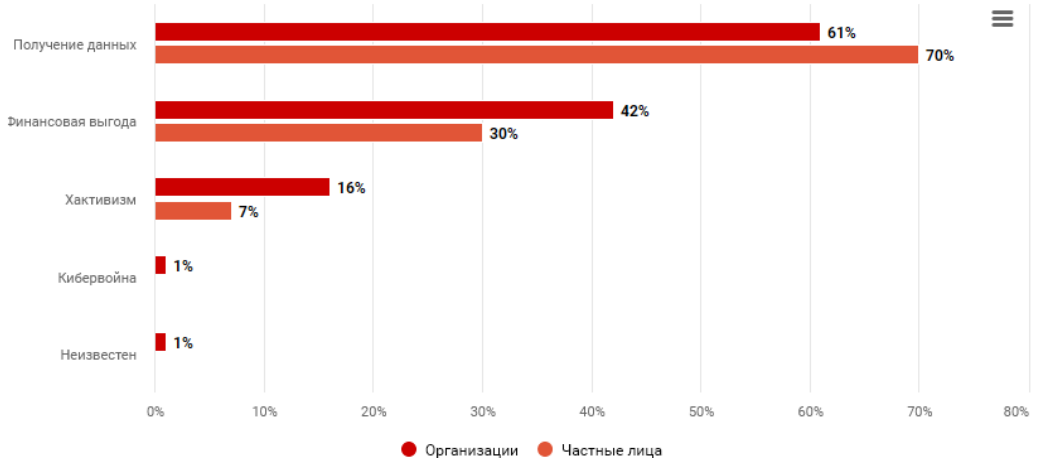


Рисунок 2 – Мотивы злоумышленников (доля атак)

На Рис.2 можно увидеть, что доля атак не сильно изменилась, по сравнению с прошлым годом, или кварталами ранее. Единственное, как и было отмечено ранее, можно зафиксировать рост атак на частных лиц именно для получения данных.

Способы атак на Web-сервисы

Наиболее распространенными объектами злоумышленников являются Web-приложения, так как они используются в огромном количестве организаций как наиболее критичные ресурсы, цель которых – обеспечивать непрерывную поддержку многомиллионных транзакций. Не лишним будет заметить, что вторжения на сетевые ресурсы могут повлечь за собой так называемое заражение клиентов, которое, в свою очередь, непосредственно связано с сервером.

На Рис.3 представлены основные виды атак на Web-ресурсы.

Рисунок 3 – Виды атак на web-ресурсы

Довольно отчетливо можно наблюдать, что межсайтовое выполнение сценариев и внедрение SQL-кода все еще являются действенными методами. Несмотря на то, что данные методы нельзя назвать новыми, они все еще остаются актуальными.

Важной особенностью, которую стоит отметить, является доля успешных атак и их связь с не изученными новыми методами, точнее, это 11%, то есть именно эта долю всех успешных атак составляют неизвестные ранее методы. Это связано как с неэффективным мониторингом атак, так и с нежеланием жертв раскрывать данные об успешных атаках [3].

При этом большинство сетевых атак на сетевые ресурсы непосредственно связаны с неверной настройкой самих Web-серверов, либо недостаточное внимание к обновлению и поддержанию систем в рабочем виде в соответствии с постоянно меняющимися условиями. Далее будет дано подробно описание таких атак [8].

К подобного рода атакам можно отнести:

- Атаки, которые эксплуатируют недостаточную аутентификацию — уязвимость подобного рода появляется в тот момент, когда web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной на то аутентификации.

• Атаки на клиентов сервера, учитывающие доверительные отношения между сервером и клиентом (пользователем) – то есть пользователь ожидает, что сайт предоставит ему легитимное содержимое, и не ожидает атак со стороны сайта:

▪ Межсайтовое выполнение сценариев (англ. Cross-site Scripting, XSS) — один из самых распространенных способов атаки на сетевые ресурсы, который дает возможность атакующему передать серверу исполняемый код, далее этот код будет перенаправлен браузеру конечного пользователя. Уникальность подобного способа атаки заключается в том, что вредоносный код может использовать авторизацию пользователя в веб-системе для получения к ней расширенного доступа или для получения авторизационных данных пользователя. Вредоносный код может включен в страницу как через уязвимость в веб-сервере, так и через уязвимость на компьютере пользователя. Для термина используют сокращение «XSS», чтобы не было путаницы с каскадными таблицами стилей, использующими сокращение «CSS». XSS находится на лидирующих позициях в рейтинге ключевых рисков. Кроме того, межсайтовый скриптинг может быть использован для проведения DoS-атаки [1];

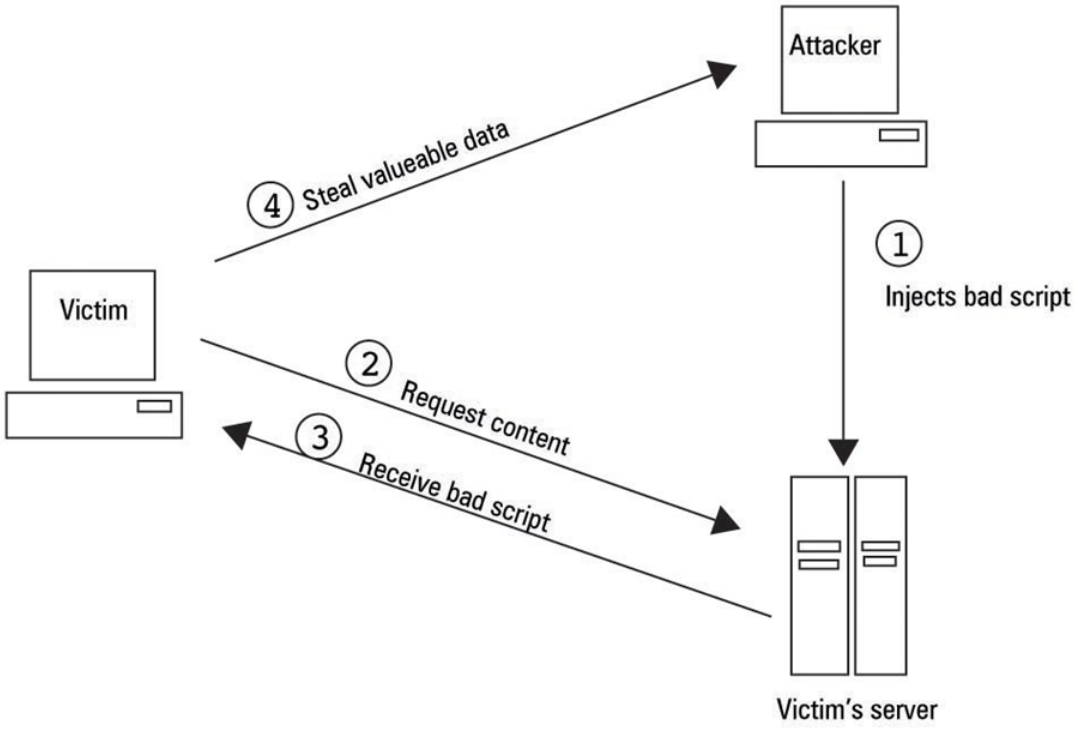


Рисунок 4 – Схема работы XSS-атаки

▪ Подмена содержимого. В данном типе атаки злоумышленник заставляет конечного пользователя поверить, что полученные страницы сгенерированы оригинальным web-сервером, а не загружены из неизвестного внешнего источника [6].

▪ Межсайтовая подделка запросов (англ. Cross-Site Request Forgery, CSRF) – уязвимость, являющаяся аналогичной уязвимости XSS, направленная на то, что браузер пользователя не проверяет источник запроса. CSRF – это вариант

Межсайтового выполнения сценариев (XSS).

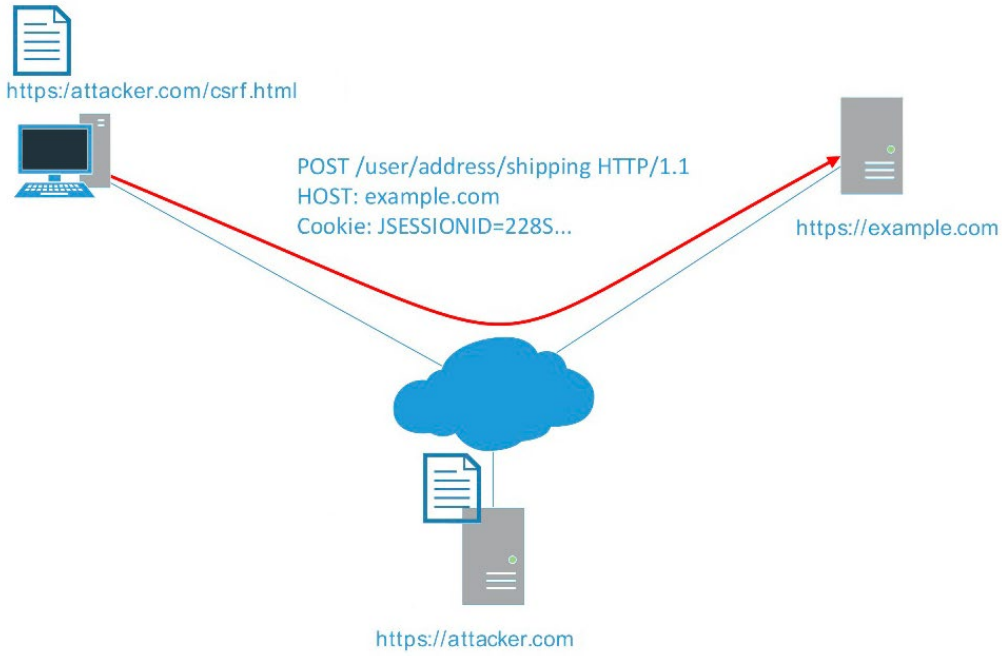


Рисунок 5 – Схема действия метода XSS

Сделав небольшой анализ этих способов можно отследить определенное сходство между CSRF и XSS, это использование в качестве вектора атаки клиентов сетевых приложений (Client-Side Attack в терминологии WASC). Уязвимости типа CSRF могут эксплуатироваться совместно с XSS или редиректорами, но представляют собой отдельный класс уязвимостей.

Уязвимость CSRF мало распространена и очень сложна в использовании.

Вновь обратимся к источнику Positive Technologies. Данные, полученные в ходе работ по пентестингу и оценки защищенности Web-приложений наглядно отображают, что этой уязвимости подвержена большая часть Web-приложений. В отличие от других уязвимостей CSRF возникает не в результате ошибок программирования, а является нормальным поведением Web-сервера и браузера. Т.е. большинство сайтов, использующих стандартную архитектуру уязвимы «по умолчанию» [10].

- Атаки, направленные на выполнение кода на web-сервере. В частности, внедрение операторов SQL (англ. SQL Injection) – эти атаки направлены на web-серверы, создающие SQL запросы к серверам СУБД на основе данных, вводимых пользователем [7].
- Атаки, направленные на эксплуатацию функций приложения или логики его функционирования:
  - Отказ в обслуживании (англ. Denial of Service, DoS) – данный класс атак направлен на нарушение доступности web-сервера Большинство DDoS-атак используют уязвимости в основном протоколе Internet (TCP/IP), а именно, способ обработки системами запросаSYN. Выделяют два основных типа атак, которые

вызывают отказ в обслуживании. В результате проведения атаки первого типа, останавливается работа всей системы или сети. Хакер отправляет системе данные или пакеты, которые она не ожидает, и это приводит к остановке системы или к ее перезагрузке. Второй тип DDoS-атаки приводит к переполнению системы или локальной сети при помощи огромного количества информации, которую невозможно обработать. DDoS-атака заключается в непрерывном обращении к сайту со многих компьютеров, которые расположены в разных частях мира. В большинстве случаев эти компьютеры заражены вирусами, которые управляются мошенниками централизовано и объедены в одну ботсеть. Компьютеры, которые входят в ботсеть, рассылают спам, участвуя, таким образом, в DDoS-атаках [2].

- Недостаточное противодействие автоматизации – эти уязвимости возникают в случае, если сервер позволяет автоматически выполнять операции, которые должны проводиться вручную, например, ручной ввод пароля пользователя с запретом автоматического подбора, также называемый методом грубой силы (англ. Brute Force) [4].

Из вышеописанного можно сделать вывод, что большинство сетевых атак на web-серверы можно предотвратить с помощью правильного конфигурирования их настроек согласно соответствующим требованиям. При этом существует и будут создаваться новейшие способы атак и обхода ограничений, которые не блокируются основными превентивными мерами. Исходя из этого стоит считать задачу защиты от сетевых атак рабочих станций и серверов как одну из самых важных и критических.

Заключение

В данной статье были затронуты основные моменты, касающиеся атак на web-ресурсы, а именно, статистика по теме, основные виды и методы атак на сетевые ресурсы. Конечно, кроме самых распространенных видов атак и методах защиты, существуют и в настоящий момент разрабатываются способы обхода защитных мер, поиск ранее незамеченных уязвимостей и глубокий анализ новейших разработок и сервисов.

Взглянув на тему с точки зрения обеспечения безопасности в Казахстане, следует сделать акцент на активной цифровизации различных сфер жизни. В рамках государственной программы «Цифровой Казахстан» в республике активно происходит процесс внедрения IT-инфраструктуры, а вместе с этим также сетевых ресурсов и сервисов. Столь широкое развитие цифровой сетевой инфраструктуры кроме несомненных плюсов несет за собой серьезные требования, не только к обеспечению бесперебойной работы данных систем, но и гарантированной защиты персональных данных, конфиденциальной информации и прочих закрытых данных. Интеграция в нашу жизнь новейших информационных систем на государственном уровне требует исключительной внимательности к построению и поддержанию защищенности жизненно важных структур. Столь быстрое развитие сетевых ресурсов обуславливает не менее быстрое создание решений в области информационной безопасности.

Анализ самых распространенных типов атак позволяет сделать выводы относительно состояния защищенности сетевых ресурсов на сегодняшний день и может внести некоторые корректировки в планирование систем защиты с учетом ошибок при проектировании. Не лишним будет отметить, что самые эффективные и критические с точки зрения последствий будут те уязвимости систем и ресурсов, которые были вовремя не обнаружены в самом начале разработки. Но также нельзя

забывать о том, что вместе с динамичным развитием средств защиты будут создаваться новые методы обхода ограничительных мер. Поэтому на повестке дня вопрос защищенности web-ресурсов будет не менее важным чем любые другие.

Литература

1. Жуков Ю.В. Основы веб-хакинга: нападение и защита, – СПб.: Питер, 2012г.
2. Ревенков П.В., Бердюгин А.А. Кибербезопасность в условиях Интернета вещей и электронного банкинга // Национальные интересы: приоритеты и безопасность, – 2016г., https://cyberleninka.ru/article/v/kiberbezopasnost-v-usloviyah-interneta-veschey-i-elektronnogo-bankinga
3. Positive Technologies. // Статистика и аналитические данные [Электронный ресурс], – 2021г., https://www.ptsecurity.com/ru-ru/
4. Гордейчик С. // Cross-site request forgery [Электронный ресурс], – http://www.securitylab.ru/analytics/292473.php
5. Щеглов А.Ю., Защита компьютерной информации от несанкционированного доступа, – СПб: Наука и Техника, 2004г.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков // «Информационная безопасность и защита информации», – 2009г.
7. В.Ф. Шаньгин // «Информационная безопасность компьютерных систем и сетей», – 2008г.
8. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы, – 2014г.
9. А.А. Гладкий // «Безопасность и анонимность работы в Интернете. Как защитить компьютер от любых посягательств извне» – 2012г.
10. Портал о информационной безопасности [Электронный ресурс], – https://intsystem.org

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ ПРИМЕНИТЕЛЬНО К АУТЕНТИФИКАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Бегимбаева Е.Е.[1], Нурманов А.Б.[2], Усатова О.А.[1], Усатов Н.С.[3]
email: enlik_89@mail.ru, a.nurmanov1998@gmail.com, uoa_olga@mail.ru, usatov.nikita2242@gmail.com

[1] Институт информационных и вычислительных технологий МОН РК, Казахстан
[2]Казахский национальный университет им. Аль-Фараби, Казахстан
[3]Университет «Туран», Казахстан

Аннотация. *В данной статье рассматриваются возможности применения механизма электронной цифровой подписи (ЭЦП) для аутентификации в информационных системах с небезопасными каналами связи. Предполагаемая система аутентификации будет строиться на инфраструктуре открытых ключей (PKI), в которой каждый из пользователей владеет парой открытого и закрытого ключа. В статье рассмотрены этапы становления цифровой подписи как международного стандарта, современные тенденции, проблемы и методы их решения. Так же анализу подвергается социокультурное значение цифровых подписей и их актуальность на сегодняшний день. Подобные схемы аутентификации, построенные на цифровых подписях, обеспечивают более высокий уровень доверительных отношений как между клиентом и сервером, так и между участниками системы. Сегодня нельзя представить безопасный интернет без них.*

Введение

Современный мир представляет из себя огромное информационное поле, внутри которого циркулируют массивные потоки разнородных данных. Для упорядочивания, классификации и индексирования таких объемов данных используются механизмы оцифровывания, которые заключаются в том, что вся входная информация преобразуется в электронный вид для ее последующего хранения на электронных носителях.

В настоящее время человеческих ресурсов для обработки большого потока информации недостаточно, поэтому крупные бизнес-компании, банки, военные предприятия и государства все чаще внедряют автоматизированные системы управления для работы с такой информацией. Одним из таких ярких примеров является система электронного документооборота, которая в добровольно-принудительном порядке внедряется в различных компаниях под надзором государства. Однако возникают проблемы связанные с проверкой подлинности, аутентичности и целостности этих данных.

Электронная цифровая подпись – это математическая схема для верификации аутентичности и целостности цифровых сообщений и документов [1]. Наличие правильной цифровой подписи, в которой соблюдены все криптографические требования, позволяет получателю удостовериться, в том, что сообщение было составлено и отправлено проверенным отправителем (аутентичности) и что оно не было модифицировано во время передачи (целостности).

Цифровые подписи являются современным стандартом информационной безопасности для многих электронных систем и часто используются как стандартные элементы многих современных криптографических протоколов. Они применяются при распространении программного обеспечения, для подтверждения финансовых транзакций, для подписи документов, для получения государственных услуг, а также во всех остальных случаях, когда необходимо обнаружить подмену или изменение исходного сообщения во время передачи по небезопасному каналу связи.

В некоторых странах использование цифровой подписи закреплено на законодательном уровне. Среди них: Южная Африка [2], Канада [3], Индия [4], Саудовская Аравия [5], Республика Казахстан [6] и др.

Появление электронного правительства и электронных услуг изменило способ работы государственных агентств и органов местного самоуправления. Электронное правительство или цифровое управление в целом определяет использование новых коммуникационных технологий и информационных приложений центральной и местной публичной администрацией с целью упорядочения деятельности административного аппарата и повышения качества государственных услуг. Цифровые подписи были введены для полной замены традиционных подписей и, как следствие, для удаления бумаги из повседневных процессов, таких как подписание контрактов, интеграция новых клиентов или юридическая регистрация. Конечная причина, по которой компании интегрируют цифровые подписи — это возможность проводить бизнес-транзакции любого типа в любом месте и в любое время на любом устройстве [7].

Так как ЭЦП являются цифровыми, то любое электронное сообщение, которое можно представить в виде потока байтов, может быть подписано и отправлено по сети. Например, электронная почта, контракты, договоры, сообщения, изображение, видео и т. д.

1. История создания электронной цифровой подписи

Даже если создается ложное впечатление о том, что технология цифровой подписи — это новая и непроверенная тенденция, важно понимать, что они существуют уже несколько десятилетий и становятся все более популярными.

Важнейшими этапами в истории становления цифровой подписи являются:

- 1976: Уитфилд Диффи и Мартин Хеллман впервые описали идею схемы цифровой подписи, но только предположили, что такие схемы существуют [8];
- 1977: Рональд Ривест, Ади Шамир и Лен Адлеман изобрели алгоритм RSA, который можно было использовать для создания цифровой подписи [9];
- 1984: Шафи Гольдвассер, Сильвио Микали и Рональд Ривест стали первыми, кто строго определил требования безопасности схем цифровой подписи [10];
- 1988: Lotus Notes 1.0, в котором использовался алгоритм RSA, разработал первый широко продаваемый программный пакет, предлагающий цифровые подписи [11];
- 1999: добавлена возможность встраивать электронные подписи в документы в формате PDF [12];
- 2000: Закон ESIGN - закон, который делает цифровые подписи юридически обязательными [13];

- 2002: основана компания SIGNiX, которая становится наиболее часто используемым программным обеспечением для цифровой подписи на основе облака;

Формат файла PDF становится открытым стандартом международной организации по стандартизации (ISO) как ISO 32000. Он включает цифровые подписи как неотъемлемую часть формата [14].

Некоторые из существующих алгоритмов цифровой подписи [15]:

- RSA.
- DSA.
- ECDSA.
- RSA/SHA.
- ECDSA/SHA.
- Схема подписи Эль-Гамаля.
- Алгоритм подписи Рабина.
- BLS (Boneh–Lynn–Shacham).
- Неотказуемая подпись.
- Агрегированная подпись.

2. Электронная цифровая подпись и ее социокультурные аспекты

Считается, что традиционные подписи не будут полностью заменены цифровыми подписями с учетом их ограничений. Эти ограничения включают в себя, например, проблемы с долгосрочным хранением, износ связанного носителя данных, устареванием формата данных и развитием криптографических алгоритмов, связанных стандартов и проверки сертификатов.

Прежде чем цифровые подписи будут преобладать, в цифровые подписи необходимо включить соответствующее чувство культуры с точки зрения принятия пользователями, долгосрочной стабильности и надежности.

Например, культура печатей в Японии [16] считается подходящей для внедрения цифровых подписей, поскольку концепции сертификатов печати и электронных сертификатов сопоставимы.

3. Назначение и использование электронной цифровой подписи

Электронно-цифровая подпись выполняет следующие функции:

- обеспечение целостности документа. Если при передаче электронного документа он был изменен, электронная подпись автоматически становится недействительной. Это связано с тем, что электронная подпись формируется на основе первой версии подписанного документа;

- правильное подтверждение автора. В документе, подписанном электронной цифровой подписью, автор не может быть изменен. Таким образом, наличие цифровой подписи под документом гарантирует личность владельца подписи;

- предоставление доказательств. Чтобы подтвердить наличие функциональной цифровой подписи, автору нужно только предоставить открытый и закрытый ключи, которые он получает при создании электронной цифровой подписи.

Исходя из этого, можно сделать вывод, о том, что цифровая подпись обеспечивает высокую степень защиты данных, что чрезвычайно важно в современных реалиях цифрового шпионажа и существовании различных методов перехвата данных.

Именно поэтому такие подписи уже используются в банковских системах, при государственных закупках, при регистрации недвижимости, в судебной системе, в торговых системах, в таможенных декларациях и во многих других сферах человеческой деятельности.

Однако нельзя не упомянуть важную особенность - документы, подписанные электронным способом, имеют юридическую силу и признаются эквивалентными бумажным документам только в том случае, если они защищены законодательной базой или оформляются по соглашению сторон.

На рисунке 1 изображена упрощенная схема генерации электронно-цифровой подписи, где Алиса подписывает сообщение «Привет Боб!», добавляя к исходному сообщению контрольную сумму, зашифрованную ее закрытым ключом. Боб получает и сообщение, и подпись. Он использует открытый ключ Алисы для проверки подлинности сообщения, то есть того, что сообщение, дешифрованное с помощью открытого ключа, точно соответствует исходному сообщению.

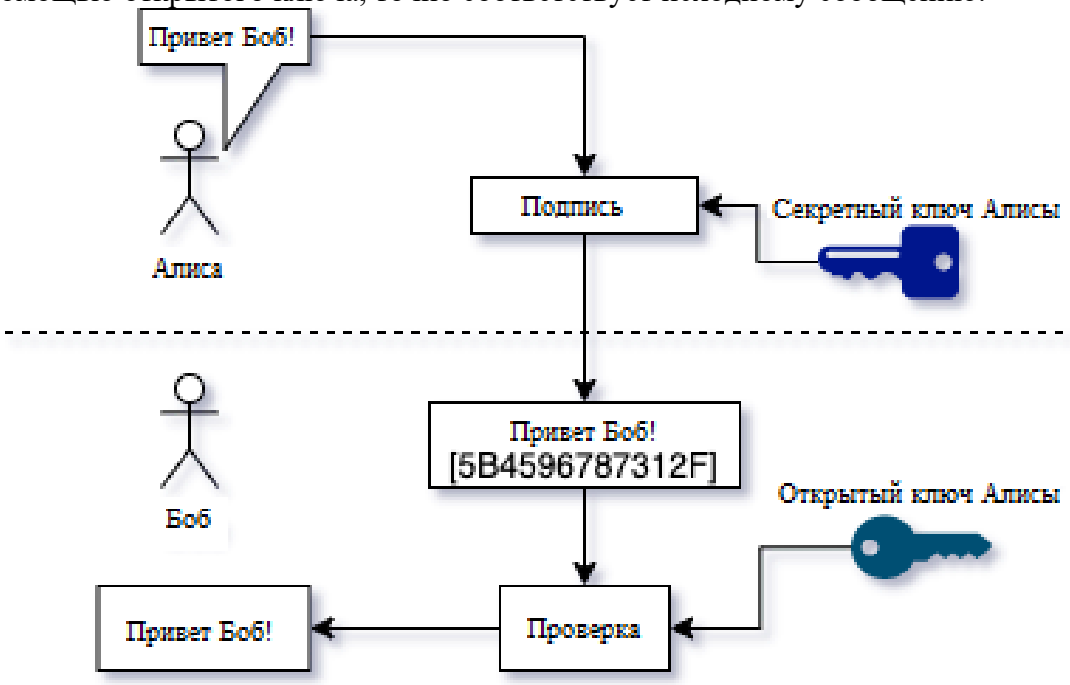


Рисунок 1 – Схема генерации цифровой подписи электронного сообщения

Решения для цифровой подписи быстро заменяют бумажные подписи и могут доминировать в процессах, связанных с формированием подписей. Основные преимущества этой технологии включают повышение эффективности, снижение затрат и большее удовлетворение потребностей клиентов.

Цифровые подписи необходимо четко отличать от обычных процессов аутентификации. Хотя аутентификация используется только для проверки личности конечных пользователей, цифровые подписи также обеспечивают целостность данных. Сочетание этих двух факторов безопасности важно для многих бизнес-транзакций, особенно для тех, которые связаны с конфиденциальными данными [17].

Цифровые подписи — это подкатегория электронных подписей. В то время как электронная подпись может представлять собой любые данные, прикрепленные к документу, например, имя, написанное под электронным письмом, цифровая подпись основана на математическом процессе защиты документа. Она включает в

себя три последовательных процесса: процесс подписи, процесс аутентификации и процесс проверки целостности данных.

Процесс создания цифровой подписи одинаков как для внутреннего, так и для внешнего администрирования. Процесс формирования подписи начинается с предоставления конечному пользователю необходимого документа.

4. Преимущества, проблемы и стратегии развития

Чтобы убедиться в том, что человек подписывает документ правильно, личность конечного пользователя проверяется с помощью множественной аутентификации, такой как PIN-код, пароль и токен-коды, генерируемые на основе случайной последовательности. После подтверждения личности подписавший получает сертификат, подтверждающий его личность и предоставляющий ему пару ключей: закрытый ключ (известный только подписавшему) и открытый ключ (известный всем). Эти ключи необходимы для подписи документа и подтверждения личности подписавшего. После выдачи сертификата из документа создается уникальный математический код. Затем этот математический код шифруется закрытым ключом (подписывается) и может быть расшифрован только с помощью соответствующего открытого ключа (проверка подписи). Затем документ, вместе с зашифрованным математическим кодом, отправляется получателю.

Чтобы гарантировать подлинность, получатель, с доступом к открытому ключу, может расшифровать математический код и, следовательно, может гарантировать подлинность. Открытый ключ работает для расшифровки только в том случае, если документ был подписан соответствующим закрытым ключом, уже подтверждающим личность подписавшего.

Целостность данных обеспечивается математическим кодом, который после расшифровки виден получателю. Чтобы убедиться, что документ не был изменен каким-либо неуполномоченным лицом, получатель вычисляет свой собственный математический код для документа. Если оба кода совпадают, то целостность данных не была нарушена, но если бы документ был изменен при передаче, то получатель получил бы совершенно другой код.

Заключение

Технология цифровой подписи будет присутствовать во многих сферах нашей повседневной жизни, связанных с конфиденциальностью.

Технологии повышают эффективность бизнеса и сокращают расходы, и они будут все чаще использоваться в качестве средства коммуникации деловыми партнерами, клиентами и государственными органами.

Для каждой относительно новой технологии необходимо преодолеть такие препятствия, как простота интеграции и согласования с существующими рабочими процессами, расчет бизнес-модели, а также отсутствие прозрачности и часто непонимание правовой ситуации.

Регламент РК способствует общей юридической силе, а также принятию законных решений. Уже есть многообещающие признаки того, что власти и отрасль поставщиков преодолевают эти проблемы.

Поскольку рынок требует быстрой окупаемости инвестиций и решения, упрощающего рабочий процесс, ожидается, что в будущем полные или частичные облачные решения займут основную долю рынка решений для цифровой подписи.

Те, кто осознают потенциал таких решений, смогут создать значительное экономическое преимущество, а также лучше поддерживать и расширять свою клиентскую базу благодаря большему удобству этих решений.

Литературы

1. Digital signature // https://searchsecurity.techtarget.com/definition/digital-signature (07.05.2021).
2. Electronic Communications and Transactions Act, No. 25. - 2002 // https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.
3. Secure Electronic Signature Regulations SOR/2005-30 // https://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-30/FullText.html (07.05.2021).
4. The information technology act, 2000 (No. 21 OF 2000) // https://dot.gov.in/sites/default/files/itbill2000_0.pdf (07.05.2021).
5. Electronic Transactions Law // https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/ElectronicTransactionsLaw.aspx (07.05.2021).
6. Закон РК Об электронном документе и электронной цифровой подписи, утв. от 7 января 2003 года № 370-II.
7. Electronic and Digital Signatures //https://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ElectronicandDigitalSignatures-v5-march2012_000.pdf (07.05.2021).
8. W. Diffie, M. Hellman New directions in cryptography // IEEE Transactions on Information Theory September 2006 https://doi.org/10.1109/TIT.1976.1055638 (07.05.2021).
9. R.L. Rivest, A. Shamir, and L. Adleman A Method for Obtaining Digital Signatures and Public-Key Cryptosystems https://people.csail.mit.edu/rivest/Rsapaper.pdf.
10. A digital Signature Scheme secure against adaptive chosen-message attacks // https://people.csail.mit.edu/rivest/GoldwasserMicaliRivest-ADigitalSignatureSchemeSecureAgainstAdaptiveChosenMessageAttacks.pdf.
11. Lotus Notes 1.0 // https://www.angioni.nl/index.php/2016/12/11/lotus-notes-the-beginning/ (07.05.2021).
12. Digital Signatures in a PDF // https://www.adobe.com/devnet-docs/etk_deprecated/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf.
13. The Electronic Signatures in Global and National Commerce Act (E-Sign Act) // https://www.fdic.gov/regulations/compliance/manual/10/X-3.1.pdf.
14. ISO 32000-2:2020 Document management — Portable document format — Part 2: PDF 2.0 // https://www.iso.org/standard/75839.html (07.05.2021).
15. Digital signature // https://en.wikipedia.org/wiki/Digital_signature.
16. V. Liu, W. Caelli, E. Foo, S. Russell Visually Sealed and Digitally Signed Documents // https://www.researchgate.net/publication/27464718_Visually_Sealed_and_Digitally_Signed_Documents.
17. An Introduction to Digital signatures For the AEC Industry // https://www.globalsign.com/en/resources/digital-signatures-for-aec-guide.pdf.

РАДИОЧАСТОТНОЕ ПОДАВЛЕНИЕ СИГНАЛОВ С ЛЧМ

Косяков И.О.
e-mail: heimmdal@mail.ru
Академия КНБ, Казахстан

Аннотация. *В докладе приводится информация о методах радиочастотного подавления сигналов с ЛЧМ, которые применяются в стандарте LoRa. Данный стандарт применяется для организации низкоскоростной передачи небольших объёмов данных в IoT. Доклад будет полезна специалистам в области информационной безопасности и связи.*

Сигналы с ЛЧМ (линейно-частотной модуляцией) в настоящее время применяются в стандарте интернета вещей LoRa. Также данные сигналы имеют широкое распространение в условиях где требуется стабильная передача небольшого количества информации в течении довольно длительного промежутка времени. ЛЧМ, в частности, в стандарте LoRa позволяет добиться высоких результатов помехоустойчивости и стабильности передачи. Из источника [1] известно, что для сигналов LoRa разница в уровнях сигнала и шума может составлять 19 дБ. Данный факт положительно сказывается на дальности передачи в тяжелых городских условиях, которая может достигать 1,5 км., согласно заявлениям производителей передатчиков LoRa. ЛЧМ-сигнал – это сигнал у которого частота изменяется по линейному закону, также ЛЧМ-модуляция является частным случаем систем с расширением спектра – способа повышения эффективности передачи информации с помощью модулированных сигналов через канал с сильными линейными искажениями (замираниями), приводящий к увеличению базы сигнала [2]. Более подробно это можно рассмотреть, используя уравнение ЛЧМ-сигнала:

$$u(t) = \begin{cases} 0, t < -\tau_u/2 \\ U_m \cos(\omega_0 t + \mu t^2/2), \ -\tau_u/2 \le t \le \tau_u/2 \\ 0, t > \tau_u/2 \end{cases} \quad (1)$$

которое описывается следующими параметрами:

BW – ширина спектра радиосигнала;

f_0; $\omega_0=2\pi f_0$ – центральная (несущая) частота радиосигнала;

$f_н = f_0 - BW/2)$; $\omega_н=2\pi f_н$ – нижняя частота радиосигнала;

$f_в = f_0 - BW/2)$; $\omega_в=2\pi f_в$ – верхняя частота радиосигнала;

SF – коэффициент расширения спектра (изменяется в диапазоне от 7 до 12); $\tau_u=2^{SF}/BW$ – длительность радиосигнала;

μ=BW/ τ_u – скорость изменения частоты радиосигнала;

$B = BW \cdot \tau_u = 2^{SF}$ – база радиосигнала.

В источнике [2] проводилось моделирование сигналов ЛЧМ и попытка их подавления. Подавление осуществлялось более широкополосным ЛЧМ сигналом, который в целом можно охарактеризовать как «белый шум» в определённой полосе частот, который на практике довольно часто встречается в каналах связи. «Белый шум» можно представить, как Гауссов случайный процесс, с плотностью вероятности:

$$p(n) = \frac{1}{\sigma\sqrt{2\pi}} exp - \frac{1}{2} \cdot \frac{n}{\sigma} \quad (2)$$

где σ^2 – дисперсия n. Данная плотность вероятности довольно точно описывает большую часть природных и индустриальных помех, свойственных городским условиям радиопередачи. Моделирование в источнике [2] подтвердило заявления производителей оборудования о помехоустойчивости в отношении случайных процессов.

Вопрос подавления сигналов с ЛЧМ, и в частности, стандарта LoRa, имеет актуальное значение, так как его решение позволит осуществлять противодействие подавлению (определение и локализацию источника помех). Для достижения поставленной цели в данном исследовании будет моделироваться подавление сигналов ЛЧМ. В качестве программного обеспечения для осуществления моделирования будет использоваться программа-симулятор Miltisim 12. Стоит отметить, что вопрос подавления сигналов LoRaWAN уже рассматривался в источнике [3], в данном источнике, в качестве метода подавления использовался метод добавления лишних битов к пакету сигнала, благодаря которым он неверно распознаётся приёмником и его дальнейшая обработка прекращается. Подобный подход к подавлению LoRaWAN требует определённых знаний в стандартах связи и принципах формирования пакетов. Зачастую подобные методы редко используются злоумышленниками, так как самым простым является именно «физическое» воздействие на канал связи с использованием подавителей, и именно данный метод и будет рассматриваться далее.

Исходя из того, что сигналы ЛЧМ имеют широкую полосу частоты передачи одного бита, можно сделать вывод о том, что самым эффективным способом подавления данных сигналов будет использование сосредоточенной помехи, в качестве которой может быть применён обычный синусоидальный сигнал:

$$y = a + b \cdot \sin(cx + d) \quad (3)$$

На рисунке 1 приведена схема для осуществления подавления сигналов ЛЧМ. На данном рисунке V4 – исходная последовательность бит с частотой следования 5 кГц; V3 – модулируемый сигнал с расширением частотного спектра от 100 до 200 кГц, и периодом повторения в 5кГц; Q1 – модулятор; V5 – источник синусоидального сигнала с частотой 150 кГц; XSC1 – осциллограф; U2 – аналоговый сумматор, моделирующий линию связи.

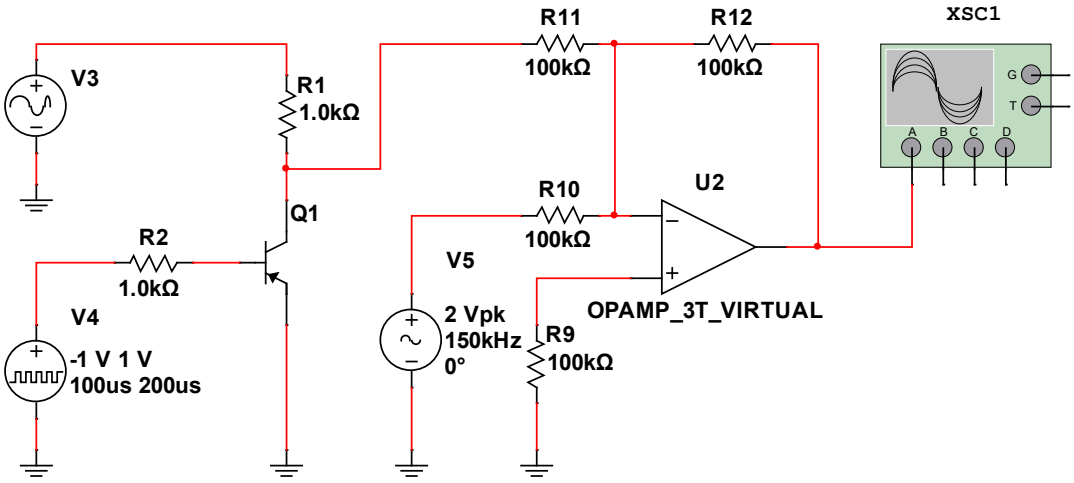


Рис. 1 Схема подавления сигналов ЛЧМ

В процессе проведения моделирования была получена осциллограмма, приведённая на рисунке 2. Как видно из данной осциллограммы, биты ЛЧМ всё ещё можно распознать среди уровней. Для качественного улучшения подавления, уровень сигнала синусоиды был поднят до 4 В, но результирующий сигнал выглядел аналогично приведённому на рисунке 2.

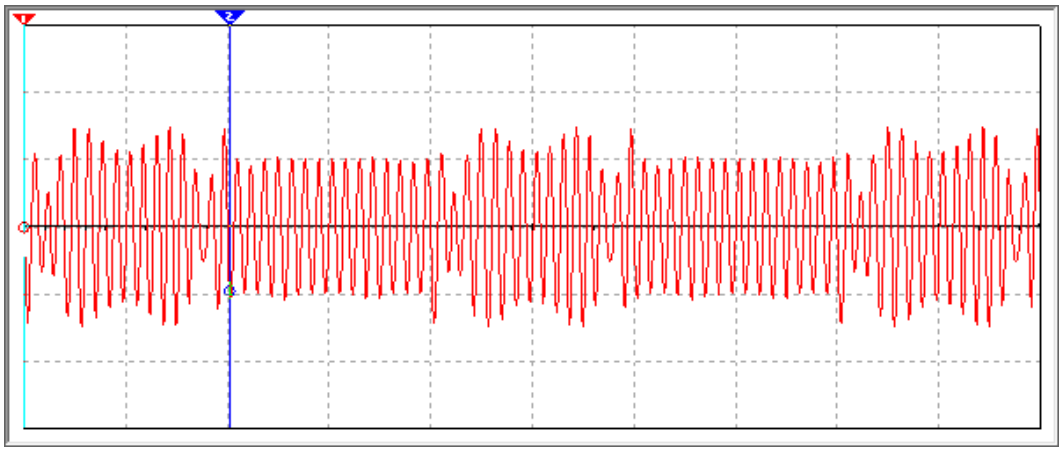


Рис. 2 Осциллограмма на выходе схемы

Для повышения общей эффективности подавления к схеме был подключен ещё один источник синусоидального сигнала с частотой 125 кГц и напряжением 2 В. В результате данного добавления было получено необходимое ухудшение сигнала LoRa. Осциллограмма сигнала на выходе схемы, после добавления ещё одного сигнала приведена на рисунке 3.

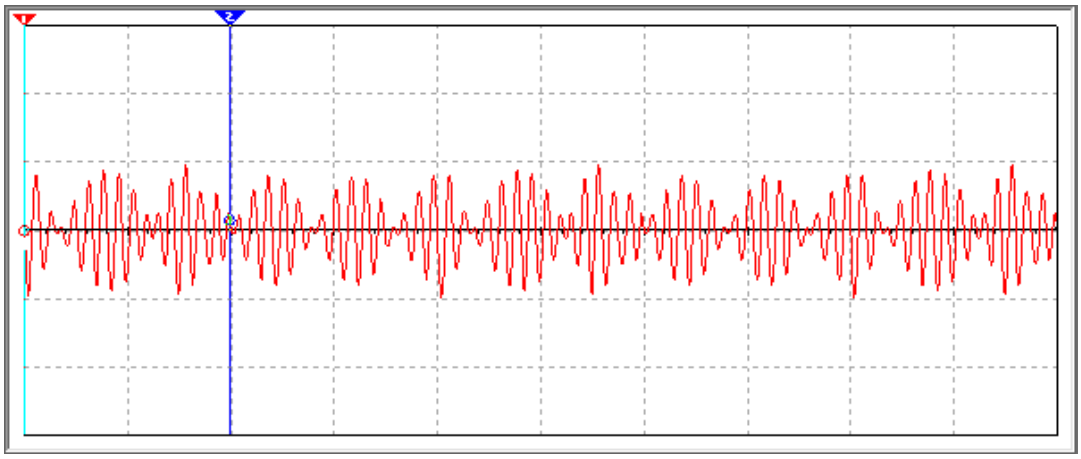


Рис. 3 Осциллограмма сигнала на выходе схемы, после добавления дополнительного синусоидального сигнала

Таким образом, задача, поставленная в начале исследования, была решена. Подводя итоги можно отметить, что сигналы использующие технологии расширения спектра, подобные ЛЧМ и ППРЧ применяемые в технике связи имеют очень высокую помехоустойчивость, вследствие чего их применение с каждым годом увеличивается. Для подавления ЛЧМ сигнала, должны быть применены два источника синусоидального сигнала с различными частотами, в диапазоне которых осуществляется передача данных и уровнем напряжения в два раза превышающем источник сигнала ЛЧМ.

Литература

1. Верхулевский К., Технология LoRa в вопросах и ответах // Технологии и стандарты – 2016 – №1, с 18-21.

2. Матаева А.Б., Косяков И.О., Оценка эффективности применения линейно частотной модуляции в сетях LoRa // Вестник КазАТК – 2017 – №100, с 185-189.

3. Aras E., Small N., and others, Selective Jamming of LoRaWAN using Commodity Hardware // 14th EAI International Conference on Mobile and Ubiquitous – 2017.

ПРИМЕНЕНИЕ АЛГОРИТМА ПРОВЕРКИ ПОДЛИННОСТИ СООБЩЕНИЙ И ХЭШ - ФУНКЦИИ

Усатова О.А.[1], Нысанбаева С.Е.[1], Бегимбаева Е.Е.[1], Усатов Н.С.[2]
e-mail: uoa_olga@mail.ru, sultasha1@mail.ru, enlik_89@mail.ru, usatov.nikita2242@gmail.com
1. Институт информационных и вычислительных технологий КН МОН РК, Казахстан
2. Университет «Туран», Казахстан

Аннотация. *В статье приведены результаты анализа современных распространенных методов аутентификации и хэш-функций. Показаны актуальность и цели их использования в различных областях информационно-коммуникационных системах. Описаны основные свойства и методы формирования кода аутентификации сообщений и хэш-функции. Рассмотрены некоторые вопросы защита целостности сообщения, проверка подлинности отправителя и обеспечение устойчивости к атакам хэш-функции.*

Ключевые слова: алгоритм аутентификации, хэш - функция, безопасность данных, алгоритм хэширования, шифрование.

Введение

Информационные технологии стали неотъемлемой частью нашей жизни в связи с осуществлением автоматизации многих процессов жизнедеятельности человека. Большая часть электронной информации хранится в различных информационных системах, которую необходимо защищать. В атаках на информационные системы злоумышленники используют как ошибки в написании и администрировании их программ, так и методы социальной психологии для получения желаемой информации. Разработчики ресурсов, на которых предполагается работа с данными пользователей, обязаны эти данные защищать и предотвращать возможность их утечек. Одной из основных проблем в нашей стране является слабое развитие отечественной индустрии информационной безопасности, в частности, в разработке средств криптографии. В Казахстане, в настоящее время, в действующих системах защиты электронных данных используются зарубежные криптографические алгоритмы и стандарты.

1. Системы аутентификации и хэш - функции

Большинство современных систем аутентификации основываются на применении вычисления хеш-функций, которые вычисляют хеш-значение на основе входной строки для дальнейшего использования в системе кодирования [1]. В качестве входной строки для хеш–функции могут быть использованы такие учетные данные пользователя как «логин, пароль», текущее время, дополнительная секретная строка и т.д [2]. Для разработки приложений с использованием функции хеширования в Республики Казахстан используется стандарт СТ РК ИСО/МЭК 10118–1–2006 «Информационная технология. Методы защиты информации. Хеш–функции. Часть 1. Общие положения, Часть 3. Специализированные хеш–функции» [3-4].

Область применения хеш-функций чрезвычайно широка: они успешно решают практически все задачи защиты компьютерной информации от обеспечения аутентичности субъектов и объектов информационного взаимодействия до внесения неопределенности в работу средств и объектов защиты. При этом стоит отметить, что задача проектирования качественной хеш-функции не проще, чем задача проектирования качественного симметричного шифра.

Преобразование, производимое хеш-функцией, называется хешированием, исходные данные называются входным массивом, «ключом» или «сообщением», а результат преобразования называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения».

Хеш-функции применяются при построении ассоциативных массивов, при поиске дубликатов в сериях наборов данных, при построении уникальных идентификаторов для наборов данных, при вычислении контрольных сумм от данных для последующего обнаружения в них ошибок, возникающих при хранении и/или передаче данных, при сохранении паролей в системах защиты в виде хеш-кода, а также при вычислении электронной подписи.

Согласно принципу Дирихле, нет однозначного соответствия между хеш-кодом и исходными данными. Возвращаемые хеш-функцией значения менее разнообразны, чем значения входного массива. При работе с хэш–функцией возможно возникновение «коллизий», когда одна и та же хеш-функция выдает для разных массивов входных данных одинаковые хеш-коды. В связи с этим для оценки качества хеш-функций необходимо проводить исследование вероятности возникновения возможных коллизий.

Алгоритмы хеширования отличаются такими свойствами, как разрядность, вычислительная сложность и криптостойкость.

Выбор хеш-функции производится в зависимости от решаемой задачи. На входе хэш-функции подается сообщение произвольной длины, а на выходе хэш-функции формируется хеш (блок данных фиксированной длины). При изменении одного бита на входе хэш-функции должно существенно изменяться выходное значение хеша.

Для обеспечения устойчивости к атакам хэш-функция должна удовлетворять следующим требованиям:

1) если известно значение h хэш-функции, то задача нахождения другого сообщения M', такого, что $H(M') = h$, должна быть вычислительно трудной;

2) при заданном сообщении M задача нахождения другого сообщения M', такого, что $H(M)=H(M')$, должна быть вычислительно трудной.

Если хэш-функция будет удовлетворять этим свойствам, то формируемое ею значение будет уникально идентифицировать сообщения, и всякая попытка изменения сообщения при передаче будет обнаружена путем выполнения хэширования на принимающей стороне и сравнением с дайджестом, полученным на передающей стороне.

Хэш-функции не допускают обратного преобразования – получить исходное сообщения по его дайджесту невозможно, в связи с этим их называют односторонними функциями шифрования. Они строятся по итеративной схеме, когда исходное сообщение разбивается на блоки определенного размера, и над ними выполняются ряд преобразований с использованием как обратимых, так и необратимых операций. Как правило, в состав хэширующего преобразования включается сжимающая функция, поскольку его выход зачастую по размеру меньше

блока, подаваемого на вход. На вход каждого цикла хэширования подается выход предыдущего цикла, а также очередной блок сообщения.

В качестве функции хэш-преобразования можно использовать блочные шифры, они рандомизируют входное сообщение. Блочные шифры являются обратимыми преобразованиями, что не противоречит свойствам хэш-функции, поскольку блочный шифр необратим по ключу шифрования, и, если в качестве ключа шифрования использовать выход предыдущего шага хэш-преобразования, а в качестве шифруемого сообщения очередной блок сообщения (или наоборот), то можно получить хэш-функцию с хорошими криптографическими характеристиками.

Недостатком хэш-функций на основе блочных шифров является невысокая скорость их работы, в связи с этим были спроектированы ряд специализированных алгоритмов, которые, обеспечивая аналогичную стойкость к атакам, выполняют гораздо меньшее количество операций над входными данными и обеспечивают большую скорость работы. Примерами подобного рода алгоритмов являются: MD2, MD4, MD5, RIPEMD –160, SHA (Secure Hash Algorithm) [5].

Хэш - функции используются для реализации алгоритмов аутентификации. Изменение одного бита входной строки влияет на все биты вычисляемого хеша, что позволяет исключить вычисляемую зависимость получаемого хеша от входной строки [6]. Посещение любого веб-ресурса, защищенного сертификатом безопасности SSL, автоматически запускает выполнение алгоритма SHA-256, он считается достаточно надёжным и криптостойким, а также с приемлемой скоростью работы. Он используется в телекоммуникационных системах, интернете, для шифрования беспроводных пакетов в IoT и других.

Основной целью аутентификации пользователя информационной системы является снижение угроз безопасности, а именно нарушение конфиденциальности и целостности информации. Несанкционированный доступ – один из самых распространенных видов нарушений, представляющий непосредственную угрозу работоспособности системы. В криптографии под защитой данных от несанкционированных изменений понимают не исключение самой возможности таких изменений, а набор методов, позволяющих надежно предупредить или зафиксировать их факты, если они имели место.

Аутентификация сообщения связана с защитой целостности сообщения, проверкой подлинности отправителя, где учитываются требования к безопасности. Для обеспечения целостности используются три функции: шифрование сообщения, код аутентификации сообщений (MAC) и хэш-функция [7].

Шифрование сообщения обеспечивает меру аутентификации, если используется симметричное шифрование, тогда получатель знает, что отправитель должен был его создать, поскольку используются только ключ отправителя и получателя, известно, что содержимое не может быть изменено, если сообщение имеет подходящую структуру, избыточность или контрольную сумму обнаруживать любые изменения.

Код аутентификации сообщений - Message authentication code (MAC): это битовая строка, которая является функцией как данных (открытого текста или зашифрованного), так и секретного ключа, и которая прикрепляется к данным для обеспечения аутентификации данных.

Функция, используемая для генерации кода аутентификации сообщения, должна быть односторонней. Данные, связанные с аутентифицированным сообщением, позволяют получателю проверить целостность сообщения.

Метод аутентификации включает использование секретного ключа для генерации небольшого блока данных фиксированного размера, известного как криптографическая контрольная сумма или MAC, который добавляется к сообщению. Поведение MAC-функции аналогичны ключевым хеш-функциям, они предъявляют другие требования к безопасности. Алгоритмы MAC могут быть построены из криптографических примитивов, таких как криптографические хеш-функции.

Получатель вычисляет MAC, используя тот же самый секретный ключ, и сравнивает вычисленное значение с полученным (формула 1). Если эти значения совпадают, то с большой долей вероятности можно считать, что при пересылке изменения сообщения не произошло.

$$MAC = C_K(M) \quad (1)$$

Рассмотрим свойства, которыми должна обладать функция MAC. Если длина ключа, используемого при вычислении MAC, равна k, то при условии сильной функции MAC противнику потребуется выполнить 2^k попыток для перебора всех ключей. Если длина значения, создаваемого MAC, равна n, то всего существует 2^n различных значений MAC.

Функция вычисления MAC должна обладать следующими свойствами. Во первых, она должна быть вычислительно сложной, т.е. зная M и $C_K(M)$, найти сообщение M', такое, что $C_K(M) = C_K(M')$, сложно, во вторых значения $C_K(M)$ должны быть равномерно распределенными, т.е. для любых сообщений M и M' вероятность того, что $C_K(M) = C_K(M')$, должна быть равна 2^{-n}, где n – длина значения MAC.

Алгоритм проверки подлинности сообщения представлен на рисунке 1.

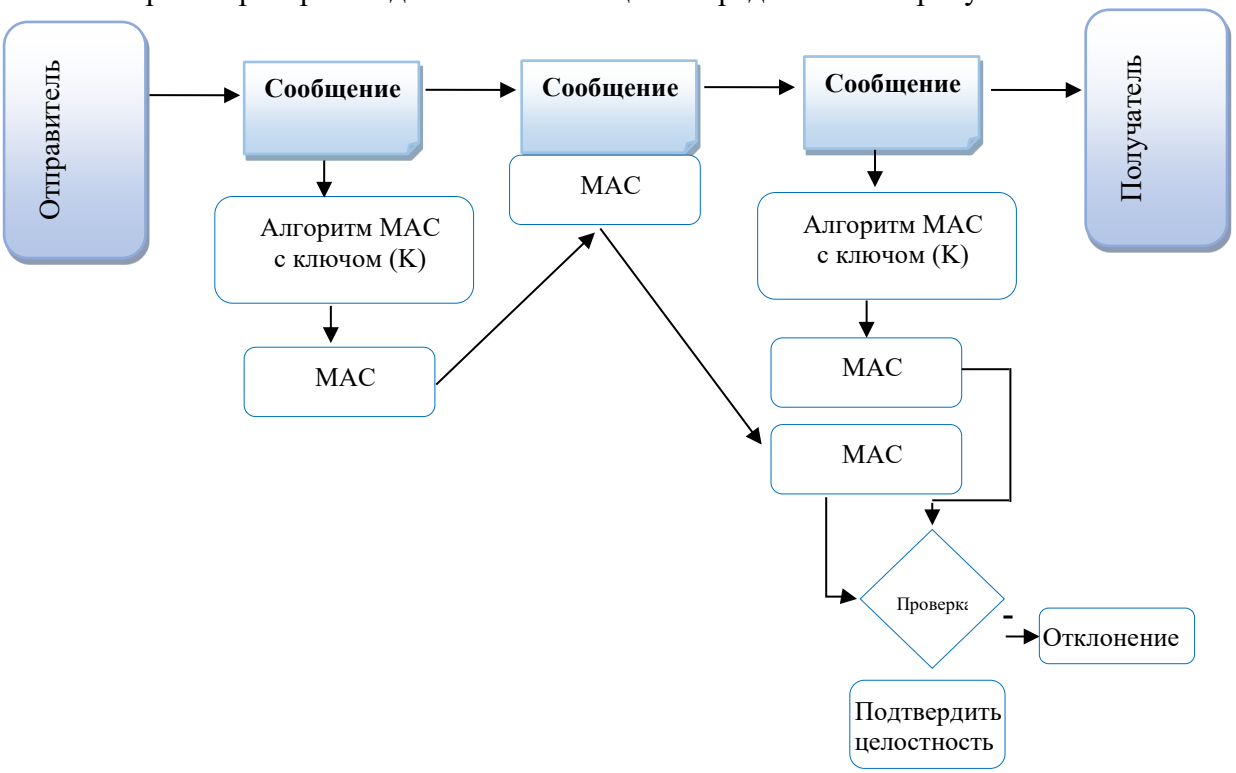


Рис. 1 – Алгоритм проверки подлинности сообщения

На рисунке 1 представлена передача сообщения от отправителя к получателю с применением MAC алгоритма. Если после проверки код аутентификации является правильным, то происходит подтверждение целостности, если нет, то отклонение. Алгоритм проверки подлинности сообщения обеспечивает конфиденциальность, также может использовать шифрование для секретности с использованием отдельных ключей до или после шифрования.

2. Вычисления MAC на основе хэш-функции

Другим способом обеспечения целостности является использование хэш-функции. Хэш-код присоединяется к сообщению в тот момент, когда известно, что сообщение корректно. Получатель проверяет целостность сообщения вычислением хэш-кода полученного сообщения и сравнением его с полученным хэш-кодом, который должен быть передан безопасным способом. Одним из таких безопасных способов может быть шифрование хэш-кода закрытым ключом отправителя. Возможно также шифрование полученного хэш-кода алгоритмом симметричного шифрования, если отправитель и получатель имеют общий ключ симметричного шифрования.

Использование хэш-функции для получения MAC состоит в том, чтобы определенным образом добавить секретное значение к сообщению, которое подается на вход хэш-функции. Такой алгоритм носит название - Хэш-код аутентификации сообщений - Hashbased message authentication code (HMAC), который изложен в RFC 2104.

Алгоритма HMAC дает возможность использовать без модификаций уже имеющиеся хэш-функции и легко заменять встроенные хэш-функций на более быстрые или более стойкие [8]. HMAC сохраняет скорость работы алгоритма, близкой к скорости работы соответствующей хэш-функции и позволяет использовать ключи.

В алгоритме HMAC хэш-функция позволяет использовать существующие реализации хэш-функций, а также дает возможность обеспечивать несложную замену существующей хэш-функции на новую.

Рассмотрим следующие обозначения:

H – встроенная хэш-функция;

b – длина блока используемой хэш-функции;

n – длина хэш-кода;

K – секретный ключ. К этому ключу слева добавляют нули, чтобы получить b-битовый ключ K+.

Применяются два вспомогательных значения:

Ipad - значение ‘00110110’, повторенное b/8 раз.

Opad – значение ‘01011010’, повторенное b/8 раз.

Далее HMAC вычисляется следующим образом (формула 2):

$$HMAC = H((K^{+} \oplus Opad) \,||\, H((K^{+} \oplus Ipad) || M)). \quad (2)$$

На рисунке 2 представлена работа функции HMAC.

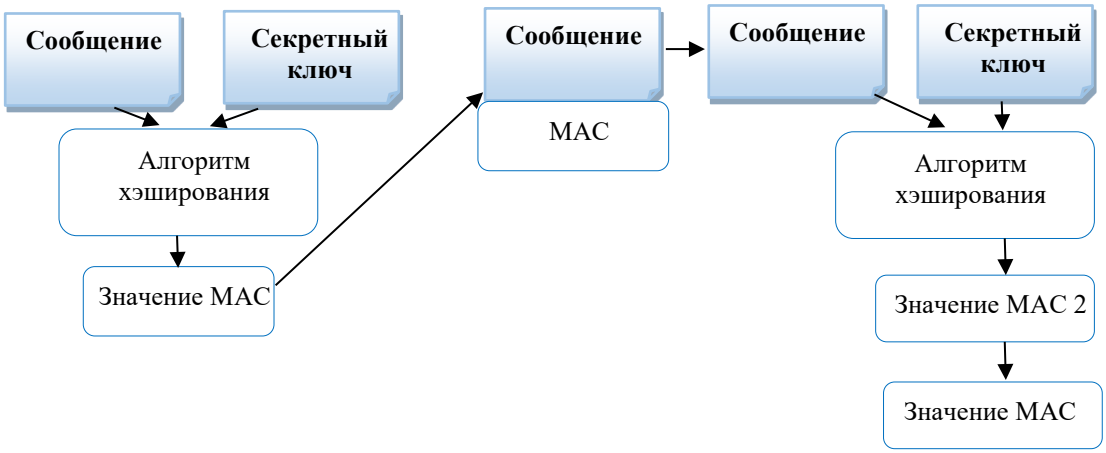


Рис. 2 - Функция HMAC

Алгоритм работы функции HMAC: отправитель добавляет симметричный ключ к сообщению, затем результат используется в алгоритм хэширования, где генерируется значение MAC. Сгенерируемое сообщение MAC добавляется к сообщению. Отправитель передает сообщение получателю, в свою очередь получатель добавляет свою копию симметричного ключа к полученному сообщению, далее получатель пропускает результат через хэширующий алгоритм и генерирует свое собственное значение MAC. Получатель сравнивает два значения MAC и если они совпадают, то сообщение не было изменено.

Следует отметить, что функция HMAC не шифрует сообщение, поэтому она не обеспечивает конфиденциальность - главное, чтобы у отправителя и получателя был одинаковый симметричный ключ.

Хэш-функции, также как и код аутентификации с использованием хэш-функций MAC, успешно используются в схемах генерации ключевой информации.

Выводы

Функции MAC аналогичны криптографическим функциям hash, они удовлетворяют различными требованиями к безопасности. Несмотря на их сходство, реализуются они по-разному: обычно алгоритм генерации MAC основан на алгоритме генерации кода hash с расширением, которое использует закрытый ключ.

Основное различие заключается в концептуальности: хэши используются для гарантии целостности данных, а MAC гарантирует аутентификацию целостности. Это означает, что хэш-код генерируется из сообщения без какого-либо внешнего ввода: то, что вы получаете, — это то, что можно использовать для проверки того, изменилось ли сообщение во время его перемещения. Вместо этого MAC использует закрытый ключ в качестве исходного кода для функции hash, которую он использует при генерации кода: это должно гарантировать получателю, что не только сообщение не было изменено, но и кто его отправил, это тот, которого мы ожидали: в противном случае злоумышленник не может знать закрытый ключ, используемый для генерации кода. HMAC - это код аутентификации сообщения на основе hash. Обычно это включает применение функции hash один или несколько раз к какой-либо комбинации общего секрета и сообщения.

Подтверждение

Исследовательские работы проводились в рамках проекта программно-целевого финансирования (ПЦФ) вне конкурсных процедур по научным и (или) научно-техническим проектам на 2021-2022 гг., на тему: «Разработка и исследование алгоритмов хеширования произвольной длины для цифровых подписей и оценка их стойкости», который реализуется в Институте информационных и вычислительных технологий при поддержке Министерства образования и науки РК.

Литература

1 O. Ussatova, S. Nyssanbayeva, W. Wojci. « Software implementation of two-factor authentication to ensure security when accessing an information system» // Вестник КазНУ им.аль-Фараби. –Алматы,2019. – С. 87–95.

2 Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule «Development of an automated system model of information protection in the cross-border exchange»// Cogent Engineering Journal. – 2020. DOI: 10.1080/ 23311 916. 2020.1724597. –P. 1–13.

3 СТ РК ИСО/МЭК 10118-1-2006 «Информационная технология. Методы защиты информации. Хеш–функции. Часть 1. Общие положения». https://online. zakon. kz/Document/?doc_id=31071245#pos=0;0.15.06.2019.

4 СТ РК ИСО/МЭК 10118-3-2006 (ISO/IEC 10118-3-2004, IDT) «Информационная технология. Методы защиты информации. Хеш–функции. Часть 3. Специализированные хеш–функции». https://online.zakon.kz/ Document / ?doc_id = 30461868#pos=0;0.10.08.2019.

5 Информационная технология. Криптографическая защита информации. Функция хеширования. ГОСТ Р34.11 – 2012. – Москва, Стандартинформ, 2012. http://docs.cntd.ru/document/gost-r-34-11-201210.08.2019.

6 Л.К. Бабенко, Е.А. Ищукова. Дифференциальный криптоанализ упрощенной функции хеширования sha // Известия ЮФУ, Технические науки, –2010.– С 203–220.

7 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf (Дата обращения 07.06.2021).

8 Функции хэширования. - https://studme.org/239586/informatika/ funktsii_ heshirovaniya (Дата обращения 10.06.2021).

АЛГОРИТМ ШИФРОВАНИЯ QALQAN

Горлов Л.В.[1,2], Ибраев Р.Б.[1], Оспанов Ж.Ж.[1,2], Итемиров Р.С.[1], Кияшко И.В.[1]
e-mail: lev.gorlov@gmail.com
[1] Satbayev University, [2] Казахский национальный университет имени Аль-Фараби

Аннотация. *В данной статье представлен алгоритм блочного симметричного шифрования Qalqan и результаты его первичного криптографического анализа, по которым он признан стойким к основным современным атакам. Данный алгоритм по своим основным свойствам не уступает лучшим мировым аналогам и может быть рассмотрен в качестве первого национально стандарта шифрования Республики Казахстан.*

Qalqan – алгоритм симметричного блочного шифрования. Размер блока составляет 128 битов, размер ключа варьируется от 256 до 1024 битов с шагом 128 битов. В зависимости от длины ключа содержит от 17 до 23 раундов преобразований [1].

Алгоритм шифрования Qalqan разработан коллективом Научно-исследовательской лаборатории информационной безопасности Института кибернетики и информационных технологий КазНИТУ им. К.И. Сатпаева под руководством к.ф-м.н. Н.А. Сейловой. Впервые представлен широкой публике в ходе конференции РусКрипто-2021, Москва, Российская Федерация.

Разработка алгоритма шифрования Qalqan осуществлена в ходе научного проекта с грантовым финансированием №AP06851287, её итогом планируется внедрение алгоритма шифрования Qalqan в качестве первого национального стандарта шифрования Республики Казахстан.

Алгоритм шифрования Qalqan построен в соответствии с архитектурой SP-сети [2], каждый раунд содержит три операции: наложение раундового ключа, нелинейную операцию (задана фиксированной подстановкой) и линейную операцию, кроме последнего раунда, который состоит только из операции наложения ключа.

Каждая из основных операций алгоритма шифрования Qalqan выполняет одну задачу, причём делает это максимально эффективно, но без ущерба быстродействию. Все они созданы на основе хорошо изученных функций и не содержат секретных значений. В соответствии с постулатами К. Шеннона [3], эти относительно простые операции обеспечивают перемешивание и рассеивание битов обрабатываемого блока и ключа на протяжении нескольких раундов.

В отличие от большинства современных алгоритмов шифрования наложение ключа происходит путём сложения с переносом битов. Только в первом и последнем раунде для этой операции применяется исключающее ИЛИ (XOR). Таким образом ценой достаточно простых операций усложняется взаимная зависимость битов обрабатываемого блока.

Линейная операция также является последовательностью операций сложения по модулю 256 (с переносом битов без выхода за пределы байта). Она сконструирована таким образом, чтобы уже за два раунда обеспечить требуемый лавинный эффект (при изменении одного бита входа каждый бит выхода меняется с вероятностью 0.5).

В виду наличия серьёзных претензий к секретной внутренней структуре таблиц подстановки алгоритма Кузнечик и хеш-функции Стрибог [4] подстановка алгоритма шифрования Qalqan разработана максимально прозрачным методом. Для этого выбран подход, аналогичный применённому в алгоритме AES, а именно генерация подстановки по методу, предложенному К. Найберг в 1991 году [5]. Константы, используемые при генерации, изменены с целью достижения более близких к оптимальным значениям [6] таких криптографически важных параметров, как снижение максимума дифференциального профиля по сложению и XOR (противодействие дифференциальному анализу), снижение максимума таблицы линейных аппроксимаций (противодействие линейному анализу), высокая алгебраическая степень, максимальное расстояние до класса аффинных преобразований.

Использованные константы легко получить путём реверсивного анализа итоговой подстановки.

В результате основные параметры подстановки приняли следующие значения:

1. Максимум таблицы линейных аппроксимаций: 32.
2. Максимум дифференциальной таблицы: 4.
3. Степень полинома Жегалкина: 7.
4. Расстояние до класса аффинных функций: 112.

Отдельно авторы предлагают при необходимости использовать собственную подстановку, обладающую не худшими параметрами.

Подстановка фиксирована в следующем виде (в Си-подобном формате):

```
uint8 sb[256] = {
0xeb, 0x89, 0xdb, 0xcb, 0xf3, 0xf5, 0xfb, 0x90, 0xe6, 0x3d, 0xe5, 0x2e, 0xe3, 0x0b, 0x56, 0xe1,
0x6c, 0x12, 0x80, 0x28, 0xed, 0x22, 0x09, 0x4a, 0xee, 0x27, 0x9b, 0x58, 0x35, 0x57, 0xef, 0x94,
0x29, 0xc0, 0x16, 0x7c, 0x5e, 0x87, 0x0a, 0x7e, 0xe8, 0x11, 0x0e, 0xaf, 0x9a, 0x84, 0x3a, 0x1a,
0x69, 0x71, 0x8c, 0xbc, 0xd2, 0x55, 0x33, 0xd1, 0x85, 0x75, 0xb5, 0x83, 0xe9, 0x50, 0x54, 0xac,
0x8a, 0xd6, 0x7f, 0x1f, 0x14, 0x4e, 0x21, 0x82, 0x30, 0x24, 0xdd, 0x9f, 0x1b, 0x32, 0x20, 0xa8,
0x6a, 0xb0, 0x97, 0x62, 0x19, 0xd8, 0xc8, 0x0c, 0x52, 0x02, 0x5c, 0x43, 0x03, 0x95, 0x13, 0x81,
0xab, 0x77, 0xa6, 0xf2, 0x59, 0x67, 0x41, 0xec, 0x76, 0x98, 0xb4, 0x73, 0x86, 0x9c, 0xf7, 0xcf,
0xdc, 0xba, 0xa4, 0xfd, 0xc4, 0x99, 0xdf, 0xce, 0xea, 0x1c, 0x36, 0xbd, 0x34, 0xd7, 0x49, 0x64,
0x5a, 0x6f, 0x74, 0x01, 0xa0, 0x39, 0x91, 0x00, 0x15, 0x3f, 0x38, 0xb8, 0x8f, 0x26, 0x5f, 0xf8,
0x07, 0xa3, 0x0d, 0xda, 0xf0, 0xe7, 0xd0, 0xd9, 0x93, 0xf6, 0x06, 0x47, 0x0f, 0xa1, 0x4b, 0xc5,
0x2a, 0xff, 0x46, 0x60, 0xd5, 0x1d, 0x2f, 0xa9, 0x92, 0x17, 0x72, 0x8e, 0x7a, 0xaa, 0x18, 0x6e,
0x37, 0x08, 0x1e, 0x63, 0x31, 0xc2, 0xbf, 0xc6, 0x9e, 0x65, 0xd4, 0x3b, 0x96, 0x9d, 0xde, 0x45,
0xca, 0x2d, 0xa5, 0xfe, 0x4d, 0xb9, 0x66, 0xc3, 0xb3, 0xcc, 0xad, 0x61, 0xbe, 0x7b, 0x68,
```

0x88,
0x25, 0x2b, 0x53, 0x5b, 0x44, 0x40, 0xa7, 0xa2, 0x5d, 0xc9, 0x51, 0xae, 0xe4, 0xc7, 0xf9, 0x78,
0x70, 0xcd, 0x42, 0x4f, 0x4c, 0x3c, 0xe0, 0x3e, 0x7d, 0xb7, 0xd3, 0xb2, 0xf1, 0x8d, 0x79, 0x8b,
0x6b, 0xe2, 0x10, 0x23, 0x04, 0x6d, 0xc1, 0xfc, 0x05, 0xb6, 0xf4, 0x48, 0xbb, 0xb1, 0x2c, 0xfa };

Инверсная подстановка, применяемая при расшифровании:

uint8 isb[256] = {
0x87, 0x83, 0x59, 0x5c, 0xf4, 0xf8, 0x9a, 0x90, 0xb1, 0x16, 0x26, 0x0d, 0x57, 0x92, 0x2a, 0x9c,
0xf2, 0x29, 0x11, 0x5e, 0x44, 0x88, 0x22, 0xa9, 0xae, 0x54, 0x2f, 0x4c, 0x79, 0xa5, 0xb2, 0x43,
0x4e, 0x46, 0x15, 0xf3, 0x49, 0xd0, 0x8d, 0x19, 0x13, 0x20, 0xa0, 0xd1, 0xfe, 0xc1, 0x0b, 0xa6,
0x48, 0xb4, 0x4d, 0x36, 0x7c, 0x1c, 0x7a, 0xb0, 0x8a, 0x85, 0x2e, 0xbb, 0xe5, 0x09, 0xe7, 0x89,
0xd5, 0x66, 0xe2, 0x5b, 0xd4, 0xbf, 0xa2, 0x9b, 0xfb, 0x7e, 0x17, 0x9e, 0xe4, 0xc4, 0x45, 0xe3,
0x3d, 0xda, 0x58, 0xd2, 0x3e, 0x35, 0x0e, 0x1d, 0x1b, 0x64, 0x80, 0xd3, 0x5a, 0xd8, 0x24, 0x8e,
0xa3, 0xcb, 0x53, 0xb3, 0x7f, 0xb9, 0xc6, 0x65, 0xce, 0x30, 0x50, 0xf0, 0x10, 0xf5, 0xaf, 0x81,
0xe0, 0x31, 0xaa, 0x6b, 0x82, 0x39, 0x68, 0x61, 0xdf, 0xee, 0xac, 0xcd, 0x23, 0xe8, 0x27, 0x42,
0x12, 0x5f, 0x47, 0x3b, 0x2d, 0x38, 0x6c, 0x25, 0xcf, 0x01, 0x40, 0xef, 0x32, 0xed, 0xab, 0x8c,
0x07, 0x86, 0xa8, 0x98, 0x1f, 0x5d, 0xbc, 0x52, 0x69, 0x75, 0x2c, 0x1a, 0x6d, 0xbd, 0xb8, 0x4b,
0x84, 0x9d, 0xd7, 0x91, 0x72, 0xc2, 0x62, 0xd6, 0x4f, 0xa7, 0xad, 0x60, 0x3f, 0xca, 0xdb, 0x2b,
0x51, 0xfd, 0xeb, 0xc8, 0x6a, 0x3a, 0xf9, 0xe9, 0x8b, 0xc5, 0x71, 0xfc, 0x33, 0x7b, 0xcc, 0xb6,
0x21, 0xf6, 0xb5, 0xc7, 0x74, 0x9f, 0xb7, 0xdd, 0x56, 0xd9, 0xc0, 0x03, 0xc9, 0xe1, 0x77, 0x6f,
0x96, 0x37, 0x34, 0xea, 0xba, 0xa4, 0x41, 0x7d, 0x55, 0x97, 0x93, 0x02, 0x70, 0x4a, 0xbe, 0x76,
0xe6, 0x0f, 0xf1, 0x0c, 0xdc, 0x0a, 0x08, 0x95, 0x28, 0x3c, 0x78, 0x00, 0x67, 0x14, 0x18, 0x1e,
0x94, 0xec, 0x63, 0x04, 0xfa, 0x05, 0x99, 0x6e, 0x8f, 0xde, 0xff, 0x06, 0xf7, 0x73, 0xc3, 0xa1};

Линейная функция $L:V_{128}\rightarrow V_{128}$ преобразует входной блок B размером 16 байтов в выходной блок R такого же размера следующим образом (байты пронумерованы от старшего к младшему):

$$R_0 = B_0 \dot{+} B_1 \dot{+} B_2 \dot{+} B_3$$
$$R_4 = B_4 \dot{+} R_0$$
$$R_8 = B_8 \dot{+} R_0$$
$$R_{12} = B_{12} \dot{+} R_0$$
$$R_5 = B_4 \dot{+} B_5 \dot{+} B_6 \dot{+} B_7$$
$$R_1 = B_1 \dot{+} R_5$$
$$R_9 = B_9 \dot{+} R_9$$
$$R_{13} = B_{13} \dot{+} R_5$$
$$R_{10} = B_8 \dot{+} B_9 \dot{+} B_{10} \dot{+} B_{11}$$
$$R_2 = B_2 \dot{+} R_{10}$$
$$R_6 = B_6 \dot{+} R_{10}$$
$$R_{14} = B_{14} \dot{+} R_{10}$$
$$R_{15} = B_{12} \dot{+} B_{13} \dot{+} B_{14} \dot{+} B_{15}$$
$$R_3 = B_3 \dot{+} R_{15}$$
$$R_7 = B_7 \dot{+} R_{15}$$
$$R_{11} = B_{11} \dot{+} R_{15}$$

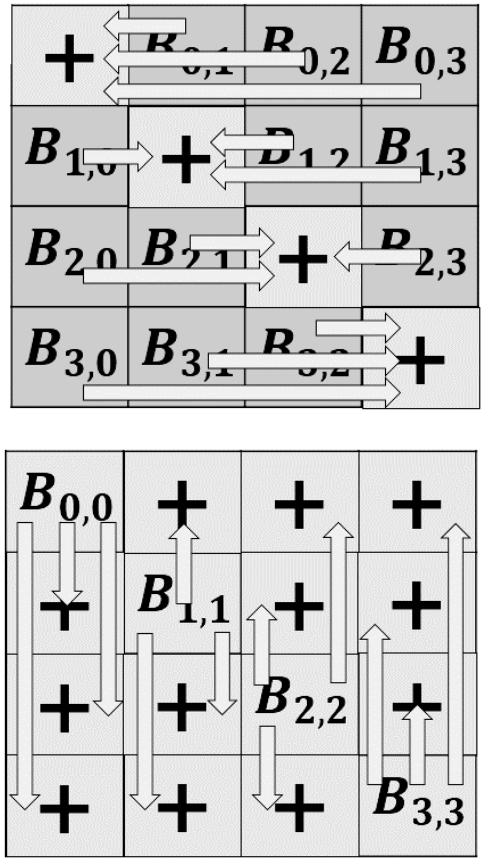


Рисунок 1 – линейная операция алгоритма шифрования Qalqan в графическом представлении

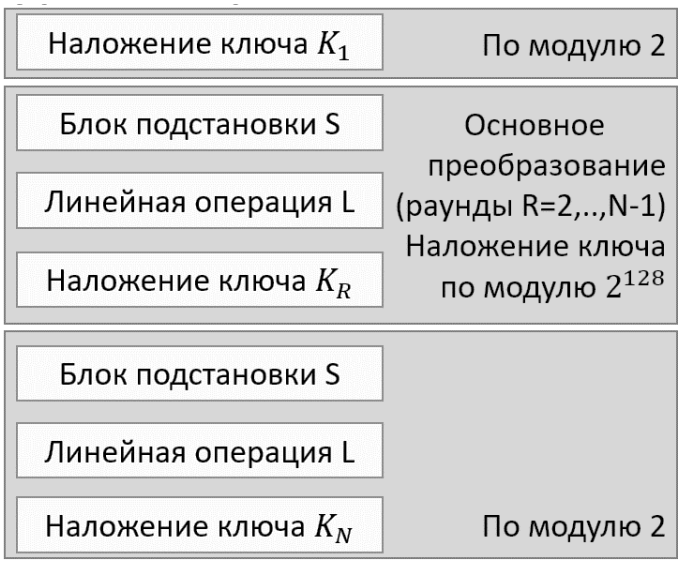


Рисунок 2. Архитектура алгоритма шифрования Qalqan

Для исключения атак, использующих ключевое расписание, в алгоритме шифрования Qalqan предприняты следующие меры:

1. Раундовые ключи невозможно вычислить один из другого.
2. Отсутствуют классы слабых ключей.
3. Атакующий, имеющий доступ к узлу развёртывания ключа, может произвольно задать максимум один раундовый ключ.
4. Высокий лавинный эффект, распространяющий отличие мастер-ключа от раундовых ключей (исключены атаки на связанных ключах).

Механизм развёртывания раундовых ключей использует принцип комбинирующего генератора на базе байтовых регистров сдвига. Однако, в отличие от линейных регистров сдвига, данные регистры используют нелинейное преобразование алгоритма шифрования Qalqan внутри функции обратной связи.

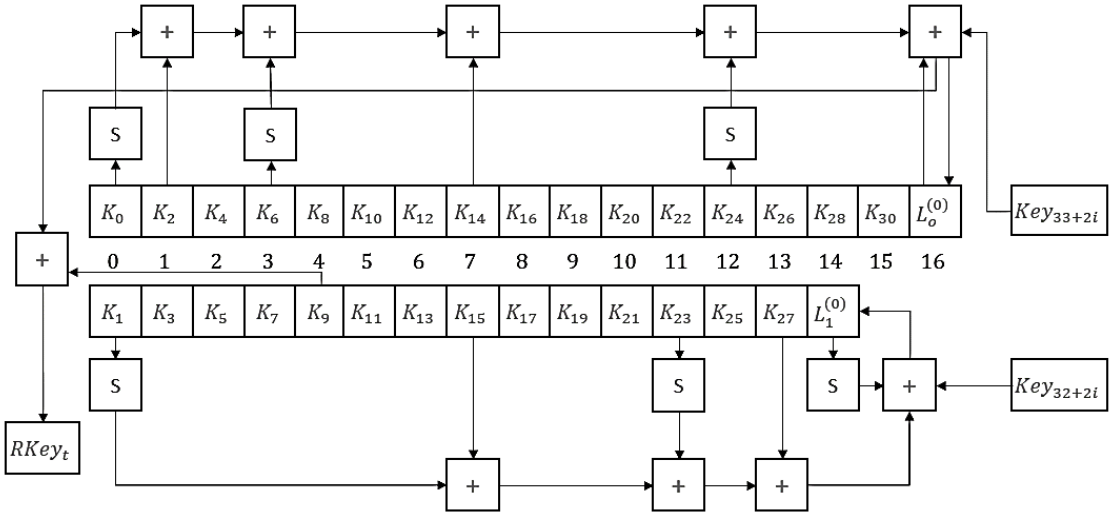


Рисунок 3 – блок развёртывания ключей алгоритма шифрования Qalqan в графическом представлении

Помимо этого, доступно разворачивание раундовых ключей на лету.

Дифференциальный криптографический анализ [7] показал, что максимальная вероятность выполнения трёхраундовой дифференциальной характеристики алгоритма шифрования Qalqan при всех допущениях составляет не более 2^{-132}. Следовательно, для успешного проведения дифференциального криптоанализа требуется более 2^{128} пар текстов, что недостижимо, таким образом, алгоритм устойчив к классическому дифференциальному криптоанализу.

Алгоритм шифрования Qalqan устойчив и к линейному анализу [8]. Для нелинейного узла алгоритма шифрования Qalqan максимальное значение таблицы линейных аппроксимаций равно 32, следовательно, отклонение вероятности равно p =144/256. Линейная аппроксимация на 16 раундов алгоритма Qalqan без линейной функции выполняется с вероятностью $P=1/2+2^{15}*(144/256-1/2)^{16}$, тогда для проведения атаки требуется 2^{98} пар открытого и шифрованного на одном ключе текста, что недостижимо на практике.

Независимая экспертиза, проведённая Институтом информационных и вычислительных технологий Комитета науки МОН РК показала, что:

1. Дифференциальный анализ на 3-раундовый алгоритм позволяет определить ключ с вероятностью 2^{-78}, после 4 раунда вероятность составляет 2^{-312}.

2. Линейный анализ требует 2^{259} пар открытых и шифрованных текстов.
3. Лавинный эффект обеспечивается на 4 раунде.

Литература

1. Горлов Л.В., Ибраев Р.Б. Кандидат в национальные стандарты республики Казахстан — алгоритм шифрования Qalqan https://www.ruscrypto.ru/resource/archive/rc2021/files/ 02_gorlov_ibrayev.pdf (15.08.2021)

2. Horst Feistel, «Cryptography and Computer Privacy / Scientific American, Vol. 228, No. 5, 1973.

3. Шеннон К. Теория связи в секретных системах (англ. Communication Theory of Secrecy Systems) / Bell System Technical Journal, 1949г.

4. Léo Perrin, Aleksei Udovenko. Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog (англ.) // IACR Transactions on Symmetric Cryptology. — 2016. — P. 99–124. — ISSN 2519-173X. — doi:10.13154/tosc.v2016.i2.99-124.

5. Kaisa Nyberg, Perfect non-linear S-boxes // EUROCRYPT 1991: Advances in Cryptology — EUROCRYPT ’91. – P. 378-386.

6. Jie Cui, Liusheng Huang, Hong Zhong, Chinchen Chang, Wei Yang, An improved AES S- box and its performance analysis // International Journal of Innovative Computing, Information and Control, 2011, volume 7, № 5(A), - P. 2291-2302.

7. E.Biham and A.Shamir, Differential cryptoanalysis of DES with a reduced number of rounds // Advanced Crypto, 1990.

8. Matsui M. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology — EUROCRYPT ’93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings / T. Helleseth — 1 — Berlin: Springer Berlin Heidelberg pp, 1993. — P. 386—397. — 465 p. — ISBN 978-3-540-57600-6 — doi:10.1007/3-540-48285-7_33.

О ПРОТОКОЛЕ ГЕНЕРАЦИИ, ФОРМИРОВАНИЯ, РАСПРЕДЕЛЕНИЯ И УПРАВЛЕНИЯ КЛЮЧАМИ, ПРИГОДНОГО ДЛЯ ИСПОЛЬЗОВАНИЯ В СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ ПРЕДВАРИТЕЛЬНОГО ШИФРОВАНИЯ

Ибраев Р.Б.[1], Оспанов Ж.Ж.[1,2], Горлов Л.В[1,2],
Итемиров Р.С.[1], Кияшко И.В.[1]
e-mail: renafm@mail.ru
[1] Satbayev University,
[2] Казахский национальный университет имени Аль-Фараби

Аннотация. *В данной работе рассмотрены основные уязвимости протоколов генерации, формирования, распределения и управления ключами, подходы к разработке собственного протокола, позволяющего организовать защищенную связь.*

1. Введение

Обеспечение конфиденциальности информации с ограниченным доступом, подлежащей передаче по каналам связи, а также циркулирующей в информационных системах, достигается применением средств криптографической защиты информации, реализующих криптографически стойкие алгоритмы шифрования. Согласно принципу Кирхгоффа, стойкость таких алгоритмов основывается только на секретности (неизвестности вероятному противнику) значения ключа шифрования. В этой связи возникает очень важная задача – генерация, формирование, распределение и управление ключами шифрования.

В настоящее время для обеспечения конфиденциальности защищаемой информации широко применяются симметричные криптографические системы. Это обусловлено рядом факторов: доказуемая стойкость, более глубокая изученность, простота реализации как в аппаратно-программном, так и в программном средствах, широкое предназначение (генерация случайных чисел, шифрование, вычисление имитовставки).

В действующих симметричных криптографических системах широко применяются следующие виды протоколов:

1) ключ шифрования генерируется с применением генераторов случайных и псевдослучайных чисел, носитель ключа шифрования заключается в специальную упаковку и доставляется посредством доверенного курьера, управление ключом шифрования осуществляется в плановом порядке;
2) генерация и формирование ключа шифрования осуществляется посредством асимметричной криптографии, распределение осуществляется по открытому каналу, ключи шифрования являются сеансовыми;
3) применяются механизмы квантовой криптографии.

Каждый из указанных видов протоколов обладает рядом как преимуществ, так и недостатков, а именно:

1) применение доверенного курьера в современных реалиях является дорогостоящим методом, хотя является самым безопасным;
2) применение асимметричной криптографии является весьма небезопасным ввиду того, что стойкость таких протоколов основывается только на

решении базовой задачи, в частности, на задачах факторизации и дискретного логарифмирования, хотя данный вид протоколов не требует финансовых затрат на распределение ключей;

3) для реализации механизмов квантовой криптографии требуется весьма сложная и дорогостоящая техника, кроме того имеющаяся на рынке техника на сегодняшний день не обладает высокой стабильностью работы и большой дальностью охвата (не более 40 км).

В этой связи в данной работе будет рассмотрен собственный протокол генерации, формирования, распределения и управления ключами, пригодный для реализации в программных средствах криптографической защиты информации Qalqan-DS и Qalqan-DSM.

Qalqan-DS и Qalqan-DSM – программные средства криптографической защиты информации, реализующие алгоритм блочного симметричного шифрования Qalqan, функционирующие под управлением Microsoft Windows, Linux, IOS и Android, предназначенные для предварительного шифрования электронных файлов и их контроля целостности и аутентичности.

Собственный протокол генерации, формирования, распределения и управления ключами разработан с учетом всех принципов современной криптографии, а именно:

1) с использованием «хорошо» изученных методов;
2) с учетом тенденции развития криптографии и криптографического анализа;
3) с учетом тенденции развития вычислительной техники;
4) с учетом особенностей реализации разрабатываемого протокола генерации, формирования, распределения и управления ключами в программном и аппаратно-программном средствах криптографической защиты информации.

2. Генерация случайной двоичной последовательности

Алгоритм блочного симметричного шифрования Qalqan не имеет классы слабых и эквивалентных ключей шифрования [1]. В этой связи главным требованием к генерации ключей шифрования является их случайность.

Для генерации случайной двоичной применяется персональное программное средство криптографической защиты информации aKey T1004, соответствующее требованиям Государственного стандарта Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования» по четвертому уровню безопасности, имеющее в составе физический генератор шума [5].

3. Формирование ключей шифрования

Ключи шифрования и ключи имитовставки, требуемые для функционирования программных средств криптографической защиты информации Qalqan-DS и Qalqan-DSM, формируются из сгенерированной случайной двоичной последовательности.

Архитектура ключевой сети – полносвязная матрица, таким образом, каждый пользователь обладает ключами для связи со всеми остальными пользователями, а также существующими в единственном экземпляре ключами для защиты собственных сведений, не подлежащих пересылке другим участникам защищённой сети связи («для себя»).

Ключи хранятся в файлах формата *.xml. Файл содержит ключи имитовставки и шифрования данных по направлению к одному или нескольким пользователям, включая ключи имитовставки и шифрования данных «для себя».

Каждый ключ состоит из нескольких полей данных:

1) KeyID – сквозной номер ключа в текущей серии ключей;

2) Username – заданное при генерации ключа имя пользователя, для связи с которым предназначен ключ;

3) IV – вектор инициализации, с помощью которого зашифрован ключ шифрования данных;

4) HashIV – вектор инициализации, с помощью которого зашифрован ключ выработки имитовставки;

5) KeyLen – длина ключа в байтах;

6) Key – зашифрованное тело ключа шифрования данных;

7) HashKey – зашифрованное тело ключа выработки имитовставки;

8) Hash – хеш ключа шифрования данных;

9) Hash_Keys_hash – хеш ключа выработки имитовставки;

10) Salt – соль, применяемая при шифровании ключа шифрования данных;

11) Hash_Salt – соль, применяемая при шифровании ключа выработки имитовставки.

4. Распределение и управление ключами шифрования

В целях обеспечения конфиденциальности ключей шифрования и ключей имитовставки в ходе их распределения применяется механизм шифрования.

Для шифрования ключей применяется алгоритм Qalqan в режиме OFB с вектором инициализации, указанном в теле ключа. В качестве ключа шифрования данных используется тысячекратный хеш от строки в формате Unicode, к которой добавляется соль, хранящаяся в теле ключа. Данная строка является паролем, с помощью которого пользователь может расшифровать ключ для последующего использования.

Пароль должен быть доставлен пользователю по защищенным каналам.

После получения ключа пользователь может изменить пароль и уничтожить файл ключа со старым паролем в целях безопасности.

Для обеспечения безопасности на уровне 1 и 2 согласно Государственному стандарту Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования» допустимо распределение ключей по каналам связи общего пользования при условии передачи паролей пользователей по защищёнными каналам связи.

Для обеспечения безопасности на уровне 3 и 4 согласно Государственному стандарту Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования» распределение ключей осуществляется посредством доверенных курьеров.

Каждый ключ используется только для одной цели. Запрещается использовать один и тот же ключ для шифрования и выработки имитовставки или для операций по разным направлениям связи. Ключи и пароли пользователей должны содержаться в секрете для обеспечения безопасности защищаемой информации.

5. Свойства безопасности протокола генерации, формирования, распределения и управления ключами

Аутентификация субъекта (Аутентификация сторон, Peer Entity Authentication) – проверка с подтверждением подлинности одной из сторон [2]. Файл ключей распределяется в зашифрованном виде, при их использовании требуется их расшифрование на специальном пароле, таким образом, осуществляется первичная аутентификация легитимного пользователя. Кроме того, передаваемые сообщения защищаются от несанкционированного изменения и подмены путем вычисления

имитовставки от них на специальном ключе имитовставки. Данных механизм позволяет осуществлять аутентификацию субъекта.

Аутентификация сообщения (Message authentication) – обеспечение аутентификации источника данных и целостности передаваемого сообщения [2]. От каждого сообщения вычисляется имитовставка на специальном ключе имитовставки, позволяющая гарантированно аутентифицировать источник данных и целостность передаваемого сообщения.

Аутентификация ключа (Key Authentication) — это свойство предполагает, что один из участников получает подтверждение того, что никакой другой участник, кроме заранее определенного второго участника (и, возможно, других доверенных участников), не может получить доступа ни к одному секретному ключу. [2] Файл ключей распределяется в зашифрованном виде, для расшифрования требуется секретный пароль, известный только легитимному пользователю.

Подтверждение правильности ключа (Key Confirmation, Key Proof of Possession) — один из участников получает подтверждение того, что второй участник (возможно, неопределенный) действительно обладает конкретным секретным ключом (либо имеет доступ ко всем ключевым материалам, необходимым для его вычисления) [2]. Файл ключей содержит необходимые исчерпывающие данные, позволяющие однозначно идентифицировать пользователей, с которыми возможен обмен зашифрованными сообщениями.

Конфиденциальность (Confidentiality, Secrecy) — свойство, состоящее в том, что специфический набор данных (обычно посылаемый или полученный как часть «защищенного» сообщения, а также сформированный на основе данных, полученных в результате обмена) не станет доступным или раскрытым для неавторизованных субъектов или процессов, а останется неизвестным противнику [2]. Файл ключей распределяется в зашифрованном виде. При первичном получении файла ключей пользователь должен сменить специальный пароль на собственный, в дальнейшем файл ключей будет храниться в зашифрованном виде именно на собственном пароле пользователя.

Литература.

1. Горлов Л.В., Ибраев Р.Б. Кандидат в национальные стандарты республики Казахстан — алгоритм шифрования Qalqan https://www.ruscrypto.ru/resource/archive/rc2021/files/02_gorlov_ibrayev.pdf (15.08.2021).

2. А.В. Черемушкин, Криптографические протоколы: основные свойства и уязвимости, ПДМ, 2009, приложение к № 2, 115–150.

3. И.А. Фомина, Управление ключами в криптографических системах, Вестник Нижегородского университета им. Н.И. Лобачевского, 2010, №4 (1), 165-169.

4. Государственный стандарт Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

5. https://www.akkamal.kz/products/tokens/akey.

О ВЫБОРЕ НАБОРА КРИТЕРИЕВ ОПТИМАЛЬНЫХ S-БЛОКОВ

Оспанов Р.М., Сейткулов Е.Н., Ергалиева Б.Б.
e-mail: ospanovrm@gmail.com
Евразийский национальный университет им.Л.Н.Гумилева, Казахстан

Аннотация. *Данная работа посвящена важному вопросу критериального подхода к оценке криптографической стойкости S-блоков. S-блоки являются одним из основных компонентов, определяющих нелинейность криптографического алгоритма. Для защиты алгоритмов от различных видов атак S-блоки должны обладать рядом криптографических свойств. Рассматривается набор критериев определяющих оптимальность S-блоков.*

Данная работа посвящена важному вопросу критериального подхода к оценке криптографической стойкости S-блоков. S-блоки (блоки подстановок) отображают блок из n битов в выходной блок из m битов (n и m не обязательно равны). Одно из формальных определений дается с помощью булевых и векторных булевых функций.

Пусть $B = GF(2)$.

Булевой функцией (от n переменных) называется отображение $F : B^n \to B$.

Векторной булевой функцией называется отображение $F : B^n \to B^m$. S-блоком называется векторная булева функция $F : B^n \to B^m$.

Координатными функциями (координатами) S-блока $F : B^n \to B^m$ называются булевы функции $f_i : B^n \to B$, $1 \le i \le m$, такие что $F = (f_1, f_2, ..., f_m)$.

Компонентными функциями (компонентами) S-блока $F : B^n \to B^m$ называются линейные комбинации m координатных функций S-блока.

S-блоки являются одним из основных компонентов, определяющих нелинейность криптографического алгоритма. Для защиты алгоритмов от различных видов атак S-блоки должны обладать рядом криптографических свойств. В настоящее время основными атаками, для которых имеют значения свойства S-блоков, используемых в криптографических алгоритмах, являются атаки, основанные на линейном, дифференциальном, алгебраическом методах криптоанализа. Другие методы анализа достаточно специфичны для отдельно взятого алгоритма, и, как правило, используют общую структуру алгоритма, а не отдельные его составляющие компоненты, как, например, S-блоки. При генерации S-блоков стремятся к достижению либо предельных показателей, обеспечивающих защиту от определенных видов атак, либо характеристик, обеспечивающих защиту от всех известных на текущий момент времени атак. Множество всех возможных критериев для оценки S-блоков можно разделить на безусловные критерии и условные критерии [1]. К безусловным относятся критерии, которым S-блоки должны удовлетворять в обязательном порядке, чтобы обеспечить их стойкость к основным криптоаналитическим атакам. К условным относятся дополнительные критерии, которым S-блоки должны удовлетворять, чтобы сравнивать S-блоки, удовлетворяющие безусловным критериям. Многие исследования показывают, что идеальных S-блоков, вероятнее всего, не существует. Поэтому было введено понятие оптимального S-блока, критерии которого определяются для конкретного криптографического алгоритма или класса криптографических алгоритмов) и являются оптимальными с точки зрения защиты от существующих видов атак [2].

S-блок $F: B^n \to B^m$ называется оптимальным, если он удовлетворяет набору критериев, определяющих криптографическую стойкость алгоритма, в котором используется данный S-блок, к основным видам криптоаналитических атак (линейной, дифференциальной, алгебраической).

Критерии оптимального S-блока могут быть установлены для целого класса криптографических алгоритмов, а также заданы и для отдельно взятого криптоалгоритма. При выборе блоков подстановок основными критериями являются нелинейность и дифференциальная равномерность. Дифференциальная равномерность является показателем стойкости против дифференциальной атаки.

S-блок $F: B^n \to B^m$ называется дифференциально δ-равномерным, если для каждого $a \in B^n$, $a \neq 0$, и каждого $b \in B^m$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений.

Также для оценки стойкости против дифференциальной атаки используется таблица распределения разностей или XOR-таблица.

Таблицей распределения разностей (XOR-таблицей) S-блока $F: B^n \to B^m$ называется матрица T^{XOR} размера $2^n \times 2^m$ с элементами $T^{XOR}_{a,b} = \left|\{x \in B^n : F(x) \oplus F(x \oplus a) = b\}\right|$, $a \in B^n$, $b \in B^m$.

Между дифференциальной δ-равномерностью и таблицей распределения разностей существует очевидная связь: $\delta = \max(T^{XOR}_{a,b})$.

Например, для 8-битных подстановок оптимальными значениями дифференциальной равномерности являются значения не больше 8.

Нелинейность является показателем стойкости против линейной атаки. Также для оценки стойкости используется таблица линейного распределения или таблица линейной аппроксимации.

Расстоянием Хэмминга $d(f,g)$ между булевыми функциями f и g от n переменных называется количество значений аргументов, на которых значения функций различаются, т.е. $d(f,g) = \left|\{x \in B^n : f(x) \neq g(x)\}\right|$.

Расстоянием Хэмминга $d(f,M)$ от булевой функции f от n переменных до некоторого множества M булевых функций от n переменных называется следующая величина $d(f,M) = min_{g \in M} d(f,g)$.

Нелинейностью $N(f)$ булевой функции $f: B^n \to B$ называется расстояние Хэмминга между f и множеством всех аффинных функций от n переменных.

Нелинейностью $N(F)$ S-блока $F: B^n \to B^m$ называется минимальная из нелинейностей компонентных функций S-блока.

Таблицей линейного распределения (таблицей линейной аппроксимации) S-блока $F: B^n \to B^m$ называется матрица T^{LAT} размера $2^n \times 2^m$ с элементами $T^{LAT}_{a,b} = \left|\{x \in B^n : (x,a) = (F(x),b)\}\right|$, $a \in B^n$, $b \in B^m$.

Между нелинейностью и таблицей линейного распределения S-блока существует непосредственная связь, выражаемая следующим соотношением: $N(F) = 2^{n-1} - \max(T^{LAT}_{a,b})$. Это позволяет легко находить значение нелинейности S-блока при известном значении максимума элементов таблицы линейного распределения, и наоборот. Таким образом, эти два свойства являются взаимозаменяемыми при оценке криптографической стойкости S-блока.

Оптимальными значениями нелинейности для 8-битных подстановок являются значения не меньше 100.

Алгебраическая степень и алгебраическая иммунность являются показателями стойкости против алгебраических атак.

Алгебраической степенью $deg(F)$ S-блока $F: B^n \to B^m$ называется число переменных в самом длинном слагаемом его алгебраической нормальной формы.

Алгебраической нормальной формой S-блока $F: B^n \to B^m$ называется представляющий его многочлен от n переменных над полем B^m вида $F(x_1, x_2, ..., x_n) = a \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus ... \oplus a_{12..n} x_1 x_2 ... x_n$, где $a, a_1, a_2, ... a_n, a_{12}, a_{13}, ..., a_{12..n} \in B^m$.

Булева функция $g: B^n \to B$ называется аннигилятором булевой функции $f: B^n \to B$, если $g \neq 0$ и $fg = 0$.

Алгебраической иммунностью булевой функции $f: B^n \to B$ называется минимальная из степеней аннигиляторов f и $f \oplus 1$.

Аннигилятором подмножества $E \subset B^n$ называется любая булева функция от n переменных, принимающая нулевое значение на этом подмножестве.

Алгебраической иммунностью подмножества $E \subset B^n$ называется минимальная алгебраическая степень всех ненулевых аннигиляторов этого подмножества.

(Базовой) алгебраической иммунностью S-блока $F: B^n \to B^m$ называется минимальная алгебраическая иммунность всех прообразов $F^{-1}(z)$ элементов $z \in B^m$.

(Графической) алгебраической иммунностью S-блока $F: B^n \to B^m$ называется алгебраическая иммунность графа $\{(x, F(x)): x \in B^n\}$ S-блока F.

(Компонентной) алгебраической иммунностью S-блока $F: B^n \to B^m$ называется минимальная алгебраическая иммунность компонентов S-блока F.

В случае 8-битных подстановок оптимальными значениями алгебраической степени являются значения не меньше 7, а максимальным значением алгебраической иммунности считается 3 при 441 уравнениях. А в случае подстановок 4 в 4 бита критерий алгебраической иммунности не играет большой роли, так как они могут быть описаны системой уравнений второй степени. Но в тоже время он не может равняться 1.

Еще в набор критериев оптимального S-блока можно включить период и количество неподвижных точек и противоположных неподвижных точек.

Периодом элемента $a \in B^n$ относительно S-блока $F: B^n \to B^n$ называется наименьшее положительное целое число r такое, что $F^r(a) = a$.

Элемент $a \in B^n$ называется неподвижной (фиксированной) точкой S-блока $F: B^n \to B^n$, если $F(a) = a$.

Элемент $a \in B^n$ называется противоположной неподвижной (фиксированной) точкой S-блока $F: B^n \to B^n$, если $F(a) = \overline{a}$, где $\overline{a} \in B^m$ такой, что $a \oplus \overline{a} = 0$.

Количество неподвижных и противоположных неподвижных точек должно быть как можно меньше для обеспечения стойкости против статистического криптоанализа.

Важным свойством определяющим оптимальность S-блока является биективность.

S-блок $F : B^n \to B^n$ называется биективным, если она инъективна и сюръективна, то есть одновременно выполняются следующие условия:

1) для любых элементов $a', a'' \in B^n$, если $a' \neq a''$, то $F(a') \neq F(a'')$ (инъекция),
2) для любого элемента $b \in B^n$ существует элемент $a \in B^n$ такой, что $F(a) = b$ (сюръекция).

Это свойство эквивалентно обратимости S-блока.

Таким образом, в случае n=m=8 набор критериев оптимальных S-блоков состоит из дифференциальной равномерности, нелинейности, алгебраической степени, алгебраической иммунности, количество неподвижных и противоположных неподвижных точек и период, а также биективность.

Информация о поддержке. Данная работа выполнена при финансовой поддержке грантового финансирования КН МОН РК, № AP09258274.

Литература

1. Gorbenko, I, Kuznetsov, A., Gorbenko, Y., Pushkar'ov, A., Kotukh Y., Kuznetsova, K. Random S-Boxes Generation Methods for Symmetric Cryptography */ 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON),* 2019, pp. 947-950, doi: 10.1109/UKRCON.2019.8879962.

2. Казимиров А.В. Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов. Диссертация на соискание учёной степени кандидата технических наук, специальность 05.13.21 – системы защиты информации. Харьковский национальный университет радиоэлектроники, Харьков, 2013.

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ПРОТИВОДЕЙСТВИЯ МАНИПУЛИРОВАНИЮ ОНЛАЙН-КОНТЕНТОМ

Ш.А. Сейдалиев, А.Д.Куракбаев
email:askar0070@gmail.com
Академия Комитета Национальной Безопасности Республики Казахстан, Казахстан

Аннотация: *в данной статье рассматриваются задачи по созданию методов и средств по проведению информационных операций на открытых каналах ресурсов Интернет в рамках противодействия манипулированию. Авторы в рамках информационного противоборства предлагают исследовать создание системы мониторинга социальных ресурсов сети Интернет на территории Республики Казахстан. В частности, систему раннего предупреждения для поэтапной разработки теоретических и технических основ защиты общества от манипулирующего воздействия Интернетом.*

Ключевые слова: манипулирование, информационные технологии, пропаганда, противодействие, мониторинг, контент;

В современном мире в условиях развития глобального информационного общества информация становится решающей составляющей в управлении обществом. Причем непосредственными носителями информации являются средства массовой коммуникации.

Считаем, что сегодня манипулирование сознанием возможно благодаря контролю над информацией и коммуникациями, которые определяют правила человеческого общения в обществе. Манипуляция, как правило, нацелена на то, чтобы для достижения своих целей заставить большинство (или меньшинство) участвовать (или не участвовать) в укоренившейся практике. Она является одним из основных средств регулирования социальных отношений, и базируется на использовании информационного аппарата и аппарата формирования идей [1].

Главным индикатором манипулирования является скрытость и неочевидность воздействия с целью целенаправленного изменения поведения системы.

Следует отметить, что государство – это основной инструмент, который обеспечивает безопасность исходной системы, то есть сам народ, его культура, искусство, наука, территория, богатство этого народа. Это управляющая структура. Уничтожить эту структуру и возродить заново можно с применением современных технологий. Информационную войну по большому счету нет смысла вести против государства, ее ведут за государство, за контроль над государством, которое становится инструментом в руках победителя для управления побежденным народом.

В этой связи задачами государственных органов, в первую очередь, Комитета национальной безопасности, Министерства внутренних дел, Генеральной прокуратуры, Верховного суда и Антитеррористического центра Республики Казахстан в данной ситуации должны стать надежная защита общества от неблагоприятного информационного воздействия и принятие адекватных мер по разработке средств информационного противодействия и преследование в судебном порядке тех, кто разрабатывает и применяет информационное оружие. В то же время

наряду с использованием технических мер для противодействия манипулированию интернет технологиями необходимо осуществлять и меры организационного характера, направленные от повышения качества нормативно-правовых документов, регулирующих эту сферу, до повышения уровня информационной культуры граждан Республики Казахстан.

Проблема информационной безопасности в контексте вызовов, рисков, угроз и трудностей, с которыми столкнулось мировое сообщество в начале XXI века, в современном мире резко возрастает. Растущая уязвимость государственных учреждений и средств массовой информации в современную эпоху привела к тому, что «эксплуатация» или манипулирование стали важными компонентами социальных, культурных и политических преобразований, затрагивающих фундаментальные интересы личности и общества. Информационная безопасность является стратегическим приоритетом и ключевой задачей обеспечения национальной безопасности, о чем изложено в Законе «О Национальной безопасности» [2].

Из закона вытекает, что в связи с открытостью национального информационного пространства и популярностью зарубежных средств массовой информации, возникает реальная угроза информационного влияния на общественное сознание населения. Информационное влияние может выражаться как в виде прямого навязывания идей, противоречащих национальным интересам страны, так и путем манипулирования информацией или ее тенденциозным освещением и комментированием.

Для противодействия подобному манипулированию общественным сознанием требуется постоянно совершенствовать эффективность государственной информационной политики и её реализации, расширить открытость, прозрачность деятельности государственных органов, повысить обеспеченность права граждан на информацию.

Однако, без выработки действенных механизмов по реализации этих нормативных документов, все эти усилия окажутся напрасными. В случае выхода ситуации из-под контроля, как это было и происходит по сценариям Ливии, Египта, Кыргызстана, Украины, Сирии и Ирака, остановить массовые беспорядки без кровопролития будет практически невозможно.

В рамках исследования данного вопроса существует проблемное поле и по нормативным составляющим. В Концепции по информационной безопасности Республики Казахстан определяются меры по выявлению и недопущению скрытого воздействия на общественное сознание со стороны других государств, транснациональных корпораций, различных структур. Однако эти меры не отражены в законодательстве, так как отсутствуют методология выявления скрытых угроз и определение основополагающего элемента информационной безопасности - это общественная нравственность. Кроме того, Концепция содержит идею об информационной войне, но в законах она не регламентирована.

Существенной проблемой является и то, что Республика Казахстан зависима от импорта информационных технологий, средств информатизации и защиты информации, использование которых может причинить ущерб национальным интересам страны.

Серьезные угрозы несет в себе проблема неконкурентоспособности отечественного информационного контента. Его качество остается недостаточным

для полноценной конкуренции с иностранным информационным и развлекательным продуктом.

В этих условиях нужно добиваться реформирования законодательства по развитию отечественного информационного пространства и поиск решений технических возможностей для осуществления контроля за информационным контентом. Государство должно выполнять роль регулятора и потребителя информационных ресурсов, ограничивая те иностранные СМИ, которые распространяют неблагонадежную продукцию на территории Казахстана.

В то же время, использование деструктивными силами новейших достижений информационных технологий, проблема нехватки квалифицированных кадров в информационно-коммуникационной сфере затрудняют полноценно использовать средства мониторинга. К сожалению, использование анонимных серверов, VPN-сервисов, создание анонимных учетных записей позволяет деструктивным силам обходить средства мониторинга сетей. Например, Интернет-сервисы верификации учетных записей, такие как sms-reg.com, hottle.com, virtualnom.ru, 7sim.net и т.д. позволяют не затрачивать средства на покупку новых sim-карт и создавать большое количество учетных записей в приложениях, требующих телефонный номер для регистрации в Интернет-ресурсах. А скрытие адресов отправителей сообщений с использованием анонимных серверов позволяют Интернет-сервисы, такие как kebrum.com, которые предоставляют выход через сервера, находящиеся на территориях других стран.

Для террористических и экстремистских целей используют возможности Интернет в так называемых «луковичных сетях» (Tor сети), которые обеспечивают анонимность пользователей. *Tor (The Onion Router) является свободным программным обеспечением и открытой сетью, для защиты от анализатора трафика, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания.*

Но Tor-трафик, как и другие средства анонимизации в сети видны и могут быть блокированы. Иран, например, наряду с другими методами использовал частичную блокировку зашифрованного трафика с помощью Deep packet inspection (DPI) [3]. А метод досудебной блокировки является относительно эффективным методом воздействия на владельца домена, чтобы запрещенный контент исчез с ресурса в кратчайшие сроки.

Социальные сети сегодня приобрели глобальный размах. Наряду с транснациональными сетями, такими как Facebook, Twitter, Instagram, TikTok развиваются и национальные социальные пространства. Для Казахстана в рейтинг социальных сетей по посещаемости входят собственные социальные сети и новостные платформы.

Считается, что одним из наиболее эффективных средств прогнозирования манипулирования является мониторинг информационных ресурсов [4].

Как правило, мониторинг включает в себя:

– формирование дайджестов электронной информации по заданной теме;
– подсчет частоты и объема упоминаний в электронных ресурсах тем, персон, товаров, компаний с учетом характера подачи информации;
– составление рейтинга упоминания персон, компаний или тем;
– отслеживание рекламных и PR-кампаний и анализ их эффективности;

– выявление начала, интенсивности и степени агрессивности информационных кампаний, выявление направленности их позитивного или негативного воздействия на население;

– выявление скрытых взаимосвязей между объектами или субъектами мониторинга в информационных потоках;

– психолингвистическая экспертиза массивов текстов статей, сюжетов, выступлений в СМИ, рекламных роликов и т.д. с целью выявления подсознательного воздействия текстов на аудиторию.

Создание контролируемых информационных ресурсов в Интернете для публикации контрпропаганды является еще одним вариантом механизма раннего предупреждения манипулирования массовым сознанием. Это могут быть записи в блогах, форумах и чатах, комментарии к статьям и запискам других людей на информационных сайтах и в социальных сетях и.т.д.. Осуществлять все это необходимо с целью формирования ценностных жизненных ориентаций. Таким образом, не изменяя моральным принципам и не поддаваясь манипулированию других государств, информацию недоброжелателей можно оставить без своего потребителя.

Глобализация информационного пространства вызывает необходимость для каждого национального государства определиться в отношении своего места и роли в глобальных геополитических процессах. Только на основе такого самоопределения возможен выбор внутренней и внешнеполитической стратегии.

Подводя итог вышесказанному, мы считаем, что по предпринятому в работе проблемы противодействия угрозам манипулирования общественным сознанием с использованием информационных технологий следует предпринять:

- формирование специальных структур для выявления признаков использования информационных технологий с целью манипулирования общественным сознанием.

Информационно-коммуникационная безопасность и нормальное функционирование всех социальных субъектов будет зависеть от эффективности деятельности этих структур.

Также следует отметить, что использование приемов манипулирования имеет значительно меньший эффект в аудитории высокообразованной, с устойчивой системой обоснованных взглядов, а также знающей технику манипулирования и обладающей некоторым опытом целенаправленной социально-психологической защиты. Кроме того, аудитория с высоким уровнем политической культуры и достаточной степенью информированности менее подвержена негативному влиянию и манипулированию.

Интенсивный рост технологий требует от общества изменений, в том числе и в модели образования. Сегодня очевидно, что необходима интеграция информации, каналов передачи информации, контента. Отсутствие целостной государственной политики в области информационной грамотности приводит к тому, что этот процесс проходит стихийно, информационная грамотность понимается узко, исключительно как ликвидация компьютерной грамотности. Поэтому государство должно отдельно сосредоточить свои усилия на интеллектуальном развитии своих граждан, формировать чувство гражданственности, поддерживать общественный диалог в медиа-среде.

Успешное противодействие манипулированию контентом и восстановление доверия к социальным сетям - без ущерба для Интернета и свободы СМИ -

потребуют времени, ресурсов и творчества. Одним из шагов в данном направлении является просвещение населения, направленное на обучение граждан тому, как обнаруживать фейковые или вводящие в заблуждение новости и комментарии. В свою очередь технологические компании государственного, квазигосударственного сектора должны внести свой вклад, пересмотрев алгоритмы курирования-фильтрации новостей, а также более активно отключая ботов и фейковые учетные записи, используемые в антидемократических целях.

Литературы

1. *Каландаров К.Х.* Управление общественным сознанием. Роль коммуникативных процессов. - М.: Гуманитарный центр Монолит, 1998.

2. Закон Республики Казахстан от 06.01.2012г. №527-IV «О национальной безопасности»

3. Блокировка зашифрованного трафика. Доступно онлайн на: https://christopher-parsons.com/is-iran-now-actually-using-deep-packet-inspection/ (23.08.2021)

4. Мониторинг социальных сетей. Доступно онлайн на: https://www.unisender.com/ru/blog/idei/monitoring-sotsialnyh-setey/ (23.08.2021)

БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ

Абдалы Ш.А.
e-mail: shyngys.abdaly@gmail.com

Аннотация. *Облачные вычисления является одним из актуальных и интересных направлений в мире информационных технологий. В связи с этим необходимо защищать информацию, в частности пользовательские данные хранящиеся в облаке. Облачные провайдеры несут ответственность за обслуживание и управление информацией в облачном хранилище. В этой статье показаны основные критерии безопасности в облаке.*

Введение

Облачные вычисления это технология которая позволяет использовать программы, сервисы, хранилища, серверы по мере необходимости, независимо от местонахождения с минимальной тратой ресурсов. Национальный Институт Стандартов и Технологий дало определение облачным вычислениям, как модель для обеспечения повсеместного, удобного сетевого доступа по требованию к общему объединению конфигурируемых вычислительных ресурсов (например, сетей, серверов, хранилищ, приложений и сервисов), которые могут быть быстро предоставлены и выпущены с минимальными усилиями по управлению или взаимодействие с поставщиком услуг[1]. Если сильно упростить это определение, то облачные вычисления это доступ к данным и программам через интернет, вместо использования жесткого диска компьютера. Но важно понимать что облако это не только хранилище, а также технология предоставлющая различные виды услуг для разных видов задач. Так как задачи все разные, использование большого объема услуг для маленькой задачи нецелесообразно, поэтому провайдеры предоставляющие услуги разделяют их на категории, такие как инфраструктура как сервис, платформа как сервис, программное обеспечение как сервис. Иначе говоря все что угодно для пользователя, компании можно предоставить ввиде услуг, это и есть технологии облачных вычислений. Также облачными технологиями могут пользоваться как один человек, так и группа людей, компании и организации. По этой причине облака можно разделить на публичные, приватные, для сообщество и гибридные. Каждый ресурс в облаке можно оплачивать по факту использования.

Проблемы безопаносности в облачных вычислениях

Для обычного пользователя, зачастую, облако это некое место, где можно хранить личные данные. Облачные хранилища в таком случае выполняют роль обычных внешних накопителей, только с отличием увеличенной памяти, а также без физической формы. Физическую форму имеет отдаленный центр данных, то есть серверная компании которая является облычным провайдером. Удобность таких хранилищ это легкая доступность информации со всех устройств, единственным критерием является подключенность к интернету. Но так как облако это не только хранилище, нужно отметить какими особенностями отличается данная технология. Облако действительно имеет ряд функций, основными из которых являются[2]:

1) Виртуальная инфраструктура: предоставляет виртуализированную технологическую платформу, которая позволяет физическим ресурсам, обработке и

сетевым возможностям быть виртуальными. Какой бы ни была структура развертывания, облачные технологии стремятся максимально использовать доступные технологии для ряда участников [3].

2) Динамические закупки: удовлетворение требований поставщика на основе текущих критериев спроса. Это делается автоматически за счет технологических достижений программного обеспечения, что позволяет расширять возможности обслуживания и сокращать их по мере необходимости. Его динамическое масштабирование должно достигаться при сохранении высокого уровня безопасности и надежности.

3) Доступ к сети - обеспечивает доступ к Интернету с широкого спектра устройств, таких как персональные компьютеры, ноутбуки и мобильные устройства. Развертывания облачных сервисов включают в себя все, от использования бизнес-приложений до новейших приложений на новейших интеллектуальных устройствах.

4) Контроллинг - использует обработку данных для контроля и автоматизации инфраструктуры, а также предоставления информации о мониторинге и выставлении счетов.. Таким образом, с пользователей взимается плата за услуги в зависимости от того, сколько они использовали в течение платежного цикла [3].

Перечисленные возможности предлагает облачный провайдер. Облачный провайдер несет ответственность за обслуживание и управление информацией в облачном хранилище. Очевидно, что защита информации - одна из основных задач поставщика облачных услуг [4]. По мнению авторов статьи[5] безопасность облачных систем можно оценить по 3 факторам таких как, Конфиденциальность, Целостность и Доступность. Конфиденциальность относится к защите личных данных от раскрытия неавторизованным пользователям. Данные пользователей часто хранятся в открытом формате. Таким образом, облачные провайдеры несут ответственность за сохранение конфиденциальности клиентских данных в течение всего их жизненного цикла. Жизненный цикл данных состоит из шести этапов: создание, хранение, использование, совместное использование, архивирование и уничтожение[6]. Это означает что облачный провайдер должен обезпечить безопасность данных на всех этапах их жизни. Как только данные созданы они должны беспрепятственно передвигаться между этими этапами. Шифрование данных является одним из методов сокрытия данных от несанкционированного пользования. Данные обычно шифруются на этапе совместного использования[7]. Целостность относится к свойству безопасности актива, то есть данных, которое гарантирует, что он не был изменен каким-либо сторонним персоналом, который не уполномочен на такую деятельность. Таким образом, точность и корректность актива по отношению к его владельцу обеспечивается этим свойством. Некоторые проблемы связанные с целостностью в облаке:

Атака SQL инъекцией может изменить содержимое таблицы используя уязвимости веб-серверов и внедряя вредоносные коды в систему. Атаки с использованием SQL-инъекций возникают, когда данные, предоставленные внешним пользователем, напрямую включаются в SQL - запрос, предварительно не проверяясь должным образом[8].

В атака межсайтовый скриптинг обычно для сбора данных используется гиперссылка с вредоносным кодом. После сбора данных веб-приложением вредоносные данные отправляются пользователю в виде выходной страницы, и пользователь считает, что это допустимый контент с веб-сайта. Межсайтовый

скриптинг - наиболее распространенная атака для извлечения информации, хранящейся в пользовательских куки-файлах, что может создать проблему с конфиденциальностью. Злоумышленник получает возможность захватывать информацию о сеансе, такую как идентификатор пользователя, пароли, информацию о кредитной карте и другие.

Атака с упаковкой является еще одной распространенной атакой для веб-сервисов и становится весьма вероятной для облачных систем. Во время перевода сообщений SOAP на уровне TLS (служба транспортного уровня) их содержимое, а также подпись дублируются и отправляются на сервер как подлинный пользователь. Таким образом, злоумышленник может вмешиваться в облако и запускать вредоносные коды, чтобы прервать обычное функционирование облачных серверов[10].

Доступность - один из наиболее важных аспектов безопасности, который должен поддерживать облачным провайдером. Различные коммерческие предприятия, которые используют облачные сервисы для обслуживания своих клиентов, должны гарантировать доступность этих сервисов, поскольку малейшее время простоя может привести к крупным денежным потерям, которые не подлежат возмещению.

Большинство Denial of Service атак нагружают сервисные ресурсы, чтобы блокировать или задерживать ответ на запросы пользователей. В отличие от традиционных сетевых DDoS-атак, DDoS-атаки на облако приводят к потенциальным нарушениям, которые пересекают традиционные организационные границы. Это связано с тем, что данными управляет облачный провайдер, и данные для разных организаций могут храниться на одном и том же физическом оборудовании. Таким образом, масштабируемость облака-это то, что создает его основные проблемы безопасности по сравнению с традиционными сетями[11].

Существуют различные методы и процедуры, применяемые для повышения безопасности данных, связанных с конфиденциальностью, целостностью и доступностью на разных этапах жизненного цикла данных. Некоторые из важных методов перечислены ниже[12]:

- Зашифровать данные на этапе посовместного использования с помощью алгоритмов которые являются стандартами, такие как AES с 256 бит блоком, RSA как один из наиболее стойких шифров.
- Использования хэш алгоритмов для сохранения конфиденциальности при программных, а также конфигурационных ошибках.
- Для проверки целостности данных может быть использован аудит третьей стороны [13, 14].
- Схема доказуемого владения данными (PDP) была инициирована Атениезе и др. для статистического исследования правильности

данных без извлечения данных, переданных на аутсорсинг в облачное хранилище

- Не хранить ключи шифрования вместе с зашифрованными данными
- Внедрить надлежащие методы идентификации и управления, для доступа пользователей к данным.
- Использовать дублирование данных, резервное копирование и устойчивые системы для решения проблем доступности.

Заключение

Информационные технологии эволюционно прогрессируют и приводят к концепции облачных технологий. Различные приложения и сервисы могут предоставляться в облаке благодаря его различным перспективным и интересным характеристикам, сервисам и приложениям. Проблемы с облаком в основном связаны с безопасностью и конфиденциальностью данных. Здесь представлен обобщенный взгляд на эти проблемы, чтобы подчеркнуть важность понимания недостатков безопасности платформы облачных вычислений и разработки подходящих контрмер для них.

Литературы

1. Mell P, Grance T. Version 15 The NIST definition of cloud computing //National Institute of Standards and Technology; October 7, 2009. – https://csrc.nist.gov/publications/detail/sp/800-145/final(17.08.2021).

2. Alam, T. // Cloud Computing and its role in the Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1(2), 2020. – P.82-93. https://pandawan.aptisi.or.id/index.php/att/article/view/59(17.08.2021).

3. Logo, Small. / Introduction to Cloud Computing // Dialogic

4. Tanweer Alam, Baha Rababah / Convergence of MANET in Communication among Smart Devices in IoT // International Journal of Wireless and Microwave Technologies(IJWMT), Vol.9, No.2, 2019. – P.1-10

5. Arjun Bardhan, Koyal Gupta,Payel Saha, Mahasweta Pal,Manjima Bose, Kaushik Basu,Saunak Chaudhury, Pritika Sarkar / Cloud Computing Security Challenges & Solutions – A Survey // ACADEMIA, 2018. – P.347-356.

6. A. Reed, C. Rezek, C and P. Simmonds / Security Guidance for Critical Area of Focus in Cloud Computing V3.0 // Cloud Security Alliance (CSA), 2011. – P.1-177.

7. Elsevier B.V / Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications. – 2018.

8. Niharika Singh, Ajay Jangra, Upasana Lakhina, Rajat Sharma/ SQL Injection Attack Detection & Prevention over Cloud Services // International Journal of Computer Science and Information Security (IJCSIS). – Vol. 14, No. 4, April 2016

9. Neeta Sharma, Mahtab Alam, Mayank Singh / Web Based XSS and SQL Attacks on Cloud and Mitigation // Journal of Computer Science Engineering and Software Testin, 2015, P.1-10

10. Kazi Z & S.V V / Security Attacks and Solutions in Clouds. – 2017

11. Andrew Carlina , Mohammad Hammoudehb , Omar Aldabbas / Defence for Distributed Denial of Service Attacks in Cloud Computing // The International Conference on Advanced Wireless, Information, and Communication Technologies AWICT. – 2015

12. P. Ravi Kumar , P. Herbert Raj , P. Jelciana / Exploring Data Security Issues and Solutions in Cloud Computing // 6th International Conference on Smart Computing and Communications, ICSCC. – 2017, 7-8 December 2017

13. C. Wang, S. Chow, Q. Wang, K. Ren and W. Lou / Privacy-Preserving Public Auditing for SecureCloud Storage // IEEE Transactions on Computers.- Vol. 62, Iss. 2, 2013, P.362-375.

14. B. Balusamy, P. Venkatakrishna, A. Vaidhyanathan, M. Ravikumar and N. Devi Munisamy / Enhanced Security Framework for Data Integrity using Third-Party Auditing in the Cloud System // In Proceedings of the Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Advances in Intelligent Systems and Computing, Springer. – Vol. 325, 2015, P.25-31.

15. G. Atieniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song / Provable Data Possession at Untrusted Stores // In Proceedings of the 14th ACM conference on Computer and Communication Security. – 2007, P.598-609

Содержание

Вступительное слово		4
Секция 1. Современные проблемы прикладной математики, информатики и теории управления. Моделирование и оптимизация сложных систем и бизнес процессов. Вычислительная математика, численный анализ и программирование, математическая логика. Теория статистики. Статистические методы		5
Шакерхан К.О., Сагындыков К.М., Мешечкин В.В., Анибаев С.К., Абильмажинов Е.Т., Конырханова А.А.	РАЗРАБОТКА БИОРЕАКТОРА ГОРИЗОНТАЛЬНОГО ТИПА ДЛЯ ФЕРМЕРОВ КАЗАХСТАНА С УЧЕТОМ КЛИМАТИЧЕСКИХ И ЭКОНОМИЧЕСКИХ УСЛОВИЙ И МАТ.МОДЕЛИ ДЛЯ УПРАВЛЕНИЯ ПРОЦЕССАМИ	6
Хисамиев З.Г.	КОМПАНЬОНЫ ПОЛЯ РАЦИОНАЛЬНЫХ ЧИСЕЛ	18
Ташев А.А., Аршидинова М.Т.	СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЧИСЛЕННОГО И АНАЛИТИЧЕСКОГО МЕТОДОВ РЕШЕНИЙ ЗАДАЧИ РАСПРЕДЕЛЕНИЯ ТЕМПЕРАТУРЫ ПО ДЛИНЕ СТЕРЖНЯ ПЕРЕМЕННОГО СЕЧЕНИЯ.	24
М.Н. Калимолдаев, Т.Ж. Мазаков, Ш.А. Джомартова.	НОВЫЕ ПОДХОДЫ РЕШЕНИЯ ЗАДАЧ МОДЕЛИРОВАНИЯ ПАВОДКОВЫХ И ПРОРЫВНЫХ ВОЛН И ПРОГНОЗИРОВАНИЕ АВАРИЙНОЙ СИТУАЦИИ	44
Байбеков С.Н.	ҚОЛДАНБАЛЫ МАТЕМАТИКАНЫ ЭКОНОМИКА ЖӘНЕ ҚҰҚЫҚТАНУ САЛАЛАРЫНА ҚОЛДАНУДЫҢ ЕРЕКШЕЛІКТЕРІ	49
Абилкаева Ж.Н., Габбасов М.Б.	МОДЕЛИРОВАНИЕ СЕБЕСТОИМОСТИ УСЛУГ В ЖЕЛЕЗНОДОРОЖНОЙ ОТРАСЛИ В ВИДЕ МНОГОМЕРНОГО ИЗМЕРИТЕЛЯ	54
Т.Ж. Мазаков, А.А.Саметова	ОРМАН ЖӘНЕ ДАЛА ӨРТТЕРІНІҢ ДАМУЫН БАҚЫЛАУ ЖҮЙЕСІ	60
Sagdat Okimbek, Razak Nurlan, Bulgyn Dyussenkulova, Shynarbekova Tolkyn, Daniyarbekov Sanzhar, Bashkeyeva Symbat, Akhmetov Iskander	RESEARCH PROPOSAL: SENTIMENT ANALYSIS OF FINANCIAL NEWS	64
L. Yermekkyzy, Zh. Madibaiuly.	VARIATIVE SOLUTION OF THE COEFFICIENT INVERSE PROBLEM FOR THE HEAT EQUATIONS IN A QUADRANGULAR PLANE	68

Kudaykulov A.K., Begaliyeva K.B., Arshidinova M.T.	APPLICATION OF THE ENERGY METHOD TO SOLVE THE NONLINEAR PROBLEM OF THERMOELASTICITY OF A ROD OF VARIABLE SECTION.	72
Козбакова А.Х., Амиргалиев Е.Н., Калижанова А.У., Маликова Ф.У., Атаниязова А., Меліс З,	ТӨТЕНШЕ ЖАҒДАЙЛАРДА ЭВАКУАЦИЯЛАУ ЕСЕПТІҢ МАТЕМАТИКАЛЫҚ ӘДІСТЕРІ МЕН МОДЕЛЬДЕРІ	78
Секция 2. Информационно-телекоммуникационные технологии. Системы и сети передачи данных. Интернет-технологии. Облачные технологии. Параллельные вычисления. Распределённые вычисления. Суперкомпьютерные и кластерные системы. Обработка больших объёмов данных (Big-data). Геоинформационные системы и технологии. Инновационные образовательные технологии		85
Бесбаева М.Қ., Медерова А. Ж.	БАЙЛАНЫС ИНЖЕНЕРЛЕРІН ҚАЙТА ДАЯРЛАУ БАРЫСЫНДА БІЛІМ БЕРУДІҢ ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯСЫ РЕТІНДЕ ИНЖЕНЕР КЕЙСІ - ӘДІСІНІҢ ҚОЛДАНЫЛУЫ	86
Мекебаев Н.О., Назкенова Б.Б., Касымова Д.Т.	БІЛІМ БЕРУДІ ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ КИБЕРПЕДАГОГИКА	91
Мухитова А.А. Адалбек А. Еримбетова А.С.	МӘЛІМЕТТЕРДІ ЕНГІЗУ МЕН ӨҢДЕУГЕ АРНАЛҒАН ГЕТЕРОГЕНДІК АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІҢ ӘКІМШІЛІК ГРАФИКАЛЫҚ ИНТЕРФЕЙСІН ҚҰРУДАҒЫ АДАПТИВТІ ТЕХНОЛОГИЯЛАР	96
Сейсенбекова П.Б.	ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДА КРИТЕРИАЛДЫ БАҒАЛАУ АРҚЫЛЫ АҚПАРАТТЫҚ-ИНТЕЛЛЕКТУАЛДЫ ҚҰЗЫРЕТТІЛІКТІ ҚАЛЫПТАСТЫРУ	103
Shakerkhan K. O., Meshechkin V. V.	MATHEMATICAL MODELING OF BIOREACTOR PROCESS CONTROL	109
Svanov A., Kintonova A.	DESIGNING AND ADMINISTERING A WEB APPLICATION CREATED WITH ASP.NET CORE TECHNOLOGY	121
Terekhov A.G., Abayev N.N.	SATELLITE MONITORING ARABLE LAND OF XINJIANG CHINA ON BASE OF NDVI-C6 AND LST-C6 FEWS NET DURING 2002-2021	126
Ермолдина Г.Т., Алипбаев К.А., Аден А.Е.,	МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ ОЦЕНКИ ЭКОЛОГИЧЕСКОГО УЩЕРБА ПРИ	131

Оразалы Е.Е., Бапышев А.М., Суйменбаев Н.Б.	ЭКСПЛУАТАЦИИ ПЕРСПЕКТИВНЫХ РАКЕТ-НОСИТЕЛЕЙ	
А.Е. Ибраимкулов, А.С.Еримбетова.	РАЗВИТИЕ ЦИФРОВОЙ ГРАМОТНОСТИ УЧАЩИХСЯ С НАРУШЕНИЯМИ СЛУХА В СПЕЦИАЛЬНЫХ (КОРРЕКЦИОННЫХ) ШКОЛАХ	140
Вуйцик В., Кисала П., Калижанова А.У., Козбакова А.Х., Кунелбаев М., Едилхан Д., Айткулов Ж.С.	ЧИСЛЕННЫЙ И ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ ОПРОСА СОГЛАСОВАННОГО ФИЛЬТРА ДАТЧИКОВ НА ОСНОВЕ ВРБ	146
Вуйцик В., Кисала П., Калижанова А.У., Козбакова А.Х., Кунелбаев М., Едилхан Д., Айткулов Ж.С, Искакова М.Т.	АНАЛИЗ МЕТОДОВ ОБРАБОТКИ СИГНАЛОВ ОТ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ	160
Вуйцик В., Кисала П., Калижанова А.У., Козбакова А.Х., Кунелбаев М., Айткулов Ж.С., Оразбеков Ж.	ИССЛЕДОВАНИЕ И АНАЛИЗ ОБРАБОТКИ СИГНАЛОВ ОТ ВОЛОКОННО-ОПТИЧЕСКИХ ДАТЧИКОВ НА ОСНОВЕ НАКЛОННЫХ ПЕРИОДИЧЕСКИХ СТРУКТУР	171
Едилханулы Мейир	ОБ ОДНОМ ПОДХОДЕ ПОСТРОЕНИЯ ГРУППОВЫХ РЕШЕНИЙ В ЗАДАЧАХ КЛАССИФИКАЦИИ	194
Ескермес Т.Е., Бимурат Ж., Мукашева А.К.	ОЦЕНКА ЭПИДЕМИОЛОГИЧЕСКОЙ СИТУАЦИИ САХАРНОГО ДИАБЕТА В РЕСПУБЛИКЕ КАЗАХСТАН: НОВОЕ ВИДЕНИЕ	199
М.С. Әлиасқар, Т.Ж. Мазаков, Г.С. Байрбекова, Н.Т. Исимов, Т.С. Шорманов, Д.К. Мухаев.	ОБРАБОТКА ГОЛОСОВОЙ ИНФОРМАЦИИ ДЛЯ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ	205
О.Долинина, М.Мансурова, Ж.Байгараева, С.Баязитова	ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ ГОРОДСКИМ ТРАНСПОРТОМ ЗА СЧЕТ ВНЕДРЕНИЯ УМНЫХ ПАРКОВОК	210

Тен В.В.	ОБМЕН ДАННЫМИ С 1С ПРЕДПРИЯТИЕМ ПРИ ПОМОЩИ ТЕХНОЛОГИИ HTTP СЕРВИСОВ	215
Шакерхан К.О., Мешечкин В.В.	МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ УПРАВЛЕНИЯ ПРОЦЕССАМИ БИОРЕАКТОРА	219
Yevgeniy Fedkin, Saule Smailova, Vitaly Zuev, Saule Kumargazhanova, Natalia Denissova, Elvira Aitmukhanbetova	CLASSIFICATION OF LMS CONTROL AND MONITORING SERVICES	232
Хакимова Т.Х., Абдиахметова З.М.	АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАРДЫ ДЕНСАУЛЫҚ САЛАСЫНДА ПАЙ-ДАЛАНУ	245

Секция 3.Технологии искусственного интеллекта. Интеллектуальные системы управления. Речевые технологии и компьютерная лингвистика. Распознавание образов и обработка изображений. Биоинформатика и биометрические системы. Человеко-машинное взаимодействие. Машинное обучение. Интеллектуальные робототехнические системы 250

Г.А.Тюлепбердинова, М. Е. Мансурова, А.Шілмағамбетова.	СТУДЕНТТЕРДІҢ ДЕНСАУЛЫҚ ЖАҒДАЙЫН БАҒАЛАУҒА АРНАЛҒАН ДЕРЕКТЕРДІ ТАЛДАУДА ҚОЛДАНЫЛАТЫН ӘДІС – ТӘСІЛДЕР	251
Г.С. Ыбытаева, О.Ж. Мамырбаев, Н.Ф. Хайрова, Б.Ж. Жумажанов.	ҚАЗАҚ ТІЛІНДЕГІ МӘТІНДЕРДЕ КОЛЛОКАЦИЯЛАРДЫ АНЫҚТАУДЫҢ СТАТИСТИКАЛЫҚ ӘДІСТЕРІН ТАЛДАУ	256
Azamat Moldabek, Muratbay Almurzayev, Pavel Lerman, Iskander Akhmetov, Rustam Mussabayev, Alexander Krassovitskiy	ANALYZING AND CLASSIFYING MEMES BY CONTENT	263
Gulmira Tolegen, Alymzhan Toleu, Rustam Mussabayev	EXPERIMENTS WITH FUZZY CLUSTERING ON TOPIC MODELING	271
Jaxylykova Assel, Akhmetov Iskander, Yerassyl Kelsingazin	SENTIMENT ANALYSIS OF KASPI PRODUCT REVIEWS	277
Sabitov A. Kintonova A. Zh.	DESIGN OF ADAPTIVE SYSTEMS	282
Sadykova A.	PARALLELIZING THE FACE RECOGNITION PROCESS FROM A BIG DATABASE	287

Yunicheva N.R., Kuchin Y., Mukhamedieva E.L.	REVIEW OF EXISTING RESOURCES AND PRODUCTION OF NATURAL URANIUM IN THE WORLD	292
Б.С.Амирханов, Т.Ж. Мазаков.	РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ СИСТЕМ КОНТРОЛЯ ВОДИТЕЛЯ	297
Емельянова М.Г.	МЕТОДЫ И АЛГОРИТМЫ АВТОМАТИЧЕСКОГО РАСПОЗНАВАНИЯ ПОВЕРХНОСТНЫХ ДЕФЕКТОВ СВАРНЫХ СОЕДИНЕНИЙ	304
Каражанов Куаныш Жумагулулы.	ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СФЕРЕ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ НА ТЕРРИТОРИИ РЕСПУБЛИКИ КАЗАХСТАН	310
Мамырбаев О.Ж., Шаяхметова А.С., Литвиненко Н.Г.	НЕКОТОРЫЕ ПРОБЛЕМЫ РАБОТЫ С БАЙЕСОВСКИМИ СЕТЯМИ	316
Мамырбаев О.Ж., Оралбекова Д.О., Othman M., Тулендиев Д.М., Жумажанов Б., Турдалыкызы Т.	РАСПОЗНАВАНИЯ КАЗАХСКОЙ РЕЧИ НА ОСНОВЕ ИНТЕГРАЛЬНОЙ МОДЕЛИ RNN-T	322
Муратбеков М.М., Барлыбаев А.Б., Алтынбек С.А.	ВЕРОЯТНОСТНЫЕ ГРАФИЧЕСКИЕ МОДЕЛИ В ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМАХ ОБУЧЕНИЯ	328
Мусабаев Р.Р., Красовицкий А.М., Меркебаев А.	ПРИМЕНЕНИЕ МЕТОДА ПОИСКА С ЧЕРЕДУЮЩИМИСЯ ОКРЕСТНОСТЯМИ VNS ДЛЯ РЕШЕНИЯ ЗАДАЧИ ГЛОБАЛЬНОЙ ОПТИМИЗАЦИИ В ПРОЦЕССЕ КЛАСТЕРНОГО АНАЛИЗА СЕГМЕНТОВ РЕЧЕВОГО СИГНАЛА	336
Мусабаев Р.Р.	АНАЛИЗА И РАСПОЗНАВАНИЯ ИНФОРМАЦИОННЫХ СТРУКТУР РЕЧЕВОГО СИГНАЛА	339
Рудаков В.П.	МОДЕЛИ И МЕТОДЫ АВТОМАТИЧЕСКОГО ФОРМИРОВАНИЯ, АНАЛИЗА И ОБРАБОТКИ ЦИФРОВОГО ОБРАЗА ЛИЧНОСТИ.	348
Самигулина Г.А., Самигулина З.И.	ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ УНИФИЦИРОВАННОЙ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ ДЛЯ УПРАВЛЕНИЯ СЛОЖНЫМИ ОБЪЕКТАМИ	356
Ширяева О.И.	РАЗВИТИЕ ПРИНЦИПОВ АДАПТАЦИИ AIS НА КЛАСС РАСПРЕДЕЛЁННЫХ СИСТЕМ	362

	УПРАВЛЕНИЯ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОПТИМАЛЬНОГО УПРАВЛЕНИЯ	
Якунин К.О., Мухамедиев Р.И., Елис М., Рабкан Я., Сымагулов А., Кучин Я., Мухамедиева Е.	ОТРАЖЕНИЕ ПАНДЕМИИ COVID-19 В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ	368
Ускенбаева Р.К., Куандыков А.А., Кальпеева Ж.Б., Рахметова П.М., Сағынулы С.	ОРГАНИЗАЦИЯ И УПРАВЛЕНИЕ ПРОЦЕССОМ АВТОМАТИЗАЦИИ ВЫПОЛНЕНИЯ СЛОЖНЫХ ОПЕРАЦИЙ В СОВОКУПНОСТИ ИНТЕЛЛЕКТУАЛЬНЫХ РОБОТОВ	375
Мухамедиев Р.И., Сымагулов А., Кучин Я., Якунин К., Елис М.	ОТ КЛАССИЧЕСКОГО МАШИННОГО ОБУЧЕНИЯ К ГЛУБОКОМУ. ОСНОВНЫЕ НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ	383
Секция 4. Информационная безопасность и защита данных. Программно-технические средства защиты информации. Математические методы обеспечения информационной безопасности сложных систем		390
Луценко Г.В.	ЗАЩИТА ЛИНИЙ СВЯЗИ НА ФИЗИЧЕСКОМ УРОВНЕ	391
Д.С. Дюсенбаев, Н.А.Капалова., К.Т. Алғазы, А.Хомпыш. .	SP ЖЕЛІСІ НЕГІЗІНДЕ ҚҰРЫЛҒАН ЖАҢА AL02 БЛОКТЫ ШИФРЛАУ АЛГОРИТМІНІҢ ҚҰРЫЛЫМЫ	398
С.Нысанбаева, Қ. Сақан.	ХЕШТЕУ АЛГОРИТМДЕРІН ЖАСАУДАҒЫ БЛОКТЫ ШИФРЛАУ АЛГОРИТМДЕРІН ҚОЛДАНУ ЕРЕКШЕЛІКТЕРІ	406
Самрат С.М.	«AL02» ШИФРЛЕУ АЛГОРИТМІНІҢ ҚАСИЕТТЕРІН ЗЕРТТЕУ	411
Аяшова А.М.	КРИПТОГРАФИЯ ЖӘНЕ СТЕГАНОГРАФИЯ АЛГОРИТМДЕРІН ҚОЛДАНА ОТЫРЫП, ШИФРЛАУДЫҢ ЖӘНЕ ДЕКОДТАУДЫҢ ЖАҢА ТӘСІЛДЕРІ.	416
Ospanov Zh.Zh., Gorlov L.V., Ibrayev R.B., Kiyashko I.V.,	OVERVIEW OF TYPICAL ATTACKS ON CRYPTOGRAPHIC PROTOCOLS FOR EXCHANGING KEY DATA.	423

Itemirov R.S.

Бобровский П.А.	СОВРЕМЕННЫЕ МЕТОДЫ СКРАПИНГА ИНФОРМАЦИИ С ВЕБ-САЙТОВ	429
Смагулов Р.Б.; Усатова О.А., PhD.	АНАЛИЗ АТАК НА WEB-РЕСУРСЫ	433
Бегимбаева Е.Е., Нурманов А.Б., Усатова О.А., Усатов Н.С.	ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ ПРИМЕНИТЕЛЬНО К АУТЕНТИФИКАЦИИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ	441
Косяков И.О.	РАДИОЧАСТОТНОЕ ПОДАВЛЕНИЕ СИГНАЛОВ С ЛЧМ	447
Усатова О.А., Нысанбаева С.Е., Бегимбаева Е.Е., Усатов Н.С.	ПРИМЕНЕНИЕ АЛГОРИТМА ПРОВЕРКИ ПОДЛИННОСТИ СООБЩЕНИЙ И ХЭШ – ФУНКЦИИ	451
Горлов Л.В., Ибраев Р.Б., Оспанов Ж.Ж., Итемиров Р.С., Кияшко И.В.	АЛГОРИТМ ШИФРОВАНИЯ QALQAN	458
Ибраев Р.Б., Оспанов Ж.Ж., Горлов Л.В, Итемиров Р.С., Кияшко И.В.	О ПРОТОКОЛЕ ГЕНЕРАЦИИ, ФОРМИРОВАНИЯ, РАСПРЕДЕЛЕНИЯ И УПРАВЛЕНИЯ КЛЮЧАМИ, ПРИГОДНОГО ДЛЯ ИСПОЛЬЗОВАНИЯ В СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ СИСТЕМАХ ПРЕДВАРИТЕЛЬНОГО ШИФРОВАНИЯ	464
Оспанов Р.М., Сейткулов Е.Н., Ергалиева Б.Б.	О ВЫБОРЕ НАБОРА КРИТЕРИЕВ ОПТИМАЛЬНЫХ S-БЛОКОВ	468
Ш.А. Сейдалиев, А.Д.Куракбаев	ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ПРОТИВОДЕЙСТВИЯ МАНИПУЛИРОВАНИЮ ОНЛАЙН-КОНТЕНТОМ	472
Абдалы Ш.А.	БЕЗОПАСНОСТЬ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ	477
Содержание		481

МАТЕРИАЛЫ
VI международной научно-практической конференции
"Информатика и прикладная математика",

29 сентября - 2 октября 2021, Алматы, Казахстан

Подписано в печать 25.09.2021 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 51.45.
Тираж 300 экз. Заказ № 006900.
Отпечатано в ИИВТ МОН РК.
Алматы, ул. Пушкина, 125