АПИБК-2021

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КАЗАХСТАНЕ

Алматы

11 июня 2021 года

Институт информационных и вычислительных технологий МОН РК

«Ғылым ордасы»

МАТЕРИАЛЫ

Международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане»
11 июня 2021года

Алматы 2021

УДК 004
ББК 32.973.202
А 35

А 35 **Актуальные проблемы информационной безопасности в Казахстане:**
Матер. Межд. науч. – практ. конф. (11 июня 2021 г.). – Алматы, 2021. – с. 131

ISBN 978-601-332-542-2

В настоящее издание вошли материалы докладов Международной научно – практической конференции «Актуальные проблемы информационной безопасности в Казахстане».

Работа конференции проводилась при участии представителей органов государственной власти, квазигосударственных предприятий, научных сообществ и вузов, руководителей и специалистов компаний – разработчиков средств защиты информации, телекоммуникационных компаний, операторов связи, организации, осуществляющих свою деятельность в области информационной безопасности.

Рассмотрены актуальные вопросы обеспечения информационной безопасности в государственном секторе, состоялся диалог представителей отрасли и регуляторов, проведены обмен опытоми повышение информированности участников конференции о состоянии информационной безопасности в Республике Казахстан.

Материалы сборника предназначены для научных работников и преподавателей вузов соответсвтующего профиля, докторантов и магистрантов, а так же для специалистов, чьей задачей является использование средств обеспечения информационной безопасности.

УДК 004
ББК 32.973.202

ISBN 978-601-332-542-2

Программный комитет

***Председатель Международного Программного комитета*:**

- Калимолдаев М.Н., Вице-президент, главный ученый секретарь НАН РК (Казахстан), академик НАН РК, д.ф.-м.н., профессор

Почетный председатель программного комитета:

- Бияшев Р.Г., д.т.н., профессор, Казахстан

Зам. председателя:

- Нысанбаева С.Е., д.т.н., ассоц. профессор, Казахстан
- Минникаев М.Н., эксперт по информационной безопасности, Казахстан

Члены международного программного комитета:

- Waldemar Wójcik д.т.н., профессор, Польша
- Pawel Komada, Польша
- Аманжолова С.Т., к.т.н., доцент, Казахстан
- Бабенко Л.К., д.т.н., профессор, Россия
- Ищукова Е.А., к.т.н., доцент, Россия
- Капалова Н.А., к.т.н., Казахстан
- Конявский В.А. д.т.н., профессор, Россия
- Мазаков Т.Ж., д.ф.-м.н., профессор, Казахстан
- Мансурова М.Е., д.ф.-м.н., ассоц. профессор, Казахстан
- Мусиралиева Ш.Ж., к.ф.-м.н., доцент, Казахстан
- Сейлова Н.А., к.т.н., доцент, Казахстан
- Тукеев У., д.т.н., профессор, Казахстан
- Туреханов В.Б., Президент ОЮЛ "Казахстанская ассоциация автоматизации и робототехники, Казахстан
- Тынымбаев С.Т., к.т.н., профессор, Казахстан
- Усатова О.А. PhD, Казахстан

Ученые секретари конференции:

- Бегимбаева Е.Е., PhD, Казахстан

Приглашенные участники:

- РГУ «Агентство Республики Казахстан по регулированию и развитию финансового рынка»
- АО «Государственная техническая служба»
- «Национальный университет обороны имени Первого Президента Республики Казахстан – Елбасы»
- АО «Национальные информационные технологии»
- АО «Казпочта»
- ТОО «Ak Kamal Security»
- АО «Транстелеком»
- Учебный центр «Микроинформ» (г. Москва)
- **«Большая четвёрка» аудиторских компаний:**
    1. Ernst & Young
    2. PricewaterhouseCoopers (PWC)

3. KPMG
4. Deloitte Touche Tohmatsu

Приглашенные аналитики:

- Владислав Витальевич Остапенко – независимый эксперт
- Гани Маликович Надирханов - независимый эксперт
- Дмитрий Александрович Черняк – АО «ЦАЭК/ АО «ЦАТЭК»» - Директор департамента информационной безопасности
- Тимур Кэлсович Имамбаев – ТОО «QazSOC» - Управляющий директор
- Алексей Александрович Стрижевский – ТОО «QazSOC» - Управляющий директор
- Иван Васильевич Коршунов - АО ДБ Альфа-банк - Директор департамента информационной безопасности
- Иван Сергеевич Завертаев - ТОО "Кар-Тел" (Beeline) Служба по развитию нового бизнеса - Старший менеджер продуктов по кибербезопасности.
- Абдрахманов Альжан Есиркепович - ТОО «Контрактное производство «Delta-IT»»
- Виктор Владимирович Покусов – Член Совета ОЮЛ «Интернет Ассоциация Казахстана»

Организационный комитет

Институт информационных и вычислительных технологий КН МОН РК.
Председатель:

- Усатова О.А. Главный ученый секретарь, PhD, Казахстан

Члены организационного комитета:

- Абдалы Ш.А.
- Алғазы К.Т.
- Варенников А.В.
- Меркебаев А.Б.
- Сақан Қ.
- Рог О.А.
- Сулейменов О.Т.
- Шахмаев Р.А.

Место проведения:

Офлайн конференция: Институт информационных и вычислительных технологий КН МОН РК.

Адрес: г. Алматы, ул. Шевченко 28, здание Ғылым Ордасы, вход со стороны ул. Курмангазы, 3 этаж, тел. + 77051000777, +77072407501

Онлайн конференция: платформа Zoom;
Тема: Актуальные проблемы информационной безопасности в Казахстане (АПИБК-2021)
Время: 11 июня 2021 09:00 AM Алматы
Подключиться к конференции Zoom:
https://us02web.zoom.us/j/84450691125?pwd=N2hWVVQvWmVhSnhENEdLbTIrN2NCZz09
Идентификатор конференции: 844 5069 1125
Код доступа: 069873

ОЦЕНИВАНИЕ ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Ахметов Б.С., Лахно В.А., Картбаев Т.С., Алимсеитова Ж.К.
e-mail: bakhytzhan.akhmetov.54@mail.ru, lva964@gmail.com, kartbaev_t@mail.ru, zhuldyz_al@mail.ru
Казахский национальный педагогический университет имени Абая, Казахстан
Национальный университет биоресурсов и природопользования Украины, Украина
Алматинская академия МВД РК имени М. Есбулатова, Казахстан
Алматинский университет энергетики и связи имени Гумарбека Даукеева, Казахстан

Аннотация. *Проведен анализ предметной области, с точки зрения оценки эффективности инвестирования в системы защиты информации объектов информатизации. Обоснована возможность получения необходимых данных для оценки эффективности мероприятий по повышению информационной безопасности компании с помощью имитационного моделирования. Предложена методика расчета для оценки результата от воздействия проведенных мероприятий по информационной безопасности, представленная на конкретном примере. В методике моделируются оценка предотвращенного ущерба, являющаяся базовым показателем при обосновании экономического эффекта от систем защиты информации. С помощью имитационного моделирования учитывается относительная неопределенность реальной ситуации с информационной безопасностью объектов информатизации. Это позволяет повысить достоверность обоснования эффективности инвестиционных проектов в сфере информационной безопасности для объектов информатизации. В отличие от существующих, в предложенной методике возможен учет воздействия как прямых, так и косвенных факторов эффективности инвестиционных проектов по информационной безопасности объектов информатизации.*

В соответствии с общепринятой точкой зрения, характерной для большинства специалистов в области информационной безопасности, сформировалось мнение, что инвестирование в информационную безопасность и ее концепция для конкретного объекта информатизации будут эффективным, если обеспечить выполнение требований государственных нормативных документов и стандартов. Такая точка зрения сформировалась на основе, отсутствия единой общепризнанной методики оценки экономического эффекта от инвестирования в информационную безопасность объектов информатизации [1-3]. Заметим, что в данном контексте проблематики оценивания эффективности инвестирования в информационную безопасность объектов информатизации мы понимаем превышение стоимостной оценки конечного результата соответствующих мероприятий над суммарными размерами инвестиций, то есть совокупными затратами финансовых ресурсов на информационную безопасность объектов информатизации в течении фиксированного периода времени [4].

Сложность оценивания реального эффекта от инвестирования в информационную безопасность объектов информатизации обуславливается достаточно большим перечнем специфических для сектора защиты информации и кибернетической безопасности обстоятельств. Не вдаваясь в их детальный анализ этих обстоятельств, заметим лишь существенное влияние на эффективность инвестирование в информационную безопасность объектов информатизации таких как

1) постоянно меняющийся ландшафт киберугроз;

2) разновариантные стратегии и тактики атакующей стороны (компьютерных злоумышленников);

3) быстрое развитие технических средств защиты информации и кибербезопасности и др.

В свою очередь, в соответствии с базовыми постулатами теории оценки эффективности систем, известно, что качество систем защиты информации может проявляться лишь в ходе их реального целевого применения на объект информатизации. Именно это обстоятельство дает возможность объективно оценивать эффективность их применения, а следовательно, и результативность инвестиций в системы защиты информации на объекты информатизации [5-7].

Дополнительная сложность при оценивании эффективности инвестирования в информационную безопасность объектов информатизации связана с неопределенностью результатов функционирования системы защиты информации. Уже на этапе проектирования системы защиты информации присутствуют факторы неопределенности. Например, связанные с тем, что может сложиться такая ситуация, при которой сторона защиты объектов информатизации затратит сотни тысяч у.е. или даже миллионы на защиту от сложных таргетированных кибератак, а атакующей стороне зачастую достаточно прибегнуть к небольшим затратам («инвестициям в кибератаку»), применив методы социальной инженерии. Такая тактика применения методов социальной инженерии в ряде случаев помогала обходить самые современные системы защиты информации [8-9]. Таким образом, по мере реализации проектов в сфере информационной безопасности уровень функциональности системы защиты информации может снизиться. Следовательно, с точки зрения методологии моделирования эффективности инвестирования в информационную безопасность, ряд функциональных метрик системы защиты информации не может быть тождественно выражен и описан детерминированными показателями.

Процедуры, которые предусматривают тестирование и сертификацию компонентов системы защиты информации, не способствуют в полной мере устранению неопределенностей свойств системы защиты. Эти процедуры не могут предусмотреть будущие сценарии атак и тактику злоумышленников. Таким образом, объективной качественной характеристикой системы защиты информации, а также, и ее приспособляемостью к требуемому уровню информационной безопасности в условиях роста количества и сложности деструктивных воздействий компьютерных злоумышленников на информационно-телекоммуникационную инфраструктуру объекта информатизации, можно обоснованно считать вероятностные параметры системы защиты информации. К последним можно отнести параметры, характеризующие, например, степень возможности конкретного средства защиты информации при заданных условиях, достигать обусловленных целей информационной безопасности. Данный вероятностный параметр и должен быть положен в основу комплексного показателя (критерия) оценки эффективности анализируемого средства защиты информации. В качестве подкритериев в таком случае можно принять пригодность определенного средства защиты информации и его оптимальность для конкретной решаемой задачи.

В контексте решаемой задачи, под пригодностью средства защиты информации будем понимать его способность совместно с другими средствами (как аппаратными, так и программными) выполнять все установленные в системе защиты информации требования. В таком случае оптимальность можно трактовать как признак способности средства защиты информации, достигать в своей работе экстремальных значений при соблюдении ряда ограничений.

Обычной практикой в процессе синтеза систем защиты информации является решение многокритериальной задачи, обуславливаемой необходимостью выполнять сравнение разновариантных архитектур контуров систем защиты информации. Как пример можно привести централизованную схему построения контуров защиты информации или децентрализованную. При решении многокритериальных оптимизационных задач в

отношении выбора системы защиты информации для распределенных вычислительных систем неизбежно возникает потребность проанализировать и показатель эффективности как отдельных средств защиты информации, так и их наборов. Собственно, такие наборы аппаратно-программных средств защиты информации, организационных и других мероприятий формируют комплексные системы защиты информации. Такие наборы средств защиты информации можно описать и используя вероятностно-временные характеристики функций распределения. К последним, в частности, можно отнести и вероятностные показатели возможности злоумышленников в течении некоторого отрезка времени преодолеть контуры системы защиты информации объекта информатизации.

Все вышеизложенные аргументы позволяют утверждать, что в процессе оценки эффективности функционирования системы защиты информации наиболее целесообразно применять вероятностные методы. В соответствии с этими методами, приемлемый для стороны защиты гарантированный уровень информационной безопасности будет трансформироваться в доверительные вероятности соответствующих метрик защиты информации и кибербезопасности объекта информатизации.

Заметим, что в ходе многокритериальной оптимизации системы защиты информации также выполняется оценивание уровня гарантий информационной безопасности. А этот уровень в большой степени зависит от размера потенциально предотвращенного ущерба для информационных массивов объектов информатизации. В таком случае, возникает новая задача, связанная с получением численной оценки риска для объектов информатизации. То есть, стороне защиты необходимо обладать представлением о распределении случайных величин ущерба в случае атаки. В такой ситуации традиционно прибегают к методам имитационного моделирования. Как альтернативный подход также используют результаты активного аудита информационной безопасности (или системы защиты информации) для анализируемого объекта информатизации.

Выводы. С помощью имитационного моделирования можно учитывать относительную неопределенность реальной действительности, что в принципе позволяет повысить достоверность обоснования эффективности проектов в сфере информационной безопасности различных объектов информатизации. В разрабатываемой методике возможен учет воздействия как прямых, так и косвенных факторов эффективности проектов информационной безопасности. Знание законов распределения суммарного значение предотвращенных потерь позволит с помощью проектируемой системы поддержки принятия решений, задавать и осуществить сценарный расчет оценки эффекта от внедрения ИТ-проекта в сфере информационной безопасности объектов информатизации с заданной гарантийной вероятностью. В достаточно специализированном сегменте рынка продуктов и услуг информационной безопасности нововведения не всегда благотворны. Инновации в сфере информационной безопасности чаще всего – это результат инвестиций в разработку и получение новых знаний, выработку идей по обновлению состава систем информационной безопасности. Инновационный процесс в сфере информационной безопасности базируется на сложной системе взаимообусловленных и взаимоувязанных мероприятий. Кроме того, важны имеющиеся у инвесторов ресурсы: финансовые, организационные, научные, технологические, производственные, организационные.

Вероятность потерь, возникающих при неверно выбранной стратегии вложения финансовых ресурсов компании в информационную безопасность, достаточно велика. Хотя остается фактом, что сфера информационной безопасности по своему характеру совсем не располагает к излишней инновационности. Успешное решение задачи выбора рациональной стратегии инвестирования в информационную безопасность объектов информатизации стало основой для успешного ведения бизнеса. Это особенно заметно по опыту реализации

успешных проектов развертывания систем информационной безопасности для компаний, занимающихся инновационными разработками. Однако мало иметь достаточные финансовые ресурсы, направляемые на реализацию проектов в сфере информационной безопасности объектов информатизации. Необходимо также располагать инструментарием для прогнозирования и оценивания вариантов стратегий вложения финансовых ресурсов в соответствующий проект. Как отмечалось выше, эффективная поддержка решений в подобных проектах не обходится без применения ИТ, и, в частности, систем поддержки принятия решений или интеллектуальных систем. Вычислительное ядро подобных интеллектуальных систем берет на себя всю рутинную работу по поиску аналитических решений в многокритериальных оптимизационных задачах. Например, в контексте решаемой проблемы появляется возможность конструктивно определять рациональные стратегии распределения финансовых ресурсов на реализацию сложных проектов в области информационной безопасности объектов информатизации.

С помощью интеллектуальных систем (или систем поддержки принятия решений) лицу, принимающему решение, в ходе прогнозной оценки легче определиться с тем, какое именно из направлений информационной безопасности является более приоритетным для вложения своих финансовых ресурсов. Все вышесказанное диктует необходимость интеллектуализации поиска рациональных стратегий инвестирования в столь сложные проекты, как обеспечение информационной безопасности объекта информатизации. И без соответствующей компьютерной поддержки для принятия столь рискованных решений лицу, принимающему решение обойтись сложно.

Литература

1.. Cost-effectiveness of security measures: A model-based framework / W. Pieters, C. W. Probst, Z. Lukszo, L. Montoya // Approaches and processes for managing the economics of information systems. - IGI global, 2014. - pp. 139-156.

2. Ахметов Б.С., Лахно В.А. Адаптивные экспертные системы распознавания угроз и аномалий / Б.С. Ахметов, В.А. Лахно // Монография. - Алматы: КазНПУ им.Абая. Издательство «Ұлағат», 2020. – 206 с

3. Brangetto, P., & Aubyn, M. K. S. Economic aspects of national cyber security strategies. / P. Brangetto, MK-S. Aubyn // Economic Aspects of National Cyber Security Strategies: project report. Annex, 2015. - 1(9-16). - 86.

4. Bakhitzhan Akhmetov, Lazat Kydyralina, Valeriy Lakhno, Gennady Mohylnyi, Jamilya Akhmetova, Anar Tashimova. Model for a computer decision support system on mutual investment in the cybersecurity of educational institutions / Bakhitzhan Akhmetov, Lazat Kydyralina, Valeriy Lakhno, Gennady Mohylnyi, Jamilya Akhmetova, Anar Tashimova // International Journal of Mechanical Engineering and Technology (IJMET) October 2018. - Volume 9, Issue 10. - P. 1114–1122.

5. Akhmetov B.S., Lakhno V.A., Malyukov V.P., Doszhanova A.A., Alimseitova Zh.K. Adaptive Model of Cybersecurity Financing with Fuzzy Sets of Threats and Resources at the Protection Side / B.S. Akhmetov, V.A. Lakhno, V.P. Malyukov, A.A. Doszhanova, Zh.K. Alimseitova // International Journal of Advanced Trends in Computer Science and Engineering. – 2020. - Volume 9, No.4. – P. 5046 – 5052

6. Boiko, A., Shendryk, V., & Boiko, O. Information systems for supply chain management: uncertainties, risks and cyber security / A. Boiko, V. Shendryk, O. Boiko // Procedia computer science. – 2019. – 149. - P. 65-70.

7. Chronopoulos, M., Panaousis, E., & Grossklags, J. An options approach to cybersecurity investment. / M. Chronopoulos, E. Panaousis, J. Grossklags // IEEE Access, 2017. – 6. – P. 12175-12186.

8. Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., Slayback, S. M., & San Miguel, J. M. Determining a Return on Investment for Cybersecurity Technologies in Networked Critical Infrastructures / R. A. Hallman, M. Major, J. Romero-Mariona, R. Phipps, E. Romero, S. M. Slayback, J. M. San Miguel // International Journal of Organizational and Collective Intelligence (IJOCI), 2021. - 11(2). – P. 91-112.

9. Nagurney, A., & Shukla, S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability / A. Nagurney, S. Shukla // European Journal of Operational Research, 2017. - 260(2). – P. 588-600.

КИБЕРҚАУІПСІЗДІК ЖҮЙЕЛЕРІНЕ ИНВЕСТИЦИЯЛАУ ПРОЦЕСІНДЕ ШЕШІМДЕРДІ ҚОЛДАУДЫҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕСІНІҢ ТҰЖЫРЫМДАМАЛЫҚ ҮЛГІСІ

[1]Ахметов Б.Б., [2]Лахно В.А., [1]Ягалиева Б.Е., [1]Тынымбаев Б.А.
e-mail: bagdat.yagaliyeva@yu.edu.kz
[1]Есенов университеті, Ақтау қ., Қазақстан
[2]Украина биоресурстар және табиғатты пайдалану Ұлттық
1 Университеті, Киев қ., Украина

Аңдатпа. *Ақпараттандыру объектісінің киберқауіпсіздік жүйелеріне инвестициялаудың ұтымды стратегиясын таңдау үшін шешімдерді қабылдауды қолдау жүйесінің тұжырымдамасы мен негізгі функционалдық үлгісін әзірлеу.*

Кіріспе.

Шешімдер қабылдау процесінің үнемі күрделенуі, атап айтқанда басқарушылық, сонымен қатар әр түрлі ақпараттандыру объектілері (АОб) үшін киберқауіпсіздікті (КрҚ) қамтамасыз ету міндеттерін, сондай-ақ шешімдерге әсер ететін факторлардың өзара байланысын қамтамасыз ететін пәндік салалардың күрделілігімен бірге шешім қабылдауды қолдау үшін сыртқы қаражаттарды тарту. Шешімдер қабылдау үшін жеткілікті анықталған ақпарат алу мүмкіндігі жоқ, нашар құрылымдалған пәндік аймақтарда (мысалы, IT инвестициялау, киберқауіпсіздік және т.б.) шешім қабылдау үшін шешімдерді қабылдауды қолдау сараптамасында олардың сапасын арттырудың жалғыз жолы болып табылады. Бұл негізінен жоғары ұйымдық деңгейдегі (мысалы, АОб аса маңызды ақпараттық жүйелері) мәселелерді шешу туралы болғандықтан, қате шешімнің «құны» қазіргі уақытта өте жоғары және үнемі өсіп отырады. Егер әр түрлі АОб үшін киберқауіпсіздік жүйелеріне инвестициялау міндеттерін шешуде қабылдауды қолдау туралы айтатын болсақ, онда инвестициялық стратегияны дұрыс таңдамау, хакерлер тарапынан деструктивті әсердің саны мен күрделілігінің тез өсуі мемлекеттік және жеке компаниялардың АТ инфрақұрылымы [1, 2] ақпарат массивтерін, беделін жоғалтуға ғана емес, сонымен қатар кибершабуыл объектісінің қаржысына айтарлықтай зиян келтіруге әкелуі мүмкін.

Осыған байланысты, АОб КрҚ инвестициялаудың ұтымды стратегиясын таңдауға қатысты шешім қабылдауды қолдау процесінде сараптамалық ақпаратты адекватты ұсыну және өңдеу көптеген мемлекеттеттердегі ғылыми зерттеулердің басым бағыты болып табылады және байланысты проблемалар осы мәселелермен осы салада жаңа зерттеулер қажет етеді.

Мақаланың негізгі материалы.

Мемлекеттік және жеке компанияларға жасалған бірқатар ауқымды кибершабуылдардан, клиенттер мен қызметкерлердің жеке деректерінің таралуынан кейін [3,4], киберқауіпсіздік мәселелеріне көбірек көңіл бөліне бастады. Бұл мәселе бүкіл әлемдегі компаниялар басшылығы мен директорлар кеңесінің назарын аударған ең маңызды мәселелердің бірі болды.

Зерттеулердің нәтижелері көрсеткендей [1, 5], бүгінде компаниялардың 2/3 астамы болашақта оларды киберқауіпсіздік саласындағы стандартты шаралармен шектеуге болмайтынын түсінеді және заманауи шешімдерді, соның ішінде роботтандыру, автоматтандыру және аналитика, жасанды интеллект технологияларды енгізе бастайды. Киберқауіпсіздік инвестицияларының көшбасшылары АОб ақпараттық қорғау тізбектерінің негізгі функционалдығын жоғарылатуды жалғастырып қана қоймай, сонымен бірге бүкіл киберқауіпсіздік архитектурасына көзқарастарды қайта қарайды. Сонымен бірге, сауалнамаға жауап берушілердің (респонденттердің) 10%-дан азы [5] олардың ақпараттық қауіпсіздік

қызметтері қазіргі қажеттіліктерді толығымен қанағаттандырады деп санайды. Ірі компаниялар өкілдерінің 75% -дан астамы және шағын компаниялар өкілдерінің 65%-ы олардың бизнесінің киберқауіпсіздігіне қатысты міндеттердің тек бір бөлігі ғана шешілетіндігін атап өтті.

Мемлекеттік мекемелердің, жеке компаниялар мен кәсіпорындардың ақпараттық активтеріне кибершабуылдың үздіксіз өсіп отыратын сценарийлері жағдайында оларды басқару сөзсіз АОб КрҚ қамтамасыз ету үшін қосымша инвестицияларды тарту мәселесін көтереді. Өз кезегінде, КрҚ инвестициялау стратегиясын таңдауды оңтайландыруға байланысты мәселелерді шешу компьютерлік шешімдерді қабылдауды қолдау жүйелері (ШҚҚЖ) мен эксперттік жүйелердің (ЭЖ) [6, 7] әлеуетін пайдалану арқылы ғана емес шешім қабылдаудың интеллектуалды болуын талап етеді.

Қолданыстағы ЭЖ мен ШҚҚЖ сарапшы берген білімдердің толықтығы мен жеткіліктілігі шектеулі, себебі сарапшы априори болғандықтан, оның бағалауына кіру үшін белгілі бір нақты шкала ұсынылады. Сондықтан, көрсетілген шектеулерді ескере отырып, сарапшыға қысым жасамай, жеке сараптамалық бағалауды алуға, түсіндіруге, өңдеуге, үйлестіруге және жинақтауға мүмкіндік беретін тиімді, дұрыс мүмкіндік беретін бірқатар процедураларды әзірлеу қажет. Сондай-ақ, дамыған ШҚҚЖ шешімдерді қолдау жүйелерін әрі қарай пайдалану барысында сарапшылардың бұрын енгізілген өзіндік бағаларын нақтылау және түзету мүмкіндігін қамтамасыз ету қажет. Іс жүзінде біз тақырыптың белгілі бір мәселесі бойынша сарапшылардың құзыреттілік деңгейіне - ақпараттандыру объектісінің киберқауіпсіздігінің инвестициялық стратегиясын таңдауына [7-10] бейімделе алатын ШҚҚЖ жаңа типін құру қажеттілігі туралы айтып отырмыз.

Нәтижесінде, бүгінде бірнеше мемлекеттік мекемелер, кәсіпорындар немесе жеке компаниялар ғана өздерінің ақпараттандыру объектісінің КрҚ саласындағы жағдайлары туралы толық ақпаратқа ие деп сенімді түрде айта алады. Өзінің жоғары білікті киберқауіпсіздік персоналы жоқ немесе сыртқы киберқауіпсіздік мамандарын тартуға және олардың ақпараттандыру объектісінің ақпараттық активтерін қорғауға жеткіліксіз ресурстарға ие көптеген компаниялар мен ұйымдар үшін жалғыз шешім - ШҚҚЖ немесе ЭЖ әлеуетін пайдалану КрҚ ұтымды инвестициялық стратегияларын іздеу мәселесін шешу. Киберқауіпсіздікке инвестициялау стратегиясын таңдау үшін интеллектуалды шешімді қолдау мәселесін шешу қажеттілігі АОб КрҚ саласындағы ШҚҚЖ тұжырымдамасының жобасын (бұдан әрі - Тұжырымдама) әзірлеу үшін мотивацияны білдіреді, оның ішінде аса маңызды компьютерлік жүйелер (АМКЖ) үшін. Тұжырымдама киберқауіпсіздік жүйелеріне инвестициялау процесінде ШҚҚЖ құрудың тәсілдері мен жолдарын анықтауға, пайдаланушыларға КрҚ жүйелеріне инвестициялаудың таңдалған стратегиясын жүзеге асырумен байланысты қаржылық және басқа тәуекелдер туралы сенімді ақпарат ұсынуға бағытталған.

Киберқауіпсіздік жүйелеріне инвестиция салу процесінде шешімдерді қабылдауды қолдау жүйесі (бұдан әрі – ШҚҚЖ) оны барлық мекемелерде немесе кәсіпорындарда кез-келген мүдделі адамдар пайдалану мақсатында жасалады, олар үшін компьютерлік зиянкестердің ақпараттық ресурстарға деструктивті әсерінің саны мен күрделілігінің артуы киберқауіпсіздік жүйесінен бұрын инвестициялық стратегияны табу міндеті қойылады.

ШҚҚЖ келесі міндеттерді шешуге арналған:

- киберқауіпсіздік жүйелеріндегі инвестициялық стратегияны таңдауға байланысты мәліметтер базасы мен мәліметтер базасын құру, ақпараттық объектінің киберқауіпсіздігіндегі инвестициялық стратегиялардың бірыңғай электронды архивін қолданушыға қол жетімділіктің сараланuымен қамтамасыз ету үшін бағдарламалық жасақтама құру;

- деректер форматтары мен алмасу хаттамаларын ішкі стандарттау арқылы ШҚҚЖ ішкі жүйелері арасындағы ақпараттық өзара іс-қимылды қамтамасыз ететін КрҚ жүйелеріне инвестициялаудың ұтымды стратегияларын есепке алу саласында бірыңғай ақпараттық кеңістік құру;

- КрҚ жүйелеріне инвестициялаудың ұтымды стратегияларын таңдау үшін шығыс құжаттамасын құрудың бірыңғай жүйесін құру;

- шешім қабылдаушылар талап ететін құжаттардың үлгілері мен шаблондарының деректер қорын (ДҚ) жүргізу;

- графикалық және баспа түрінде шешім қабылдау үшін талдамалық ақпаратты қалыптастыру;

- дәстүрлі қолдау мен бақылаудың дәстүрлі формалары мен әдістерін қолдана отырып, киберқауіпсіздік жүйелеріне инвестицияларды ақпараттандыру дамуының дәйектілігін, күрделілігі мен дәйектілігін қамтамасыз ету.

Ақпараттық және киберқауіпсіздік бағдарламаларына арналған ШҚҚЖ-дің негізгі функциялары, әдетте, төмендегілерді орындау қажеттілігіне негізделген:

киберқауіпсіздік мәселелерін кешенді талдау принциптері;

шешімдерді қабылдауды қолдау процесінде қолданылатын ресми және бейресми әдістерді біріктіру мүмкіндіктері;

мәселенің қазіргі жағдайына байланысты ақпараттың сенімділігі мен өзектілігі принциптері. Сонымен бірге, әдетте, олар есептердің барлық түрлерін, статистикалық деректерді, аналитикалық шолуларды, сондай-ақ мониторингтің ішкі жүйелерінен алынған деректерді пайдаланады;

шешімдерді қабылдаудың қолдаудың интеллектуализациясының әдістері мен модельдерін автоматтандырылған таңдау принциптері;

ШҚҚЖ күйлерді одан әрі дамыту принциптері;

қызмет ету тиімділігі мен бақылау іс-шараларын жасау процесінде шешім қабылдаушы қолдана алатын алынған ұсынымдар мен тұжырымдардың негізділігін арттыру мақсатында ШҚҚЖ-ні динамикалық басқару принциптері;

шешілетін мәселені талдау, жедел басқару және бақылау модульдерінің әлеуеті.

ШҚҚЖ-нің толық жұмыс істеуін қамтамасыз ету үшін, әдетте, ол келесі негізгі модульдер мен ішкі жүйелерді қамтуы керек, 1-суретті қараңыз:

1. Деректер базасының модульдері, білім базасы, модельдер базасы және шешім қабылдау үшін қолданылатын ережелер.

2. Интерфейсті басқару жүйесі. ШҚҚЖ архитектурасы негізінде жасалған - жергілікті немесе клиент-сервер.

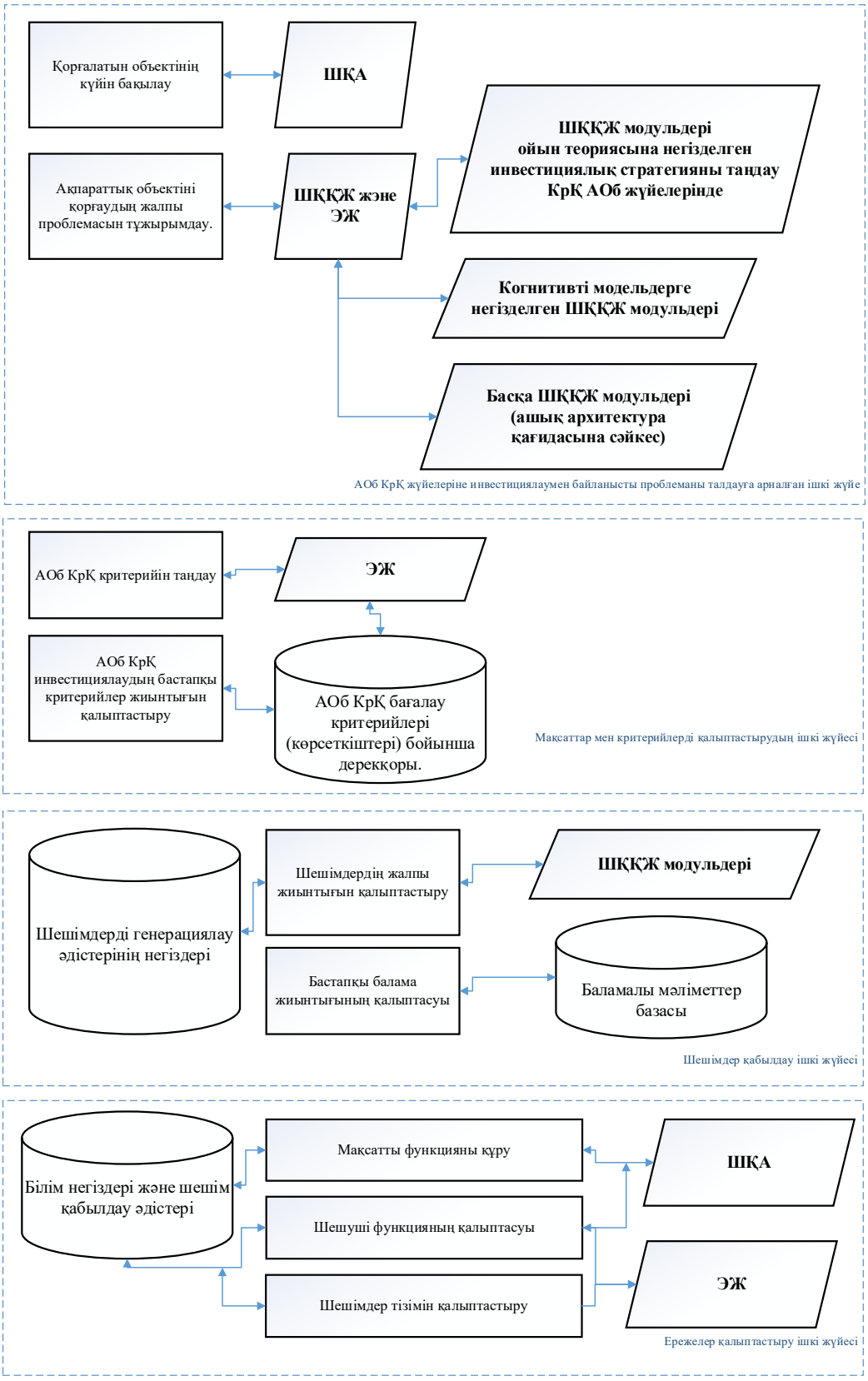
3. Басқа модульдер мен ішкі жүйелер, олардың қажеттілігі пәндік аймақтың ерекшеліктерімен байланысты.

ШҚҚЖ шешімдерді қолдаудың келесі түрлерін ұсынуы керек:

сараптамалық қолдау;

автоматтандырылған шешім шығару;

аралас шешім.



Сурет 1 – АОб КрҚ инвестициялаудың ұтымды стратегиясын таңдауға қатысты шешім қабылдау процесінде ШҚҚЖ архитектурасы

Қорытынды

Мақала авторлары қарама-қарсы жақпен (хакермен) динамикалық қарсыласу кезінде киберқауіпсіздік жүйелеріне инвестициялау стратегиясының ұтымды (оңтайлы) нұсқасын талдау және таңдау процесінде ШҚҚЖ жұмысының құрылымдық диаграммасын ұсынады. Жүйенің үздіксіз және тиімді жұмысын қамтамасыз етуге ықпал ететін осындай ШҚҚЖ негізгі функционалды модульдері қарастырылған.

Жоғарыда келтірілген схема шағын компаниялардан немесе кәсіпорындардан бастап ірі ақпарат объектілеріне дейін ақпараттандыру объектілерінің кез-келген ауқымдағы киберқауіпсіздік жүйелеріне инвестициялаудың ұтымды стратегияларын таңдау процесінде толық шешімдер қабылдауды қамтамасыз етеді.

Әдебиеттер

1. Mohammadhassani, A., Teymouri, A., Mehrizi-Sani, A., & Tehrani, K. (2020, June). Performance Evaluation of an Inverter-Based Microgrid under Cyberattacks. In 2020 IEEE 15th International Conference of System of Systems Engineering (SoSE) (pp. 211-216). IEEE.

2. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929.

3. Pally, Y. A. (2020). Cyberattacks and disinformation campaigns. Journal of Social Political Sciences, 1(3), 195-206.

4. Sokolov, S., Nyrkov, A., Knysh, T., & Shvets, A. (2020, December). Countering Cyberattacks During Information Operations. In Proceedings of the XIII International Scientific Conference on Architecture and Construction 2020 (pp. 84-100). Springer, Singapore.

5. Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77, 103201.

6. Philp, D., Chan, N., & Sikos, L. F. (2020). Decision support for network path estimation via automated reasoning. In Intelligent Decision Technologies 2019 (pp. 335-344). Springer, Singapore.

7. Lakhno, V. A., Kasatkin, D. Y., Blozva, A. I., Kozlovskyi, V., Balanyuk, Y., & Boiko, Y. (2020, October). The Development of a Model of the Formation of Cybersecurity Outlines Based on Multi Criteria Optimization and Game Theory. In Proceedings of the Computational Methods in Systems and Software (pp. 10-22). Springer, Cham.

8. Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. European Journal of Operational Research, 282(1), 161-171.

9. Hallman, R. A., Major, M., Romero-Mariona, J., Phipps, R., Romero, E., John, M., & Miguel, S. (2020, May). Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration. In COMPLEXIS (pp. 43-52).

10. Farao, A., Panda, S., Menesidou, S. A., Veliou, E., Episkopos, N., Kalatzantonakis, G., ... & Xenakis, C. (2020, September). SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In International Conference on Trust and Privacy in Digital Business (pp. 65-74). Springer, Cham.

АВТОМАТТАНДЫРЫЛҒАН АҚПАРАТТЫҚ ЖҮЙЕНІҢ ҚОЛЖЕТІМДІЛІКТІ ШЕКТЕУ ЖҮЙЕСІ

Бегимбаева Е.Е.[1,2] ,Тұрғанбай А.Н.[1]
E-mail: enlik_89@mail.ru, armanturganbai@gmail.com
[1]Әл-Фараби атындағы ҚазҰУ, Алматы қаласы, Қазақстан
[2]Ақпараттық және есептеуіш технологиялар институты ҚР БҒМ ҒК, Алматы, Қазақстан

Аңдатпа. *Мақалада автоматтандырылған ақпараттық жүйелер (ААЖ) ресурстарына қолжетімділікті шектеуді басқарудың жалпы мәселелері қарастырылады. ААЖ-ға тән қасиеттер және қол жеткізуді шектеу әдістері мен ережелерін жүзеге асыратын оның қауіпсіздік саясатына қойылатын талаптар талданады. Тапсырма ААЖ-ға қол жеткізуді шектеуді басқарудың жаңа модельдерін, әдістері мен алгоритмдерін жасау болып табылады.*

Кілттік сөздер: *ақпаратты қорғау, қол жетімділікті шектеу, қол жетімділікті басқару, қауіпсіздік саясаты, ақпараттық жүйе, рұқсат етілмеген кіру*

Кіріспе

Қазіргі таңда әлемде ақпарат стратегиялық ресурсқа әрі экономикалық дамыған мемлекеттің негізгі байлықтарының біріне айналуда. Әлемдегі ақпараттандырудың тез жетілуі, оның жеке адамның, қоғамның және мемлекеттің өмірлік маңызды мүдделерінің барлық салаларына енуі сөзсіз артықшылықтардан басқа бірқатар маңызды проблемалардың пайда болуына себеп болып отыр. Олардың ең маңыздысы ақпаратты қорғау қажеттілігі болды. Қазіргі уақытта экономикалық әлеует ақпараттық құрылымның даму деңгейімен көбірек анықталатынын ескере отырып, экономиканың ақпараттық әсерлерден әлеуетті осалдығы пропорционалды түрде өсуде.

Ақпараттың белгілі бір құндылығы бар. Сонымен қатар, ақпараттың бірқатар қасиеттерінің өзгеруі мұндай құндылықтың жоғалуына әкелуі мүмкін. Деректерді қорғау туралы қолданыстағы заңнамаға сәйкес осындай қасиеттердің қатарына мыналар жатады:

- Құпиялылық — үшінші тұлғалардың деректерге қол жеткізудің мүмкін еместігі;
- Тұтастық — тиісті рұқсаты бар тұлғалардың ғана ақпаратты өзгерту мүмкіндігі;
- Қолжетімділік — аппараттық деңгейдің проблемаларына немесе зиянды бағдарламалық қамтаманың әрекетіне байланысты пайдаланушының қажетті ақпаратқа шектеусіз қол жеткізуін қамтамасыз ету.

Көптеген заманауи зерттеушілердің еңбектерінде, сондай - ақ халықаралық және отандық стандарттар мен нормативтік автоматтандырылған ақпараттық жүйенің қол жетімділігін шектейтін қауіпсіз жүйенің құрылуы пайдаланушылардың жүйенің ақпараттық ресурстарына қол жеткізуін басқарудың ресми модельдерін қолдануға негізделгені атап өтілді.

Автоматтандырылған ақпараттық жүйенің қол жетімділігін шектеу жүйесін жобалау үшін оларды қолдану тұрғысынан қол жеткізуді басқарудың ең көп таралған формальды модельдерін талдау барысында қарастырылған модельдердің ешқайсысы автоматтандырылған ақпараттық жүйенің жоғарыда аталған қасиеттерін ескеруге мүмкіндік бермейтіні және оны негізгі ретінде пайдалану мүмкін еместігі анықталды. Дегенмен, қол жеткізуді шектеудің жеке міндеттерін ресми сипаттау үшін ұсынылған модельдердің кейбірін ішінара пайдалану мүмкіндігі бар. Сонымен қатар, кез-келген модель аясында стандартты бөлімшелердің болуына байланысты ақпараттық ресурстардың ұйымдық құрылымын ескеру мүмкін емес. Алайда, бұл мәселені шешу үшін ұйымдық құрылымды есепке алу үшін қолдану аясын кеңейту арқылы жетілдірілген қол жетімділікті тақырыптық шектеу моделін қолдануға

болады. Осылайша, автоматтандырылған ақпараттық жүйенің ақпараттық ресурстарына қол жеткізуді бөлудің тиімді жүйесін құру үшін қол жетімділікті шектеудің қолданыстағы модельдерінің тіркесімі негізінде құрылуы мүмкін қол жетімділікті шектеудің ресми моделін жасау қажет. Сонымен қатар, қол жеткізуді шектеу модельдерінің қасиеттеріне сүйене отырып, модельдің жеткіліктілігінің дәлелі болып табылатын модель қауіпсіздігінің ресми дәлелі болуы керек.

Автоматтандырылған ақпараттық жүйенің функционалды-рөлдік моделі келесі ұғымдарға негізделген: функционалды модуль, рөл, түрлендіру процедурасы, аналитикалық процедура. Деректерді өңдеу процедураларын жүйенің жеке субъектілері ретінде бөлу олардың құрамына кіретін операцияларды пайдаланушыға субъектіге қол жетімділікті беру туралы шешім қабылданған кезде қол жеткізуді басқару жүйесі басқара алмайтындығына байланысты. Сондықтан, осы субъектілерге қол жеткізу құқығын тағайындау туралы шешімді жүйенің әкімшісі қабылдайды, ол осы субъектінің қауіпсіз екенін анықтайды, яғни.қауіпсіздік саясатын бұзбайды. Деректерді өңдеу процедураларының жиынтығын процедуралардың екі ішкі жиынына бөлу оларды қолдану мен қол жеткізуді ұйымдастырудағы айырмашылықтарға байланысты. Түрлендіру процедуралары жүйенің функционалды логикасын жүзеге асыратын мәліметтерді өңдеу процестерін орындауға арналған. Олар функционалды модульдерге және оларды орындайтын пайдаланушыларға нақты бекітілген. Аналитикалық процедуралар оларды өзгертпестен арнайы түрде құрылған мәліметтер жиынтығын ұсынуға арналған. Көптеген аналитикалық процедуралар автоматтандырылған ақпараттық жүйенің пәндік аймағын көрсететін иерархиялық құрылымға ие, ал қол жетімділік нақты процедураға емес, оның тақырыбына реттеледі. Автоматтандырылған ақпараттық жүйенің пайдаланушылары ақпараттық объектілерге функционалдық модульдер құрамында іске асырылған түрлендіру процедураларын немесе талдамалық процедураларды орындау арқылы қол жеткізе алады.

Автоматтандырылған ақпараттық жүйенің қол жетімділікті шектеку жүйесінде жұмыс істейтін сипатталған ақпараттық ағындардың қауіпсіздігін бақылауға және қамтамасыз етуге тиіс. Қол жеткізуді басқарудың ресми модельдерін және автоматтандырылған ақпараттық жүйенің қасиеттерін талдау негізінде функционалды-рөлдік модельдің келесі құрамы ұсынылды және бірыңғай модель аясында қол жеткізуді басқарудың ресми модельдерінің қолданылу салаларын бөлу анықталды:

Модель атауы	**Мақсаты**
Қол жеткізуді ұйымдастырушылық шектеу моделі	Ақпараттық объектілерге қолжетімділікті басқару
Қол жеткізу матрицасына негізделген дискрециялық модель	Түрлендіру процедураларына қол жеткізуді басқару
Қол жеткізуді тақырыптық шектеу моделі	Талдамалық рәсімдерге қол жеткізуді басқару
Рөлдік модель	Пайдаланушылардың рөлдері мен өкілеттіктерін басқару

Қол жеткізуді шектеудің рөлдік моделі жүйеде пайдаланушыларды, рөлдерді және рөлдердің өкілеттіктерін басқару үшін қолданылады. Сонымен қатар, осы модельдің барлық түрлерінің ішінен рөлдер жүйесін иерархиялық ұйымдастыруға негізделген модель таңдалды. Рөлдік модельдің бұл түрін таңдау оның кәсіпорындар мен ұйымдардағы нақты ұйымдастырушылық - басқарушылық және ұйымдастырушылық - технологиялық схемаларға жақындығына байланысты. Пайдаланушылардың өкілеттіктері функционалдық модульдерді жандандыру құқығымен айқындалады. Бұл ретте функционалдық модульдер арқылы жүзеге

асырылатын ақпараттық ресурстарға қол жеткізуді басқару функционалдық - рөлдік модельдің құрамына кіретін басқа да модельдер шеңберінде бақыланады.

Қол жеткізуді ұйымдастырушылық шектеу моделі. Ұйымдастырушылық құрылым негізінде ақпараттық объектілерге қол жеткізуді ұйымдастыру үшін көптеген нысандарда кәсіпорынның ұйымдық құрылымын оңтайлы сипаттайтын иерархиялық ағаш салынды. Ағаш түйіндері ұйымның бөлімшелерін білдіреді, ал бір ағаш түйінінің екіншісіне бағынуы осы түйіндерге сәйкес келетін бөлімшелердің ұйымдық бағыныштылығын білдіреді.

Қол жетімділік матрицасына негізделген дискрециялық модель түрлендіру процедураларына қол жеткізуді басқару үшін қолданылады. Қол жеткізу объектілері-түрлендіру процедуралары, ал субъектілер — пайдаланушылар.

Қол жеткізу матрицасы пайдаланушылардың түрлендіру процедураларын орындау құқығын анықтайды. Түрлендіру процедурасы функционалды модульдерге біржақты бекітілгендіктен, әр функционалды модульмен пайдаланушылардың осы функционалды модульді түрлендіру процедураларын орындау құқығын анықтайтын өзіндік қол жетімділік матрицасы байланысты. Жұмыста пайдаланушы ешқандай жағдайда ол үшін рұқсат етілмеген түрлендіру процедураларын орындамайтынын көрсетеді, яғни жүйе пайдаланушылардың түрлендіру процедураларына қол жеткізуін қауіпсіз басқаруды қамтамасыз етеді.

Қол жеткізуді тақырыптық бөлу моделінде қол жеткізу объектілері аналитикалық процедуралар, субъектілер – пайдаланушылар болып табылады. Нысандарды жіктеудің негізі мандаттық модельдердегідей қауіпсіздік деңгейі емес, қол жеткізу объектілері мен субъектілерінің тақырыптық санаты болып табылады. Автоматтандырылған ақпараттық жүйенің ақпаратының пәндік саласы иерархиялық тәсіл негізінде құрылған тақырыптық жіктеуішпен ұсынылады. Қолданыстағы субъектілердің қолданыстағы объектілерге қауіпсіз қол жеткізуіне санкция беру қол жеткізуді шектеу туралы келесі ереже негізінде жүзеге асырылады.

Көптеген пайдаланушылар мен ресурстар, автоматтандырылған ақпараттық жүйенің пайдаланушылары құрамының өзгеруі, аумақтық бөлу көптеген ішкі әкімшілік міндеттердің пайда болуына әкеледі, демек, қателіктер қаупі артады. Мысалдар дұрыс емес немесе уақтылы тағайындалмауы / қол жетімділік құқығынан айырылуы, сәйкестендіру деректерін заңсыз пайдалану, қауіпсіздік саясатының ережелерін бұзу және т.б. болуы мүмкін, сонымен бірге пайдаланушылардың құқықтары мен өкілеттіктерін шектеу процестерін автоматтандыру көбінесе әдепкі қондырғылармен шектеледі. Қол жетімділікті шектеуді одан әрі басқаруды қауіпсіздік әкімшісі "қолмен" режимде жүргізеді. Бұл тәсілдің бірқатар кемшіліктері бар. Атап айтқанда, шабуылдаушы "әдепкі" схеманы білуі мүмкін, ал схеманың өзі алдын-ала анықтау мен жеке параметрлерді қажет етеді. Бұл қол жеткізу құқықтарын орнату және басқару процестерін ішінара немесе толық автоматтандыруға мүмкіндік беретін алгоритмдердің сұранысына әкеледі.

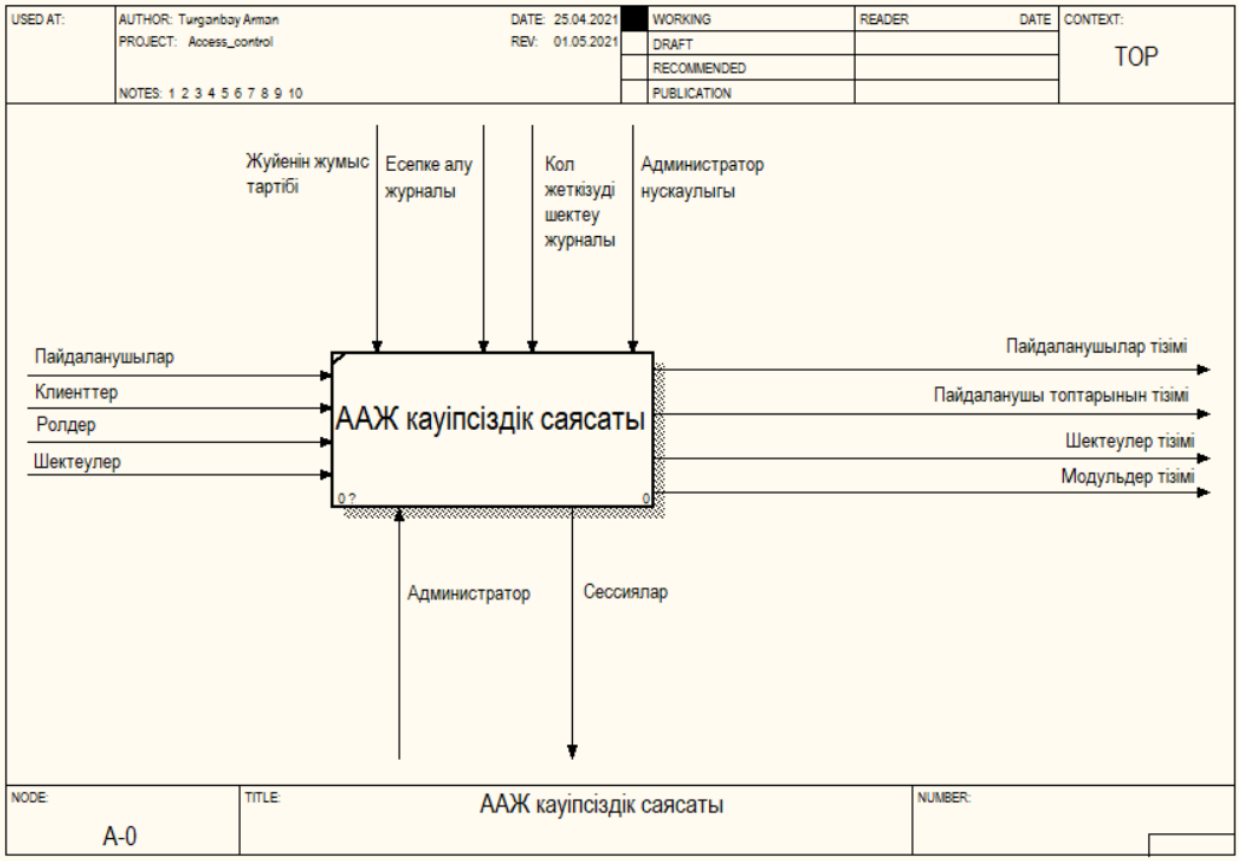
ААЖ пайдаланушылары мен объектілері санының едәуір өсуіне және оның қол жеткізуді бөлу саясатының өзгеруіне байланысты қол жетімділікті шектеу саясатын жобалауға дәстүрлі төмендеу тәсілі іске асыру кезеңінде қиындықтарға тап болады. Саясатты құру принципі кеңінен таралуда. ААЖ талдау үшін қажетті ақпараттың үлкен көлеміне байланысты бұл тәсілді қолмен іске асыру мүмкін емес. Сондықтан "төменнен жоғары" тәсіл негізінде қол жетімділікті шектеу саясатын қалыптастыру процестерін автоматтандыру алгоритмдерін әзірлеу өзекті міндет болып табылады.

ААЖ-ға қол жетімділікті шектеу саясатын құру және қолдау кезінде туындайтын өзекті мәселелердің жоғарыда келтірілген тізімі пайдаланушылар мен ақпараттық ресурстар туралы үлкен көлемде мәліметтерді өңдеу жағдайында қол жеткізуді шектеуді басқарудың жаңа

ғылыми негізделген модельдерін, әдістері мен алгоритмдерін жасау қажеттілігін анықтайды. Осы мақсатқа жету үшін келесі негізгі міндеттерді шешу қажет:

1. Қол жеткізуді шектеудің классикалық модельдерін талдау және формализациялау ААЖ ерекшеліктерін ескере отырып.
2. ААЖ объектілеріне қол жетімділікті рөлдік, мандаттық және дискрециялық шектеуді құру процестерін автоматтандыру әдістері мен құралдарын әзірлеу.
3. Әр түрлі критерийлер негізінде ААЖ қол жетімділікті шектеу саясатын оңтайландыру әдістері мен құралдарын әзірлеу.
4. ААЖ-ға қол жетімділікті шектеудің әртүрлі саясатын біріктіру процестерін автоматтандыру әдістері мен құралдарын жасау.
5. ААЖ-ға қол жеткізуді шектеудің бөлінген саясатын құрудың әдістері мен құралдарын әзірлеу.

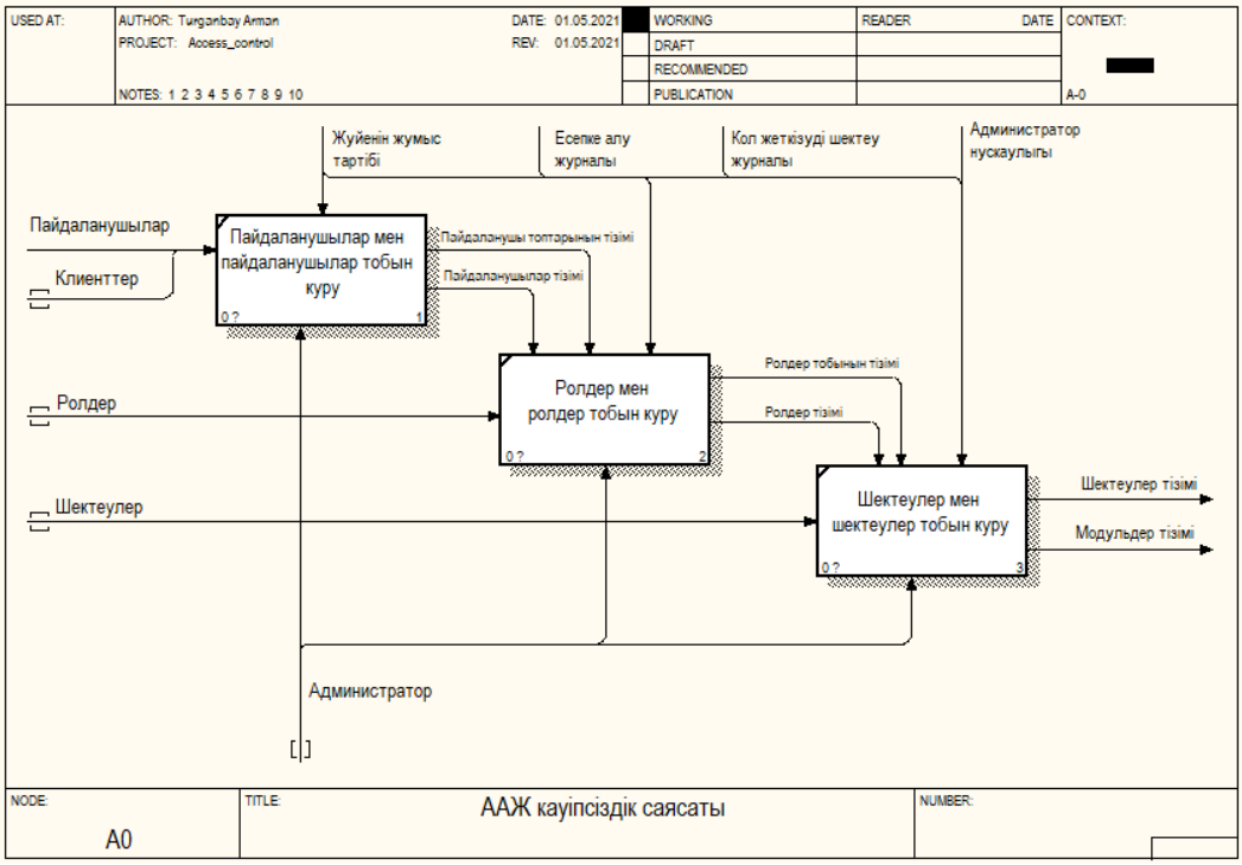
Жоғарыда аталған бірқатар мақсатқа жету барысында қол жетімділікті шектеу жүйесінің құрылымдық және функционалдық моделі жасалды (1-сурет).



1-сурет. ААЖ қауіпсіздік саясатының функционалдық моделі.

Автоматтандырылған ақпараттық жүйені модельдеудің бастапқы кезеңінде оның кешенді құрылымдық-функционалдық талдауы, негізгі материалдық және ақпараттық ағындарды зерттеу, технологиялық процестер мен операцияларды құрылымдау және жүйелеу жүзеге асырылады. Өндірістік немесе өндірістік емес жүйелерді құрылымдық және функционалдық үлгілеу кезіндегі ең перспективалы бағыттардың бірі CASE-технологияларды және тиісті аспаптық құралдарды пайдалану болып табылады. Декомпозиция принципі автоматтандырылған ақпараттық жүйенің барлық күрделі процестерін оның құрамдас

функцияларына бөлу кезінде қолданылады. Декомпозициялау жүйенің моделін жеке диаграммалардың иерархиялық құрылымы ретінде біртіндеп және құрылымдық түрде ұсынуға мүмкіндік берді Бұл процесті құрылыдық талдау барысында байқауға болады (2-сурет).



2-сурет. ААЖ-ның функционалдық декомпозициясы.

ААЖ-ның барлық жұмыс ағындарындағы негізгі элементтер-бұл жұмыс бірліктері (процестер), олардың арасындағы байланыстар, сілтеме объектілері, сонымен қатар ағындардың өзара әрекеттесу логикасын көрсететін элементтер болып табылатын біріктіру және тармақтау қиылыстары болып табылады. Осы арқылы ААЖ-ның негізгі функцоналдық моделі құрылды.

ААЖ — ға қол жеткізуді шектеу саясатының өзгеруіне байланысты негізгі проблема – бұл жүйенің субъектілері арасындағы қолданыстағы ақпараттық ағындардың шатасуына, қайталанатын субъектілердің пайда болуына және т.б. әкелетін саясаттың стихиялық эволюциясы. Мұндай проблемаларды жаңа талаптарға сәйкес қол жеткізуді шектеу саясатының негізгі құрылымдарын оңтайландыру арқылы шешуге болады. Бұл жағдайда оптимизмді кең мағынада жүйенің ең тиімді жұмысының сипаттамасы ретінде түсіну керек. Мұндай оңтайландыру міндеті көп өлшемді екені анық, кейбір өлшемдер бір-біріне қайшы келуі мүмкін. Өкінішке орай, қазіргі заманғы ақпараттық жүйелердің көпшілігінде қол жетімділікті шектеудің белгілі бір моделін енгізу кезінде оптималдылық мәселелеріне тек жобалау кезеңінде назар аударылады. Ал қол жетімділікті шектеу саясатын қайта құру немесе оны оңтайландыру пәндік аймақтың жаңа талаптарын үздіксіз қалыптастыруға және қолданыстағы талаптарды нақтылауға негізделген итеративті процесс болуы керек.

Қорытынды

Ақпараттық ресурстарға қол жеткізуді басқару технологиялары қазіргі заманғы ақпараттық жүйелердің ауқымын, күрделілігін және әртектілігін ескеретін қол жеткізуді ажыратудың формальды модельдері мен әдістеріне негізделуі тиіс.

Қол жеткізуді басқару жүйесін дамытудың қазіргі деңгейінде қол жеткізуді бөлу саясатын басқару қол жеткізуді бөлуді басқару бойынша операциялардың көпшілігін қауіпсіздік әкімшісі "қолмен" жүзеге асыратындығымен немесе "әдепкі" және шаблондық шешімдер арқылы орнататындығымен сипатталады. Бұл ААЖ-мен жұмыс істеу кезінде бірқатар проблемалардың пайда болуына әкеледі.

ААЖ-ға қол жеткізуді шектеу саясатын құрудағы және сүйемелдеудегі анықталған проблемалар қол жеткізуді бөлу саясатының өмірлік циклінің барлық кезеңдерінде ААЖ-ға қол жетімділікті шектеуді басқару процестерін ішінара немесе толық автоматтандыруға мүмкіндік беретін жаңа модельдердің, әдістер мен алгоритмдердің дамуын жандандырады. Пайдаланушылардың ресурстарға қол жетімділігін саралауды басқару процестерін автоматтандыру қол жетімділікті шектеуді басқару жүйесінің жылдамдығы мен өнімділігін арттырады және әкімшілік қателіктердің ықтималдығын азайту арқылы ақпараттық қауіпсіздік тәуекелдерін азайтады. Бұл жағдайда автоматтандыру мүмкіндігі қол жетімділікті шектеу саясатын құру тәсілдеріне негізделеді, бұл неғұрлым сенімді және болжамды с әзірлеуге мүмкіндік береді.

Әдебиеттер

1. Демурчев Н. Г., Проектирование системы разграничения доступа автоматизированной информационной системы на основе функционально-ролевой модели на примере высшего учебного заведения, – Ставрополь, 2006.

2. Богаченко, Н.Ф., «Анализ проблем управления разграничением доступа в крупномасштабных информационных системах.» №2(46) (2018), 30 июнь 2018 г.

3. Попов, Константин Витальевич, Любовь Павловна Коротких, и Андрей Сергеевич Кольцов. «Обеспечение Безопасности Информационной Системы На Основе Моделей Ролевого Разграничения Доступа», 123–25. Закрытое акционерное общество «Университетская книга», 2017.

4. Перминов, Геннадий Вадимович, и Сергей Владимирович Зарубин. «Концептуальная Модель Технологии Функционирования Защищенной Автоматизированной Информационной Системы». Охрана, Безопасность, Связь 1, вып. 4 (4) (2019 г.).

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ ВОПРОСОВ ОБЕСПЕЧЕНИЯ ПРАВОВЫХ НАЧАЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Бисалиев М.С.
e-mail: mbissaliyev@gmail.com
Директор департамента информационных технологий,
АО «Казахская корпорация здравоохранения и медицинского страхования «Интертич»,
Республика Казахстан, г. Алматы, проспект Нурсултана Назарбаева 275Е;
магистрант кафедры международного права,
Казахский национальный университет им. аль-Фараби
Республика Казахстан, г. Алматы, проспект аль-Фараби 71.

Аннотация. *Вопросы защищенности внутренних информационных систем организаций активно соприкасаются с внешней средой посредством сети Интернет. Обеспечение организационно-технических и правовых начал информационной безопасности тесно перемешаны с вопросами правового и организационного характера. С точки зрения международного частного права большинство вопросов регулирования проблем кибербезопасности не имеют наднационального значения и посредством коллизионных норм отданы на откуп национальным правопорядкам. Изложенное не позволяет говорить о том, что в международном праве сегодня сложилась единая концепция правового регулирования вопросов обеспечения кибербезопасности. Для решения отмеченных выше и иных потенциально выделяемых проблем в указанной сфере в статье предлагаются различные средства и способы совершения действий и операций, использования средств. Описывается определенный и последствия влияния на выбор для использования конкретного набора средств. Например, в качестве такого средства могло бы выступить обобщение судебной практик по отдельным категориям дел, связанным с кибербезопасностью. Правотворческие органы давно и успешно применяют категориальный аппарат «кибербезопасности» для регулирования общественных отношений. Особую важность имеет наличие правовых социальных и морально-этическим норм. В статье выделены близкие к правовым методам научные методы, включая концепции, методики в рамках организационно-технических методов и способов возможно выделение собственно информационных методов обеспечения кибербезопасности. В статье были использованы общенаучные, частнонаучные и иные методы исследования: социологический, исторический, формально-логический, сравнительно-правовой. Нормативную правовую базу составили нормы международного права, опубликованные и неопубликованные материалы отечественной и международной юридической практики, авторские эмпирические исследования в области международного и информационного права. При написании работы автором изучены присутствующие в открытом доступе Положения (Уставы) большинства министерств, административных служб и агентств, нормативная правовая база стран содружества.*

Ключевые слова: *кибербезопасность, источники права кибербезопасности, информационная безопасность, информационное право*

Введение

Нормы права США и Великобритании, разумеется, не входят в систему норм международного права. Вместе с тем, с учетом развитости национальных экономик указанных стран многие вопросы информационного права, стоящие сегодня перед мировым сообществом, в том числе, в деле обеспечения кибербезопасности, уже в той или иной степени

решены в США и Великобритании; в данных государствах наработана и практика применения указанных норм. По этим причинам предложенные американским и британским законодателем, национальными судебными системами алгоритмы разрешения проблем обеспечения кибербезопасности в указанной сфере могут быть восприняты и международным правом как на уровне двусторонних (многосторонних) договоров и соглашений, так и в виде норм конвенций и иных источников международно-правового регулирования. Для ученых «Запада» характерно рассмотрение вопросов кибербезопасности большей частью не в рамках юриспруденции, а в рамках науки об управлении, экономической теории и т.д. Не стала «информационная безопасность» значимой темой и для научных разработок советского периода.

Состояние разработки вопросов обеспечения кибербезопасности в США

Для США характерна, в первую очередь, значительная база источников законодательства об обеспечении кибербезопасности. Это такие группы документов как:

1. Нормативные правовые документы (Указы и Директивы Президента США, федеральные законодательные акты, национальные стратегии, затрагивающие вопросы обеспечения информационной безопасности страны, а также военные доктрины и стратегии по ведению операций в киберпространстве).

2. Пресс-релизы Белого Дома, министерств и ведомств США, выступления, комментарии и интервью официальных лиц США.

3. Аналитические обзоры, доклады и отчеты министерств и относящихся к ним комиссий, корпорации РАНД (RAND), Центра стратегических и международных исследований (CSIS), Главного контрольно-финансового управления США (GAO), исследовательской службы Конгресса США (CRS).

4. Официальные документы (резолюции, конвенции, стратегии, руководящие принципы, доклады рабочих и экспертных групп) таких международных организаций, как «Большая восьмерка», Организация экономического сотрудничества и развития, Совет Европы, Организация Объединенных Наций, Организация по безопасности и сотрудничеству в Европе, Организация Североатлантического договора, Международный союз электросвязи, Организация американских государств, Шанхайская организация сотрудничества и Форум «Азиатско-Тихоокеанского экономического сотрудничества».

5. Итоговые документы двух этапов Всемирной встречи на высшем уровне по вопросам информационного общества; двусторонние соглашения и договоренности по вопросам обеспечения информационной безопасности.

6. Статистические и аналитические материалы организаций, занимающихся вопросами информационной безопасности: НортонЛайфЛок (NortonLifeLock), Лаборатория Касперского (Kaspersky Lab), Мандиант (Mandiant), МакАфи (McAfee), Нортон (Norton), Джавелин Стратеджи и Ресерч (Javelin Strategy and Research), Гартнер (The Gartner), АйДиСи (IDC).

Основным фундаментальным документом в указанной сфере является Стратегия национальной кибербезопасности США 2018 года [1]. В частности, в главе первой данного документа отмечается, что «…администрация уполномочивает Министерство внутренней безопасности (Department of Homeland Security, DHS) на обеспечение безопасности федеральных министерских и ведомственных сетей, за исключением систем национальной безопасности, Министерства обороны (Department of Defense, DOD) и систем разведывательного сообщества (Intelligence Community) …». Подобная формулировка означает, что МВБ США получает права как регулирующего органа, определяющего требования по информационной безопасности, так и контролирующего органа. При этом следует отметить возможность доступа со стороны Министерства ко всем сетям, за

исключением сетей Министерства обороны США и сетей разведывательного сообщества. Де-факто, такой подход означает техническую возможность получения практически любой информации из контролируемых сетей, минуя судебные процедуры. Более того, в конце главы Стратегии отмечено: «…Администрация проведет совместную работу с Конгрессом по обновлению законодательных актов об электронном надзоре и компьютерных преступлениях с целью расширения возможностей правоохранительных органов на законных основаниях осуществлять сбор необходимых доказательств преступной деятельности…». Данная формулировка означает, что техническая возможность по контролю сетей со стороны МВБ США будет подкреплена де-юре. С большой долей вероятности можно предположить, что в настоящий момент вычислительные сети, подпадающие под действие указанной стратегии, оснащены разнородными средствами защиты информации от различных производителей. Это вполне оправданное предположение, поскольку рынок систем и средств защиты информации сформировался уже несколько десятилетий назад и к текущему моменту на нем определились как свои лидеры, так и аутсайдеры. Вместе с тем, рынок систем и средств защиты информации все еще остается новым, правила и нормы регулирования на нем еще требуют уточнения. В качестве первого шага по регулированию этого рынка рассматриваемым документом, с целью унификации используемого оборудования предписывается проведение более тщательного отбора поставщиков. Еще одним примечательным моментом является закрепление права требовать финансовую ответственность как с исполнителей кибератак, так и с их организаторов. В целом, документ является эволюционным развитием предыдущих его редакций. Ряд новых положений, вне всякого сомнения, повлекут за собой существенные изменения в области международной информационной безопасности и повлекут за собой в ближайшие месяцы изменения, которые коснутся и всей отрасли в целом.

Обращаясь к гражданской сфере, отметим, что федеральное законодательство США, регулирующее сферу кибербезопасности, активно развивается с 80-х годов прошлого столетия. Учитывая большое число законов, затрагивающих различные аспекты обеспечения информационной безопасности, для рассмотрения в данной части исследования были отобраны лишь основополагающие федеральные законодательные акты, которые определяют направление развития законодательной системы и в целом являются важной составляющей стратегии информационной безопасности США. Закон «О компьютерной безопасности» 1987 года [2] стал первой законодательной инициативой, направленной на повышение безопасности и обеспечение неприкосновенности информации, размещенной в федеральных компьютерных системах. Данный закон предписывал разработку стандартов и норм для федеральных компьютерных систем; разработку планов безопасности для всех операторов федеральных компьютерных систем, содержащих чувствительную информацию; проведения обязательных регулярных обучающих программ для персонала, имеющего отношение к управлению или использованию федеральных компьютерных систем. В развитие данного закона в 2002 году был принят Закон «Об обеспечении безопасности федеральных информационных систем» [3], которым были установлены рамки безопасности для федеральных информационных систем, а также определены ответственные исполнители в системе государственных институтов. Согласно закону, Национальный институт стандартов и технологий отвечает за выработку стандартов безопасности; Служба управления и бюджета Белого Дома является органом, ответственным за проведение обзора политики федеральных институтов в области информационной безопасности. При этом основная ответственность за функциональные аспекты обеспечения кибербезопасности федеральных информационных систем была возложена на МВБ. Также был создан Федеральный центр происшествий (Cybersecurity and Infrastructure Security Agency), в задачи которого входил сбор информации об инцидентах и нарушениях в информационных системах федеральных органов, для

проведения анализа и принятия мер противодействия, а также разработки планов по управлению рисками [4]. В качестве одного из последних базовых нормативных документов в национальной сфере в США выступает также Закон «Об обмене информацией о кибербезопасности» 2015 года [5]**.** Этот закон, по сути, призван защитить представителей бизнеса от возможных судебных исков со стороны пользователей, если передаваемая властям информация о киберугрозах будет содержать в себе их персональные данные. Согласно закону, американские компании, в управлении которых находятся объекты критически важной инфраструктуры должны сотрудничать с правительственными органами, чтобы обе стороны были убеждены в надежности критически важных инфраструктур. К таким важным объектам в законодательных актах относят электро- и атомные станции, компьютерные сети банков и бирж, объекты коммунального хозяйства, например, городские системы водо- и газоснабжения и другие. Тем не менее, у закона есть и противники, требующие его отмены. Например, они считают, что закон радикальным образом изменит отношения между пользователями и компаниями. Он подрывает основы доверия в интернете, которые состоят в том, что компании работают в первую очередь на пользователей, а не на правительство. Против закона выступают и крупнейшие американские компании в сфере ИТ-технологий [6].

Законодательство о защите личных персональных данных не консолидировано: по-прежнему нормы о защите персональных данных приняты в рамках актов, действующих в конкретных областях правовых отношений. В частности, был принят ряд законов, предусматривающих уголовные наказания за несанкционированное использование личных данных пользователей. Среди них — Закон «О медицинском страховании» 1996 года [7], который регламентирует использование медицинскими институтами и страховыми компаниями защищенной информации о пациентах, хранящейся как в бумажном, так и электронном виде, возможные случаи ее раскрытия, а также процедуры обеспечения безопасности данных. За разглашение личных данных или их несанкционированное использование законом предусмотрено наказание до пяти лет лишения свободы [7]. Еще один акт той же направленности — закон «О краже личных данных» 1998 года, которым впервые федеральным уголовным правом США кража личных данных была отнесена к преступлениям. Закон предусматривает наказание за совершение или попытку совершения кражи личных данных (максимальный срок – 15 лет лишения свободы и максимальный денежный штраф в размере 250 тысяч долларов США) и конфискацию собственности, которая была использована для осуществления мошеннических действий, включая электронные устройства, программное обеспечение и средства технического обеспечения [8].

Подводя итоги по исследованию в указанной части, отметим, что для законодательства США в сфере обеспечения кибербезопасности характерны следующие основные черты. Во-первых, это законодательство достаточно массивно и широко распространено, оно проникает во все сферы жизни общества. Во-вторых, законодательство мало консолидировано; законодатель применяет в различных областях общественных отношений схожие механизмы, не создавая единого универсального правила. В-третьих, развита как публичная правовая, так и частная правовая база в области правового обеспечения кибербезопасности. В-четвертых, большое внимание уделяется организационным, процедурным моментам обеспечения кибербезопасности и взаимодействия различных субъектов права в указанной сфере.

Состояние разработки вопросов обеспечения кибербезопасности в Великобритании

В публичной сфере законодательство Великобритании об обеспечении кибербезопасности менее масштабно, нежели законодательство США. Тем не менее, массив нормативных правовых актов и здесь достаточно велик. Среди фундаментальных документов можно отметить Стратегию кибербезопасности (Cyber Security Strategy) от 25 ноября 2011 года

[9]. В Стратегии признается, что Интернет революционизирует наше общество, стимулируя экономический рост и давая людям новые способы общения и сотрудничества друг с другом. Снижение затрат означает, что доступ к Интернету станет дешевле и проще, что позволит большему количеству людей в Великобритании и во всем мире использовать его, "демократизируя" использование технологий и подпитывая поток инноваций и производительности. Все это будет стимулировать дальнейшее расширение киберпространства, и по мере его роста будет расти и ценность его использования. Как и в случае большинства изменений, увеличение нашей зависимости от киберпространства приносит новые возможности, но также и новые угрозы. В то время как киберпространство способствует развитию открытых рынков и открытых обществ, сама эта открытость может также сделать нас более уязвимыми для тех – преступников, хакеров, иностранных спецслужб – кто хочет причинить нам вред, компрометируя или повреждая наши критически важные данные и системы. Причем, эти последствия уже ощущаются и будут расти по мере того, как будет расти наша зависимость от киберпространства. Сети, на которые мы теперь полагаемся для наших повседневных нужд, выходят за рамки организационных и национальных границ. События в киберпространстве могут происходить с огромной скоростью, опережая традиционные реакции (например, эксплуатация киберпространства может означать, что такие преступления, как мошенничество, могут совершаться удаленно и в промышленных масштабах).

Таким образом, стратегия более оперирует понятием рисков, связанных с «расширением» киберпространства, в качестве неизбежного следствия последнего, а также признает уже сложившуюся зависимость от него общества. В отличие от стратегических документов в исследуемой сфере в США, британская стратегия изначально делает больший акцент не на государственных и национальных публичных интересах, а на интересах частных лиц – членов гражданского общества. В частности, в ней указывается, что в качестве основных целей стратегии такие факторы как: люди знают, как защитить себя от преступлений в Интернете; предприятия осознают угрозы, с которыми они сталкиваются, свои собственные уязвимости и работают с ними и т.п. Одновременно Стратегия не упускает из виду и возможную коммерческую выгоду: в качестве следствий ее реализации указано, чтобы британские компании, опираясь на свои сильные стороны, создали процветающий и динамичный рынок услуг кибербезопасности по всему миру, поскольку в нынешнем экономическом климате Великобритания как никогда нуждается в выявлении и использовании областей международной конкурентной силы для стимулирования роста. Реализация Стратегии, по мнению ее разработчиков, призвана показать, что Великобритания является безопасным местом для ведения бизнеса в киберпространстве. Непосредственно в стратегии заложены и внушительные суммы, которые должно выделять правительство для обеспечения кибербезопасности: 650 миллионов фунтов стерлингов государственного финансирования на четырехлетнюю Национальную программу кибербезопасности [10].

Стратегия в числе прочего предлагает поощрять суды в Великобритании использовать существующие полномочия для наложения соответствующих взысканий, предусматривает создание нового национального потенциала борьбы с киберпреступностью как частью новой национальной преступности, поощрение привлечения «кибер-специалистов», предусматривает технические меры в целях повышения осведомленности об угрозах в международной сети, содействует повышению уровня международного сотрудничества и взаимопонимания в указанной сфере. Особое внимание уделено улучшению реагирования на инциденты в связи с киберпреступностью, а также укреплению доверия в киберпространстве. Заявлен пересмотр существующего законодательства, например, Закона 1990 года «О неправомерном использовании компьютеров», с тем чтобы оно оставалось актуальным и

эффективным [11]. Предусмотрено даже создание единой системы отчетности для граждан и малого бизнеса о киберпреступности для принятия защитных мер для того, чтобы правоохранительные органы могли установить масштабы киберпреступности (включая то, как она влияет на отдельных лиц и экономику).

Обращаясь к частно-правовой сфере, основной проблематикой регулирования в Великобритании в указанной области также остаются вопросы обеспечения безопасности обмена сообщениями, которые опосредуют совершение юридически-значимых действий (служебная, государственная и частная переписка – передача информации, совершаемые государством регистрационные действия в отношении частных лиц и публичных субъектов права, заключение договоров и сделок в электронной форме, обработка персональных данных и их передача и т.п.). Традиционно в британском праве эти вопросы решаются применительно к контрактам, поскольку контракт как аналог служебного информирования распространен и системе государственного управления.

Состояние разработки вопросов обеспечения кибербезопасности в Республике Казахстан

В российской науке вопросы информационной безопасности непоследовательно и достаточно бессистемно изучались и в сфере управления [12]. Как правило, это касалось деятельности специализированных организаций (партийных органов, правоохранительных служб, органов безопасности, архивов и т.п.) и то лишь по отдельным вопросам. При этом авторы связывали необходимость обеспечения информационной безопасности более с охраной государственной тайны, что требовало «органического сочетания отраслевой и территориальной систем управления» [13], а иные функции института информационной безопасности рассматривались только с точки зрения комплексного экономического и социального развития регионов. Однако в обоих случаях информационная безопасность понималась не как самостоятельный институт права, а как разновидность управленческой, контрольной и надзорной практики компетентных органов, к тому же, комплексного подхода к проблеме не было.

В концепции кибербезопасности «Киберщит Казахстана», утвержденной Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 [14], указана необходимость развития собственной школы по разработке средств криптографической защиты информации и криптографии. Поскольку многие передовые технологии обеспечения информационной безопасности, разработанные в других странах, используются в государственных органах и организациях Республики Казахстан, то есть риск столкнуться с ситуацией, в которой Казахстан выступает в качестве объекта действительной атаки на важные объекты информационно-коммуникационной инфраструктуры. В связи с этим самостоятельное с учётом передового зарубежного опыта решение вопросов и проблем обеспечения криптографической защиты информации в информационном взаимодействии как внутри страны, так и в трансграничном пространстве до сих пор являются актуальными.

Фундаментальных исследований категории «кибербезопасность» нет и в настоящее время. Отдельные аспекты кибербезопасности находили отражение в публикациях, либо в учебных курсах по информационному праву, однако единого подхода, общей направленности на создание целостной картины категории «кибербезопасности» они не имели. Между тем данный вопрос требует глубинной разработки проблем кибербезопасности и ее совершенствования. Государства все более и более осознают ценность подхода с позиций кибербезопасности к правовому регулированию общественных отношений. Одной из причин довольно низкого уровня внимания к проблемам кибербезопасности на уровне ее научных разработок, нормотворческой регламентации и т.п. является довольно низкая на сегодняшний

день эффективность самого технологического обеспечения информационной безопасности. Получается замкнутый круг: информационная безопасность в киберпространстве так и не стала одним из значимых институтов общественной регуляции в силу своей малой эффективности, а эффективность ее низка поскольку к ней отсутствует необходимое внимание со стороны ученых-теоретиков, субъектов правотворчества и применения и иных заинтересованных государственно-властных структур.

Помимо разработки концепций кибербезопасности, проработки отдельных вопросов регулирования и, безусловно, популяризации этих разработок хотя бы в среде государственного аппарата, следует активно привлекать экспертов в области информационной безопасности в киберпространстве на всех этапах и стадиях любой разновидности юридической практики. Например, в последние десятилетия в правотворческой деятельности все большее значение придается различного рода экспертным исследованиям, проверкам проектов нормативно-правовых актов по различным критериям и параметрам. Законодательством об экологической экспертизе предусмотрена экологическая экспертиза проектов нормативно-правовых актов на предмет влияния практики их реализации на состояние экологической обстановки. Широко известна криминологическая экспертиза проектов. Немало высказано предложений и о экспертизе потенциальной «коррупционности» проекта, «взяткоемкости» урегулированных нормативным правовым актом процессов. Все это, безусловно, правильно и позитивно. Между тем, как в теории правотворчества, так и в практике деятельности правотворческих органов неоправданно не учитывается одна из наиболее значимых возможных экспертиз проектов нормативно-правовых актов – экспертиза с точки зрения последующей информационной безопасности того или иного нормативного правового акта. С позиций теории общественного производства нормативный правовой акт является, своего рода, общественным продуктом, благом, «потребляемым» обществом. Данный продукт, следовательно, должен быть «пригодным к потреблению» как сам по себе, так и в системе «потребления» других нормативно-правовых актов. Речь, таким образом, идет о необходимости «экспертизы информационной безопасности» проекта нормативно-правового акта как на предмет его внутренней согласованности и непротиворечивости, так и наиболее оптимального соотношения с другими нормативно-правовыми актами, позволяющими устранить те или иные внешние или внутренние угрозы, либо снизить соответствующие риски. В частности, можно говорить о применении собственно информационных методов обеспечения информационной безопасности в киберпространстве. Существо анализа информации выражается в обобщении и оценке следующих показателей и характеристик: уровень, структура, динамика, причины и условия, иные показатели деятельности. В зависимости от направления исследования возможны следующие виды аналитической работы: общий анализ состояния информационной безопасности в странах содружества; обзоры о работе органов государственной власти и местного самоуправления по соответствующему направлению их деятельности; анализ состояния информационной безопасности на отдельных крупных объектах; обобщение правоприменительной практики по отдельным сферам правовых отношений и другие.

Можно также говорить об особых способах обеспечения информационной безопасности, связанных с использованием трудовых ресурсов (привлечение к работе определенного количества специалистов, экспертов, работников вспомогательного персонала), правильного учета психологических особенностей людей. Для обеспечения этого, что для информационной безопасности необходимы человеческие ресурсы с особыми качествами. Прежде всего, всегда следует учитывать такие свойства человеческой личности как характер и темперамент [15]. Полагается, что наиболее предпочтителен для лиц, участвующих в процессе обеспечения информационной безопасности, сангвинический и холерический темпераменты. Такого рода

темпераменты будут наиболее соответствовать активной, поисковой составляющей деятельности по обеспечению информационной безопасности. Другим близким к темпераменту и не менее важным фактором является характер человека, который определяется в его отношении к самому себе, окружающим его людям и явлениям [16]. В отличие от темперамента характер является наиболее пластичными может подвергаться существенной корректировке с помощью различных способов социального воздействия [17]. Как отмечают авторы, крайне важным является изучение темперамента и характера людей при решении вопроса об их принятии на службу в правоохранительные органы и иные государственные органы. Думается, что в любой юридической деятельности (особенно профессиональной деятельности в сфере обеспечения информационной безопасности в киберпространстве) к лицам, ею занимающимся, предъявляется целый ряд существенных психологических требований. Указанное справедливо и в отношении лиц, обеспечивающих реализацию программ информационной безопасности. Среди желаемых черт их характера мы отметим стремление к компромиссу и согласованности, активность с одновременной уравновешенностью и т.п.

Необходимо также выделять управленческие методы обеспечения кибербезопасности, которые включают в себя разработку программ обеспечения информационной безопасности в киберпространстве определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц [18]. Стоить также отметить нормативные правовые акты Республики Казахстан для субъектов страховой деятельности, а именно: Постановление Правительства Республики Казахстан от 31 января 2001 года № 164 «Об утверждении Правил подготовки и использования сетей телекоммуникаций общего пользования, ресурсов единой сети телекоммуникаций для нужд государственных органов, органов обороны, безопасности и охраны правопорядка Республики Казахстан» [19]; Постановление Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 июня 2007 года № 177 «Об утверждении Требований к деятельности организации по формированию и ведению базы данных» [20]; Постановление Правления Национального Банка Республики Казахстан от 27 августа 2018 года № 198 «Об утверждении Правил формирования системы управления рисками и внутреннего контроля для страховых (перестраховочных) организаций, филиалов страховых (перестраховочных) организаций-нерезидентов Республики Казахстан» [21]. В этой связи можем указать, что среди управленческих методов важнейшими следует признать финансовые (денежные средства, ценности, доходы, источники их поступления и т.п.) методы или способы. Как правило, соответствующих строк нет ни в бюджетах всех уровней, включая федеральный, ни в сметах средств, выделяемых для обеспечения деятельности конкретных органов власти (властных вертикалей) и их должностных лиц. С другой стороны, даже при наличии таких указаний, наверное, невозможно было бы оценить финансовые ресурсы, предусмотренные для обеспечения информационной безопасности в киберпространстве, что называется, в целом. Это частично было бы возможно только в отношении конкретного органа (системы, вертикали и т.п. органов). Предполагается, что в определении финансовых затрат на обеспечение кибербезопасности крайне важно учитывать два момента. Во-первых, крайне важно выделить постоянные и переменные затраты, так как деятельность по обеспечению кибербезопасности осуществляют люди, для которых, как правило, данные обязанности не являются основными. Во-вторых, значительная затратная часть процесса обеспечения кибербезопасности – это оплата труда лиц, осуществляющих данную деятельность.

Обращаясь к средствам обеспечения кибербезопасности, при совершении волевых действий субъекты и участники названных правоотношений используют отдельные технические средства. В узком смысле слова под средством понимается орудие (предмет, совокупность приспособлений) для осуществления какой-либо деятельности, а вот А.В. Малько считает правовые средства правовыми явлениями, которые выражаются в инструментах и технологиях, при помощи которых удовлетворяются интересы субъектов права, обеспечивается достижение социально полезных целей [22], в нашем случае – обеспечение кибербезопасности. Средства обычно бывают обще-социальными, специально-юридическими, информационными, психологическими, техническими [23]. Например, в нашем случае такими средствами являются нормы права, определяющие порядок обеспечения безопасности информации, требования к ее защите и т.п. (правовые средства).

В целом же можно выделить самые разнообразные средства обеспечения кибербезопасности, которые как бы опосредуют те методы (способы), которыми кибербезопасность обеспечивается на практике. В частности, можно выделить физические; аппаратные; программные; аппаратно-программные (технические); криптографические; административные (организационные); законодательные (правовые); морально-этические и любые иные средства обеспечения кибербезопасности. Сосредоточимся на социальных и морально-этических средствах обеспечения кибербезопасности. Так, к правовым средствам относятся нормативные правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей [24–26]. К морально-этическим средствам относятся нормы поведения и правила обращения с информацией, которые традиционно сложились в том или ином обществе [27,28].

Подводя итоги, отметим, что одним из элементов содержания исследуемого правоотношения является также метод или способ (прием) совершения действий и операций, способ использования средств. Относительно стройная система общих методов обеспечения кибербезопасности предложена И.М. Рассоловым. В частности, указанный автор подразделяет методы на правовые, организационно-технические и экономические.

Не остается и без внимания вопрос и регламентации споров в сфере кибербезопасности. Так в 2016 году в Нью-Йорке была создана рабочая группа по вопросам кибербезопасности в международном арбитраже. В 2020 году группа выпустила «Протокол кибербезопасности» для международного арбитража [29]. Протокол кибербезопасности призван помочь заинтересованным сторонам в арбитражном процессе решать вопросы кибербезопасности, признавая, что арбитраж в настоящее время часто является в значительной степени цифровым процессом, который может быть предметом более распространенных кибератак. Протокол кибербезопасности преследует две цели:

1. Обеспечение основ для определения разумных мер информационной безопасности для индивидуальных арбитражей. Основа включает процедурное и практическое руководство для оценки рисков безопасности и определения доступных мер.

2. Повышение осведомленность об информационной безопасности в международных арбитражах, включая осведомленность о рисках информационной безопасности в арбитражном процессе.

Протокол состоит из 14 принципов, которые призваны обеспечить руководства высокого уровня для судов, сторон и управляющих учреждений при рассмотрении того, какие меры информационной безопасности целесообразно применять. Эти принципы дополняются пояснительными комментариями, графиками, глоссарием, образцом языка для решения

вопросов информационной безопасности. Например, примеры шагов, которые могут быть предприняты для лучшей защиты данных пользователей, список преобладающих стандартов кибербезопасности и другие соответствующие ресурсы. Протокол, несомненно, окажется полезным инструментом как для сторон, так и для трибуналов, чтобы обеспечить кибербезопасность в арбитраже, а также в качестве руководства для участников арбитража в привлечении внимания к проблеме исполнению соответствующих процедурных указаний. Кибербезопасность также необходимо решать в контексте уравновешивания конкурирующих требований к участникам арбитража в контексте обработки данных. Участники арбитража должны понимать свои индивидуальные обязательства, включая свои обязательства по защите данных в соответствии с «Общим регламентом по защите данных» (GDPR) от 27 апреля 2016 года [30] или другими применимыми законами о защите данных. Участники должны быть подготовленными для выполнения этих обязательств сбалансированным образом, который сохраняет интересы справедливости, скорости и эффективности арбитражного процесса. Поэтому, Протоколом кибербезопасности необходимо руководствоваться вместе с другими ресурсами по соблюдению требований защиты данных и применять в контексте доступных онлайн-инструментов, которые помогают оптимизировать арбитражный процесс и обмен данными между его участниками. Следует отметить, что в РФ существует Международный коммерческий арбитражный суд при Торгово-промышленной палате Российской Федерации (МКАС) с 1932 года. С 1999 года МКАС является членом Международной федерации коммерческих арбитражных институтов [31]. Если в США инструменты для решения международных споров начали готовить к концу 2020 годов, то еще с начала 2000 года в Индии был создан Кибер-апелляционный трибунал в соответствии с Законом «Об информационных технологиях» 2000 года под эгидой Контролера удостоверяющих органов (Controller of Certifying Authorities) [32]. Первый и единственный кибер-апелляционный трибунал в стране был учрежден центральным правительством Индии в соответствии с положениями, содержащимися в разделе 48 (1) Закона «Об информационных технологиях» 2000 года [33]. Создание кибер-апелляционного трибунала и Протокол кибербезопасности в системе международных арбитражей может иметь положительный результат. Механизмы правового регулирования могут быть повышены путем повышения осведомленности общественности и властей, а также путем привлечения компетентных кадров. Важно улучшить технологические возможности, чтобы справиться с возникшей ситуацией кибербезопасности. Необходимо поддерживать целостность, конфиденциальность и аутентификацию каналов и процессов связи. В отношении определенных видов правонарушений существует потребность в более быстром принятии решений в определенных судах. Неотъемлемая часть в регламентации вопросов кибербезопасности является международное сотрудничество.

Заключение

В статье предложены характеристики всех указанных выше методов. Дополнительно к ним предлагается выделять близкие к правовым методам научные методы, включая концепции, методики и т.п., в рамках организационно-технических методов и способов возможно выделение собственно информационных методов обеспечения кибербезопасности. Возможно также говорить об особых способах обеспечения кибербезопасности, связанных с использованием трудовых ресурсов (привлечение к работе определенного количества специалистов, экспертов, работников вспомогательного персонала), правильного учета психологических особенностей людей. Среди же управленческих методов важнейшими следует признать финансовые (денежные средства, ценности, доходы, источники их поступления и т.п.) методы или способы, которым также дана характеристика в работе.

Также можно выделять самые разнообразные средства обеспечения кибербезопасности, которые как бы опосредуют те методы (способы), которыми кибербезопасность обеспечивается на практике, например, физические; аппаратные; программные; аппаратно-программные (технические); криптографические; административные (организационные); законодательные (правовые); морально-этические и любые иные средства обеспечения кибербезопасности. Указанные виды средств объединены в три основные группы, предложены их наиболее важные характеристики. В целом, по результатам исследования возможно заключить, что законодательство Великобритании характеризуется не менее важными стратегическими положениями, чем и законодательство США в указанной сфере. Особо значимым можно считать приведенное в соответствии с реалиями киберпространства законодательство о борьбе с киберпреступностью, включая проблематику уголовной ответственности за киберпреступления. Некоторый «крен» в британском законодательстве в сторону регулирования вопросов кибербезопасности именно с точки зрения заключения и исполнения контрактов, передаче информации между частными лицами и т.п. и актуальная судебная практика большей часть по данному вопросу объясняется правовыми традициями романо-германской правовой семьи, а также тем, что по ряду вопросов (например, в части столь «популярного» в США законодательства о защите персональных данных) имеются акты Европейского Союза. Положения о выходе Великобритании из состава ЕС не предусматривают отмены действия данных актов на территории Великобритании до тех пор, пока они не войдут в конкуренцию с вновь принятыми национальными нормами права.

В целом, по результатам исследования, возможно систематизировать существующие на сегодня проблемы правового обеспечения кибербезопасности государств следующим образом. Во-первых, это проблемы защищенности внутренних информационных систем организаций, активно соприкасающихся с внешней средой посредством сети Интернет от проникновения извне (кибератаки и проч.), часть из которых имеет явный технический характер, но отдельные вопросы регулируются и правом. Указанные проблемы особенно актуальны для объектов критической инфраструктуры, а также банков и финансовых учреждений (кредитных организаций), где различные технологии производства продукта (например, банковского продукта) совмещаются с информационной технологией и не могут существовать без нее (например, в части проведения транзакций в электронном виде и т.п.). Во-вторых, это защита персональных данных в тех сферах (в том числе, на объектах критической инфраструктуры, где их аккумулируется объективно много, например, в сфере здравоохранения. Здесь тесно перемешаны вопросы правового и организационного характера. Для решения отмеченных выше и иных потенциально выделяемых проблем в указанной сфере в науке предлагаются различные средства и способы совершения действий и операций, использования средств. В этом смысле способ всегда конкретен - это как бы «путь» достижения поставленной цели с использованием конкретного арсенала средств в заданной ситуации, при наличии определенных внешних факторов. В каком-то смысле средства определяют способ (общее правило), но и способ влияет на выбор для использования конкретного набора средств (специфику набора). В науке информационного права данный вопрос разработан слабо. Большинство авторов стоит все-таки на управленческих и технологических позициях и предлагает в качестве способов обеспечения кибербезопасности выделять управление рисками, повышение устойчивости к деструктивным воздействиям (например, создание систем парирования и ликвидации последствий деструктивных воздействий), создание систем и средств защиты от угроз, уничтожение (изоляция) источников угроз [34].

Литература

1. National cyber security strategy of the United States of America of September of 2018.
2. Computer Security Act of 1987.
3. Federal Information Security Management Act of 2002.
4. Federal Information Security Modernization Act of 2014.
5. R. Burr, “S.754 - 114th Congress (2015-2016): To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.,” https://www.congress.gov/bill/114th-congress/senate-bill/754 (Дата обращения: 11.05.2021).
6. П. Тарасенко, “США повышают свою кибербезопасность – Мир – Коммерсантъ,” 2015. https://www.kommersant.ru/doc/2842133 (Дата обращения: 11.05.2021).
7. Health Insurance Portability and Accountability Act of 1996.
8. Identity Theft and Assumption Deterrence Act of 1998.
9. UK Cyber Security Strategy of 2011.
10. Crown Copyright, “Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review.”2010. [Электронный ресурс]. Available: https://webarchive.nationalarchives.gov.uk/20121018082048/http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf (Дата обращения: 11.05.2021)
11. Computer Misuse Act 1990.
12. П. М. Керженцев, *Принципы организации*. Государственное издательство «Ленинград - Москва», 1968.
13. В. Аверьянов, “Содержание деятельности аппарата государственного управления и его организационные формы,” *Советское государство и право*, № 6, сс. 60–68, 1988.
14. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 «Об утверждении Концепции кибербезопасности (“Киберщит Казахстана”).
15. Д. Котомин, “Влияние характера и темперамента человека на его юридическую деятельность,” 2010.
16. Э. Кречмер, “Строение тела и характер. Исследования к проблеме строения и к обучению теории темпераментов,” *М.: Изд-во Эксмо*, с. 112, 2003.
17. Д. С. Котомин, “Некоторые аспекты исследования технологии лоббистской деятельности,” *Юридическая техника*, № 3, 2009.
18. И. Рассолов, “Информационное право: учебник и практикум для академического бакалавриата,” *М.: Юрайт*, сс. 79–85, 2017.
19. Постановление Правительства Республики Казахстан от 31 января 2001 года № 164 «Об утверждении Правил подготовки и использования сетей телекоммуникаций общего пользования, ресурсов единой сети телекоммуникаций для нужд государственных органов, органов обороны, безопасности и охраны правопорядка Республики Казахстан».
20. Постановление Правления Агентства Республики Казахстан по регулированию и надзору финансового рынка и финансовых организаций от 25 июня 2007 года № 177 «Об утверждении Требований к деятельности организации по формированию и ведению базы данных».
21. Постановление Правления Национального Банка Республики Казахстан от 27 августа 2018 года № 198 «Об утверждении Правил формирования системы управления

рисками и внутреннего контроля для страховых (перестраховочных) организаций, филиалов страховых (перестраховочных) организаций-нерезидентов Республики Казахстан».

22. А. В. Малько, “Стимулы и ограничения в праве (Теорет.-информ. аспект),” 1995.

23. Б. Н. Карташов, *Юридическая деятельность: понятие, структура, ценность*. Изд-во Сарат. ун-та, 1989.

24. Е. В. Климович, “Административная ответственность как средство юридической защиты конфиденциальной компьютерной информации,” *Российское право в Интернете*, № 4, сс. 2–2, 2006.

25. Д. Б. Савчишкин, “Административная ответственность как средство обеспечения информационной безопасности.,” *Административное и муниципальное право*, № 6, сс. 55–63, 2011.

26. З. И. Хисамова, “Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий,” *Юридический мир*, № 2, сс. 58–62, 2016.

27. А. С. Кабанов, А. Б. Лось, and А. В. Суроев, “Методы социальной инженерии в сфере информационной безопасности и противодействие им,” *Российский следователь*, № 18, сс. 32–37, 2015.

28. С. В. Баринов, “О правовом определении понятия «информационная безопасность личности»,” *Актуальные проблемы российского права*, № 4 (65), 2016.

29. International Council for Commercial Arbitration, “ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2020 Edition).” 2020.

30. Общие правила защиты данных от 27 апреля 2016 года.

31. Торгово-промышленная палата РФ, “Международный коммерческий арбитражный суд. Материалы,” 2017. http://mkas.tpprf.ru/ru/materials/ (Дата обращения: 11.05.2021).

32. Ministry of Law, Justice and Company Affairs (Legislative Department), “Ministry of Law, Justice and Company Affairs (Legislative Department) | Ministry of Electronics and Information Technology, Government of India.” https://www.meity.gov.in/content/ministry-law-justice-and-company-affairs-legislative-department-0 (Дата обращения: 11.05.2021).

33. The Information Technology Act, 2000.

34. A. Maksurov, “Coordination in legal systems of the countries of Europe,” с. 119, 2018.

СИММЕТРИЯЛЫ ШИФРЛАРДА ҚОЛДАНЫЛАТЫН СЫЗЫҚТЫ ЕМЕС ТҮЙІНДЕРДІ ЗЕРТТЕУ

Д.С. Дюсенбаев[1,2], К.Т. Алғазы[1,2], Қ.С. Сақан[1,2]
email: dimash_dds@mail.ru
[1]ҚР БҒМ ҒК «Ақпараттық және есептеуіш технологиялар институты»
[2]әл-Фараби атындағы ҚазҰУ
Алматы қаласы, Қазақстан Республикасы

***Аннотация**. S-блоктарды құру және зерттеу симметриялы криптографияда негізгі жұмыстардың бірі болып табылады. Осыған байланысты, жұмыста S-блоктарды зерттеуге арналған бағдарлама жөнінде айтылған және осы бағдарламаның көмегімен өлшеміне байланыссыз кез-келген S-блоктың сипаттамаларын алуға болады. Сонымен бірге, бағдарламаның көмегімен басқа да белгілі алгоритмдердің ауыстыру кестелеріне талдау жүргізіп, нәтижесін салыстыруға болады.*

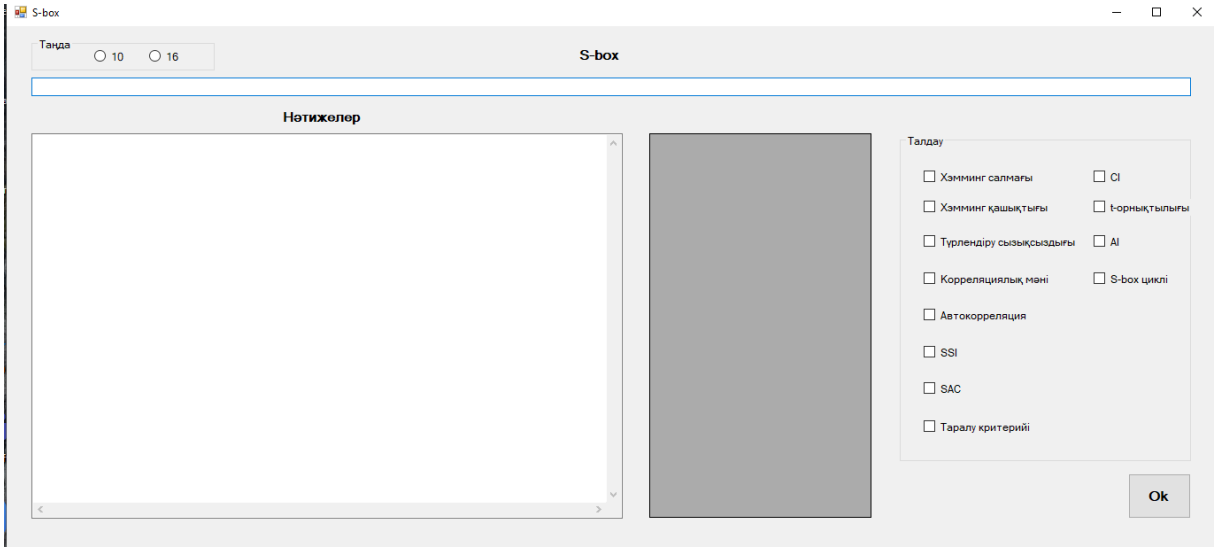
Қазіргі таңда, симметриялық блоктық шифрлар - ең кең таралған және тиімді криптографиялық примитивтердің бірі болып отыр. Оған себеп, кілтінің қысқалығы, шифрлау жылдамдығы және т.б. Заманауи блокты шифрлар құру, зерттеу және оны қолдану шарттарын негіздеу күрделі және уақытты қажет ететін жұмыс. Стандартталған криптоалгоритм қауіпсіздіктің жоғары деңгейін қамтамасыз етуі, қажетті жылдамдыққа ие болуы және әр түрлі есептеу платформаларында тиімді жұмыс істеуі қажет. Қазіргі заманғы көптеген алгоритмдердің құрылымы сызықты және сызықты емес түйіндерден тұрады. Сызықты түрлендірулерді – ашық мәтін элементтерін араластыру үшін, сызықты емес түйіндерді – ашық мәтін мен шифр мәтін арасында сызықты емес байланыс жасау үшін пайдаланады. Ал, сызықты емес түйін ретінде көп жағдайда S-блок ауыстырулары пайдаланылуда, яғни олар шифрлаудың сызықты-еместігін анықтайтын бірден-бір элемент болып табылады. Сондықтан, блокты шифрлаудағы басты есептерінің бірі *S*-блоктардың қасиеттерін зерттеу және оларды жетілдіру жолдарын қарастыру болып табылады.

S-блок – кірісі *n*-биттен және шығысы *m*-биттен тұратын функция. Практикалық себептеріне байланысты *S*-блоктың өлшемі 8-ден 10-ға дейінгі аралықта (диапазонында) болғаны тиімді [1]. Криптографиялық примитивтерді әр түрлі шабуылдардан қорғау үшін S-блоктар бірқатар критерийлерге сәйкес келуі керек [2-3]. Олардың көптігіне, бір-біріне сәйкес келмеуіне немесе ішінара тәуелділігіне байланысты барлық талаптарды қанағаттандыратын ауыстыру кестесін құру қиынға соғады. Осыған байланысты, іс жүзінде нақты бір симметриялық алгоритмге қажет сызықтық емес түйіндер қолданылады. Мұндай S-блоктар әдетте тиімді S-блоктар деп аталады [4-5].

S-блокқа сызықтық, дифференциалдық және басқа да статистикалық талдау жасайтын компьютерлік бағдарлама құрылды. Бағдарламаның негізгі жұмыс терезесі 1-суретте көрсетілген. Осы бағдарламаның көмегімен S-блоктардың келесі сипаттамаларын алуға болады:

- хэмминг салмағын;
- хэмминг қашықтығы;
- сызықсыздықтың минималды және максималды мәндерін;
- корреляциялық минималды және максималды мәндерін;
- автокорреляциялық минималды және максималды мәндерін;
- теңшелгенін немесе теңшелмегенін;
- SSI (sum-of-squares indicator) мәнін;
- SAC (strict avalanche criterion) орындалуын;

- таралу критерийінің шарттарының орындалуын;
- CI (correlation immunity) орындалуын;
- t-орнықтылығын;
- циклын.



Сурет 1 – S-блокты талдауға арналған бағдарламаның негізгі терезесі

Жоғарыда аталған сипаттамалардың көмегімен S-блоктың тиімділігін анықтау үшін қолданылатын негізгі ұғымдар мен анықтамаларды келтірейік [6 – 9]. Мұндағы, n – айнымалылар саны.

Теңшелген деп бульдік функцияның ақиқаттар таблицасындағы мәндер жиынындағы «0» мен «1»-дің тең болуы: $hw(f) = 2^{n-1}$.

Аффиндық функция деп $f = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n \oplus a_0, a_i \in GF(2), i = 0,1,2,\ldots,n$ түрдегі бірінші дәрежелі алгебралық қалыпты формасын айтады, егер $a_0 = 0$ болса, онда f функциясы сызықты деп аталады.

α векторының *Хэмминг салмағы* деп вектордағы (тізбектегі) бірліктер саны және hw(α) түрінде белгіленеді: $hw(f) = \sum_{x=1}^{2^n} f(x)$.

Хэмминг қашықтығы $d(f,g)$ дегеніміз екі тізбектің немесе вектордың сәйкес орындағы (позициядағы) мәндердің тең болмауының саны (басқаша айтсақ, нөлдік емес вертикалды биграммалар саны), мұндағы $d(f,g)$ - f және g функцияларының сәйкес позициядағы тең емес мәндерінің саны: $hd(f,g) = \sum_{x=1}^{2^n}(f(x) \oplus g(x))$.

N_S түрлендірудің сызықсыздығы дегеніміз S түрлендіруінің шығыс тізбегі мен қандай да бір өрістегі барлық аффиндық функциялардың шығыс тізбектерінің арасындағы ең кіші (минималды) Хэмминг қашықтығы: $N_S = \min\{d(S,\varphi)\}$, мұндағы φ - аффиндық функциялар жиыны.

N_f функцияның сызықсыздығы дегеніміз f функциясы мен $GF(2^n)$ өрісіндегі барлық аффиндық функциялардың арасындағы ең кіші Хэмминг қашықтығы: $N_f = \min\{hd(f,\varphi)\}$, мұндағы φ - аффиндық функциялар жиыны. Немесе $N_f = \frac{1}{2} \cdot (2^n - \max(|W(\omega)|))$, $W(\omega)$ – корреляциялық мән арқылы анықтауға болады.

Бульдік функциясының алгебралық қалыпты формасы (АҚФ немесе Жегалкин көпмүшелігі) деп келесі өрнекті айтамыз:

$f(x_1, x_2, \dots, x_n) =$
$a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus \dots \oplus a_{i\dots i+j} x_i \dots x_{i+j} \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n, \quad a_i \in GF(2), i = 0,1,2, \dots, n.$ Бульдік функцияның дәрежесі деп алгребралық қалыпты форманың (АҚФ) коэффициенті нөлден өзгеше мономдардың ең жоғары дәрежесі айтылады.

$GF(2^n)$ өрісіндегі f функциясының $F(\omega)$ *Уолш түрлендіруі* $F(\omega) = 2^{-n} \sum_x (-1)^{f(x) \oplus \langle \omega, x \rangle}$ функциясының нақты мәндерді қабылдауымен анықталады, мұндағы $\langle \omega, x \rangle$ – скаляр көбейтінді.

$f(x)$ бульдік функциясы мен барлық сызықты функциялар жиыны арасындағы *корреляциялық* мән Уолш түрлендіруі ретінде анықталады: $W(\omega) = \sum_{x=1}^{2^n} (-1)^{f(x) \oplus \langle \omega, x \rangle}$.

$r_f(\alpha)$ *автокорреляциялық функциясы f(x)* бульдік функциясының ақиқаттар кестесіндегі $\alpha \in GF(2^n)$ бағытындағы барлық айнымалылар үшін функцияның туындысы болып табылады және келесідей түрде беріледі: $r_f(\alpha) = \sum_{x=1}^{2^n} (-1)^{f(x) \oplus f(x \oplus \alpha)}$. Басқаша айтқанда, $r_f(\alpha)$ автокорреляциялық функция - $f(x)$ функциясы α орынға жылжығанда өзінен қаншалықты өзгеретінін көрсетеді, кейде оны индикатор деп де атайды.

Автокорреляциялық функцияның *максималды абсолютті мәні* келесідей анықталады: $|AC|_{max} = max_\alpha |r_f(\alpha)|$.

SSI «квадраттар қосындылары» (sum-of-square indictors): $\sigma = \sum_{x=1}^{2^n} r_f^2(\alpha)$.

$f(x)$ бульдік функциясының *лавиндік әсердің қатаң критерийін* (SAC) қанағаттандырады дейді, егер барлық s үшін келесі шарттар орындалса:

$$\begin{cases} hw(s) = 1 \\ \sum_{x=1}^{2^n} \big(f(x) \oplus f(x \oplus s)\big) = 2^{n-1} \cdot \end{cases}$$

$f(x)$ буль функциясы $k(PC(k))$ *ретті таралу критерийін* қанағаттандырады, егер тек нөлдік емес $\alpha \in GF(2^n)$ векторы үшін келесі шарттар орындалса:

$$\begin{cases} 1 \le hw(\alpha) \le k \\ \sum_{x=1}^{2^n} \big(f(x) \oplus f(x \oplus \alpha)\big) = 2^{n-1} \cdot \end{cases}$$

$f(x)$ буль функциясы $m(CI(m))$ *ретті корреляциялық иммунитетке* ие болады, егер төмендегі теңдеулер жүйесі барлық w үшін ақиқат болса:

$$\begin{cases} 1 \le hw(w) \le k \\ W(w) = 0 \end{cases} .$$

Егер $f(x)$ буль функциясы бір уақытта теңшелген және t-ші ретті корреляциялық иммунитетке ие болса, онда мұндай функция *t-орнықты* деп аталады.

$g(x)$ функциясы $f(x)$ функциясының аннигиляторы болсын, яғни $f(x) \cdot g(x) = 0$. Онда $g(x) \neq 0$ функциясының минималды алгебралық дәрежесі $f(x)$ функциясының *алгебралық иммунитеті* деп аталады, егер $\begin{bmatrix} f(x) \cdot g(x) = 0 \\ (f(x) \oplus 1) \cdot g(x) = 0 \end{bmatrix}$ орындалса және ол $AI(f)$ арқылы белгіленеді.

Мысал ретінде, аталған бағдарламаның көмегімен 4x4 өлшемді S-блокты зерттеп көрейік.

1-кесте – S-блок ауыстыруы.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	9	14	5	1	8	11	13	10	6	7	15	3	12	4	0	2

2-кесте – S-блок ауыстыруының екілік түрде жазылуы.

x	x_1	x_2	x_3	x_4	y_1	y_2	y_3	y_4	y
0	0	0	0	0	1	0	0	1	9
1	0	0	0	1	1	1	1	0	14
2	0	0	1	0	0	1	0	1	5
3	0	0	1	1	0	0	0	1	1
4	0	1	0	0	1	0	0	0	8
5	0	1	0	1	1	0	1	1	11
6	0	1	1	0	1	1	0	1	13
7	0	1	1	1	1	0	1	0	10
8	1	0	0	0	0	1	1	0	6
9	1	0	0	1	0	1	1	1	7
10	1	0	1	0	1	1	1	1	15
11	1	0	1	1	0	0	1	1	3
12	1	1	0	0	1	1	0	0	12
13	1	1	0	1	0	1	0	0	4
14	1	1	1	0	0	0	0	0	0
15	1	1	1	1	0	0	1	0	2

Жасалаған компьютерлік бағдарлама арқылы алынған нәтижелер:

- хэмминг салмағы – 8;
- теңшелген – True;
- хэмминг қашықтығы – 8;
- сызықсыздықтың минималды мәні – 4;
- сызықсыздықтың максималды мәні – 12;
- корреляциялық минималды мәні – «-8»;
- корреляциялық максималды мәні – «8»;
- автокорреляциялық минималды мәні – «-8»;
- автокорреляциялық максималды мәні – «-8»;
- SSI минималды мәні – 640;
- SSI максималды мәні – 640;
- SAC – False;
- таралу критерийі – False;
- CI (correlation immunity) – False;
- t-орнықтылық – False;
- циклдар – 1: - (0; 14; 11), 2: - (4; 13; 4), 3: - (12; 12; 1).

Бағдарламаның көмегімен алынған нәтижелерге саралау жүргізейік. Хэмминг салмағы, теңшңлгендігі және хэмминг қашықтығы - қойылатын талаптарды қанағаттандырады. Зерттеліп отырған S-блоктың өлшемі 4x4 болғандықтан сызықты криптоталдауға берік болуы үшін алынатын мән 2^3=8 дің маңайында болуы керек. Алынған нәтижелерде минималды және максималды мәндері сәйкесінше 4 және 12-ге тең. Олай болса, ауытқуы 4 – ке тең, ал ауытқу ықтималдығы 0,25-ке тең болады. Яғни, зерттеп отырған S-блок сызықты криптоталдауға берік емес деген қорытынды шығаруға болады. Сонымен қатар, SAC, таралу критерийі, CI, t-

орнықтылық шарттары орындалмайды. Циклдарын қарайтын болсақ, үшінші циклдың ұзындығы 1-ге тең, яғни өзгермейтін немесе бекітілген нүктесі бар. Қорыта айтқанда, мысал үшін таңдап алынған S-блок қойылатын талаптарды толық қанағаттандырмайды.

Аталған бағдарламаның көмегімен кіріс және шығыс өлшемдері бірдей кез-келгшен ұзындықтағы S-блокты бағалауға болады.

Жұмыс Қазақстан Республикасы Білім және ғылым министрлігінің AP08856426 «Шифрлау алгоритмін әзірлеу және зерттеу және оны іске асыру үшін бағдарламалық-аппараттық кешен құру» гранттық қаржыландыру бағдарламасы аясында жүзеге асырылды.

Әдебиеттер тізімі

1. В. Столлингс Криптография и защита сетей: принципы и практика. 2-е изд. / Пер. С англ. – М.:Вильямс, 2001.
2. Daemen J. AES Proposal: Rijndael, AES algorithm submission [Electronic resource] / J. Daemen, V. Rijmen. – Mode of access : www. URL:! http://csrc.nist.gov/archive/aes/index.html.
3. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування: Підручникдля вищих навч. закладів. – Харків: Вид-во «Форт», 2013. – 880 с.
4. Казимиров А. В. Использование векторных функций при генерации подстановок для симметричных криптографических преобразований // Системи обробки інформації. –2012. – № 6 (104). – С. 97–102.
5. Казимиров А. В. Метод построения нелинейных узлов замены на основе градиентного // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2013. – Вып. 172: Информационная безопасность. – С. 104–108.
6. Bart Preneel. Analysis and Design of Cryptographic Hash Functions. [Электронный ресурс] – Режим доступа: homes.esat.kuleuven.be/~preneel/phd_preneel_ feb1993.pdf
7. Carlet C. Vectorial Boolean functions for // CambridgeUniv. Press, Cambridge. – 95 p. [Электронный ресурс] – Режим доступа: www.math.univ-paris13.fr/~carlet/chap-vectorial-fcts-corr.pdf
8. Carlet C. Boolean functions for cryptography and error correcting codes // Cambridge Univ. Press, Cambridge. – 2007. – 148 p. [Электронный ресурс] – Режим доступа: www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf
9. A.A. Kuznetsov, I.M. Bilozertsev, A.V. Andrushkevych // Applied Radio Electronics: Sci. Journ. — 2015. — Vol. 14. — № 4. — P. 343–350.

ОСОБЕННОСТИ, ТРЕБОВАНИЯ, АТРИБУТЫ И МЕТРИКИ ЗАЩИЩЕННОСТИ ПРОГРАММНЫХ СРЕДСТВ КОСМИЧЕСКОГО НАЗНАЧЕНИЯ

Е.Е. Исмаил, Н.К. Утелиева, Р. Мулаев, Т.Ауельбеков, А. Кусаинов
e-mail: e.ismail@aues.kz, nurshatu7@mail.ru, rus.mulaev@mail.ru, temirlan261096@gmail.com
НАО «Алматинский университет энергетики и связи им. Гумарбека Даукеева»,
г. Алматы, Республика Казахстан,

Аннотация. *Целью данной работы является анализ особенностей защищенности программных средств космического назначения (ПСКН), идентификация и формализация основных атрибутов и метрик характеристик связанных с защищенностью. Проведен анализ особенностей и требований к защищенности ПСКН. Идентифицированы основные объекты защищенности ПСКН и влияющие факторы, а также критерии их оценки. Определены базовые атрибуты и предложен комплекс метрик для количественной оценки защищенности ПСКН. Полученные результаты создают предпосылки для формализации и объективного решения задачи количественной оценки защищенности ПСКН.*

Ключевые слова: защищенность программных средства космического назначения, особенности, требования, модель, атрибуты, метрики

1. Введение

Растущая сложность и вследствие этого уязвимость программно-технических комплексов и программного обеспечения космических систем для случайных и непредвиденных негативных воздействий выводят проблему защищенности программных средств космического назначения (ПСКН) в разряд важнейших в космической инженерии. Сложность современных программных продуктов, а также многообразие средств, которые могут быть использованы злоумышленниками для их взлома, приводят к необходимости разработки формальных методов анализа и оценки свойств защищённости.

Недостаточное внимание к защищенности программного обеспечения систем критического назначения во многих случаях обуславливает дефекты и отказные ситуации. Недостаточно формализуются требования к защищенности ПСКН, к характеристикам и атрибутам, которыми они должны определяться, а также как их необходимо измерять и оценивать соответствие заданным требованиями.

Оценка защищенности, являющейся важнейшей составляющей качества ПСКН, является жизненно важным условием для его последующего применения. Важно наличие у разработчиков подтверждения того, что это ПСКН обладает заданными свойствами и имеет определенную степень защиты от влияния преднамеренных или случайных изменений.

Тщательная спецификация, анализ и оценка защищенности ПСКН является ключевым фактором их эффективного применения. Это может быть достигнуто на основе выделения, определения и обеспечения требуемых характеристик защищенности с использованием стандартизированных и формализованных методов.

Традиционная неопределенность понятия защищенность ПО и их атрибутов, обычно приводит к тому, что реальные значения этих характеристик также остаются весьма неопределенными.

В серии современных стандартов качества ПО ISO/IEC 25000 (SQuaRE) определена концепция и общая методология описания и оценки качества программных продуктов общего назначения. Однако, в них не определены конкретные показатели, метрики, методы

измерения, которые позволили бы оценить установленные характеристики качества, особенно для критических программных средств. В связи возникает необходимость устанавливать свои собственные модели качества конкретных ПО с учетом их особенностей, метрики и методы измерения приоритетных атрибутов характеристик качества, таких безопасность.

Целью данной работы является анализ особенностей защищенности ПСКН, внесение определенности в отношении понятия защищенности ПО с позиции общей методологии оценки качества программного продукта, принятой в семействе международных стандартов ISO/IEC 25000, а также идентификация и формализация основных атрибутов и метрик показателей связанных с защищенностью ПСКН.

2. Понятие, модель, объекты и угрозы защищенности ПСКН

В соответствие с моделью качества программного продукта, установленного стандартом ISO/IEC 25010 [1], «защищенность (Security)» является характеристикой качества верхнего уровня модели качества, которая характеризует внутреннее и внешнее качество программного продукта.

Защищенность программного продукта в ISO/IEC 25010 определяется, как степень защиты программным продуктом или системой путем ограничения доступа людей, других продуктов или систем к данным в соответствии с типами и уровнями авторизации. Защищенность применима также и к данным при передаче в случаях, когда данные сохраняются непосредственно в продукте или системе или вне их [1]. Для характеристики «защищенность» в стандарте ISO/IEC 25010 определены следующие подхарактеристики (атрибуты): «Конфиденциальность» (Confidentiality), «Целостность» (Integrity), «Неподдельность» (Non-repudiation), «Отслеживаемость» (Accountability) и «Подлинность (аутенчиность)» (Authenticity).

В стандарте ISO/IEC 9126-1:2001 «защищенность (Security)» имеет статус подхарактеристики характеристики «Функциональные возможности (Functionality)» и определяется как «атрибуты программного обеспечения, относящиеся к его способности предотвращать несанкционированный доступ, случайный или преднамеренный, к программам и данным» [2].

В работе [3] защищенность программного средств определяется, как «примитив качества программного средства, который представляет собой свойство, характеризующее способность программного средства противостоять преднамеренным или нечаянным деструктивным (разрушающим) действиям пользователя».

В [4] предлагается рассматривать понятие защищённости программного продукта, как «способность противодействовать несанкционированному вмешательству в нормальный процесс его функционирования, а также попыткам хищения, незаконной модификации, использования, копирования или разрушения самого программного продукта, его составляющих, данных и информации, входящих в состав продукта, доступных ему в процессе выполнения или заложенных в него во время разработки».

В стандарте ГОСТ 28806-90 [5] дано следующее определение защищенности программного средства: «Совокупность свойств программного средства, характеризующая его способность предотвращать несанкционированный доступ как случайный, так и умышленный, к программам и данным, а также степень удобства и полноты обнаружения результатов такого доступа или действий по разрушению программ и данных».

Анализируя вышеприведенные определения, предлагается рассматривать характеристику «защищенность программного средства» как совокупность свойств (атрибутов) ПС, определяющих его способность обеспечивать заданную степень защиты самого программного продукта, его функций и информационных процессов, данных,

используемых и вырабатываемых в процессе функционирования, от несанкционированного доступа в соответствии с типами и уровнями авторизации, а также преднамеренных или случайных деструктивных действий. Такой подход не противоречит нормативному определению характеристики «защищенность программного продукта», данному в стандарте ISO/IEC 25010. В то же время позволяет более четко определить объекты и функции защиты.

В соответствие с предложенным определением характеристики «защищенность программного средства», можно выделить следующие основные объекты защиты:

- программный продукт и его компоненты (объектный код программ, который выполняется вычислительными средствами в процессе в процессе их функционирования);
- функции программного продукта (исполняемые модули, нарушение целостности которых может привести к изменению логики работы ПС);
- данные и информация, входящие в состав ПС и доступные ему в процессе функционирования;
- данные и информация, которая вырабатывается в процессе функционирования ПС и передается выдается потребителям (пользователям), на управляющие устройства.
- информационные процессы, реализуемые ПС в процессе функционирования;
- входная информация и данные (подлинность, достоверность).

На объекты защиты воздействуют различные дестабилизирующие факторы (угрозы), которые влияют на защищенность ПС. Все источники дестабилизирующих факторов можно разделить на внутренние, присущие самим объектам, и внешние, обусловленные средой, в которой функционирует ПО.

В таблице 1 систематизированы факторы, влияющие на защищенность ПСКН, и приведены критерии оценки, используемых для анализа таких факторов.

Таблица 1 - Факторы, влияющие на защищенность ПСКН, и критерии их оценки

Факторы, влияющие на защищенность ПСКН	**Критерии оценки**
1 Дефекты процессов разработки ПСКН	Отсутствие дефектов при определении целей и задач проектирования ПО, при формулировании требований к функциям и характеристикам средств обеспечения защиты; Отсутствие дефектов и ошибок при определении условий и параметров внешней среды, в котором должны быть применены ПС; Отсутствие ошибок проектирования функций защиты; Отсутствие ошибок и дефектов программирования в текстах программ и описаниях данных, а также в документации на ПО; - Эффективность выбранных методов и средств защиты программ и данных, восстановления работоспособности системы в условиях случайных и преднамеренных негативных воздействий.
2 Дефекты программного продукта	Отсутствие дефектов в реализации функций ПСКН; Прослеживаемость функций на соответствие требованиям к ПСКН; Независимость проведения верификации ПСКН; Полнота тестирования ПСКН.

Факторы, влияющие на защищенность ПСКН	Критерии оценки
3 Непредвиденные, случайные факторы, оказывающие негативные воздействия на защищенность	Степень защищенности от искажений и потерь данных в телекоммуникационных каналах; Наличие функций предварительной обработки и контроля достоверности данных, поступающих от внешних источников и передаваемых потребителям; Наличие функций обработки исключительных ситуаций при искажении и выходе за допустимые пределы значений входной и выходной информации; Наличие функций защиты от сбоев и отказов в вычислительной и телекоммуникационной и другой аппаратуре.
4 Преднамеренные негативные воздействия с целью искажения, уничтожения или хищения программ, данных	Наличие функции контроля и регистрации доступа к данным; Наличие функций защиты от несанкционированного доступа; Наличие функций защиты данных; Наличие функций защиты от вирусов.
5 Ошибки и несанкционированные действия оперативного, административного и обслуживающего персонала в процессе эксплуатации ПО и системы	Наличие функций обработки ситуаций, связанных с ошибками персонала; Наличие функций обработки ситуаций, связанных с несанкционированными действиями персонала

3. Атрибуты и метрики защищенности ПСКН

Одним из подходов для оценивания защищенности ПСКН является методология оценки характеристик качества ПС, принятая в семействе международных стандартов ISO/ IEC 25000, которая основана на оценке соответствующих атрибутов качества, установленной для каждой характеристики качества.

В соответствие с этой методологией, для оценивания защищенности ПСКН и установления соответствия показателей защищенности требованиям технических заданий и спецификаций необходимо установить комплекс измеряемых показателей (мер), специальные метрики и обеспечить их измерение с требуемой объективностью, точностью и достоверностью.

Для характеристики «Защищенность (Security)» стандартом ISO/IEC 25010 установлены следующие атрибуты (подхарактеристики): «Конфиденциальность» (Confidentiality), «Целостность» (Integrity), «Неподдельность» (Non-repudiation), «Отслеживаемость» (Accountability) и «Подлинность (аутенчиность)» (Authenticity) [1].

Для каждого из перечисленных атрибутов необходимо определить набор метрик, позволяющих количественно оценить соответствующие атрибуты ПС. Под метрикой понимается система измерений качества ПС, позволяющая получить численное значение некоторого его свойства. Метрика включает оцениваемый показатель или меру (quality measures) и его оценочные элементы (quality measure element), количественный масштаб (шкалу) и метод, используемый для измерений.

В стандарте ISO/IEC 25010 определен набор базовых метрик для базовых подхарактеристик, однако эти стандартные метрики не могут в полной мере характеризовать

защищенность конкретного ПС с учетом его особенностей. Поэтому рекомендуется расширять стандартный набор метрик или разрабатывать собственные метрики, в которых будет более точно учтены проблемы и особенности защищенности конкретных ПС. Практика также показывает, что большая часть наиболее важных метрик в ответственных проектах разрабатывается индивидуально на основе особенностей проекта, целей, назначения, условий реализации и др.

Анализ существующих метрик, предлагаемых для оценки защищенности ПС, показывает следующее:

- существует небольшое количество общепринятых метрик, применимых для характеристики защищенность (эти метрики, как правило, предназначены для оценки отдельных аспектов информационной безопасности); применение этих метрик для оценки защищенности ПСКН не даёт гарантированной уверенности в защищенности программного продукта;
- существующие метрики не учитывают специфику ПСКН (требования к защищенности, объекты защиты, факторы, влияющие на защищенность и др.);
- отдельные метрики носят чисто теоретический характер, поэтому их реализация для проведения оценки защищенности ПСКН в реальных условиях достаточно проблематична;
- некоторые из предлагаемых оценочных показателей являются достаточно сложными для их измерения.

Для оценки характеристик безопасности ПСКН целесообразно установить метрики и методы их измерения с учетом их особенностей, условий конкретного приложения и установленной категории критичности. Кроме того выбранные метрики защищенности ПСКН должны соответствовать общепринятым требованиям, таких как: коррелируемость, трассируемость, непротиворечивость, предсказуемость и селективность.

Характеристика «Защищенность» в соответствие со стандартом ISO/IEC 25010 рассматривается в отношении внутреннего и внешнего качества программного продукта [1]:

- показатели внутреннего качества применительно к характеристике «Защищённость» это показатель степени, с которой свойства программного продукта, связанные к его архитектурой, структурой и компонентами, обеспечивают заданные требования к защищенности;
- показатели внешнего качества применительно к характеристике «Защищённость» это показатель степени, с которой поведение (функционирование) программного продукта, удовлетворяет заданным и реализованным требованиям к его защищенности.

Ниже в таблицах 2 и 3 приведены предлагаемые для ПСКН метрики для оценки характеристики «Защищенность (Security)» применительные для внешнего и внутреннего качества.

Таблица 2 - Метрики характеристики «Защищенность (Security)» внешнего качества ПСКН

№	Название и назначение метрики	Меры, оценочные элементы, интерпретация значений
1.1	Степень обеспечения конфиденциальности (Confidentiality). Оценка уровня обеспечения ограничения несанкционированного доступа (НСД) к ресурсам ПС (функции, данные)	а) Уровень протоколирования доступа: X = A/B: A - число фактов доступа к ресурсам ПС (функции, данные), зафиксированных в протоколе системы; B - число фактов доступа к ресурсам ПС, которые были произведены во время испытаний;

		b) Уровень контролируемости доступа общая: X = A/B: A - количество выявленных и предотвращенных попыток НСД к ресурсам ПС; B - количество попыток НСД к ресурсам ПС; c) Уровень контролируемости доступа по видам НСД: X = A/B: A - число обнаруженных видов НСД; B - число видов НСД в спецификации; 0<=X<=1, чем ближе к «1», тем лучше.
1.2	Степень обеспечения целостности (Integrity). Оценка степени предотвращения модификации компьютерных программ или данных	a) Уровень защищенности от искажения и потери данных: X = A/B, где A - количество случаев выявления и успешного восстановления искаженных или утерянных данных; B - количество попыток искажения или уничтожения данных; 0<=X<=1, чем ближе к «1», тем лучше; b) Уровень защищенности от перехвата данных: X = 1-A/B, где A - количество успешных попыток перехвата и расшифровки данных; B - количество выполненных попыток перехвата и расшифровки данных; 0<=X<=1, чем ближе к «1», тем лучше.
1.3	Степень обеспечения доказуемости действий (Non-repudiation) Оценка степени, с которой может быть доказан факт события или действия, связанного с защищенностью	a) Способность к мониторингу текущего состояния - определяют экспертным методом; б) Способность удостоверения доступа: X = A/B, где A - количество выявленных и удостоверенных случаев доступа к системе или данным; B - количество фактических случаев доступа к системе или данным; 0<=X<=1, чем ближе к «1», тем лучше.
1.4	Степень обеспечения учета (контроль, регистрация) действий по доступу к системе, данным (Accountability) Оценка степени отслеживаемости действий по контролю и регистрации доступа к системе, данным.	a) Способность выполнения контроля и регистрации выполняемых действий - определяют экспертным методом; б) Способность учета доступа к системе, данным: X = A/B, где A - количество зафиксированных случаев доступа к системе или данным; B - количество фактических случаев доступа к системе или данным; 0<=X<=1, чем ближе к «1», тем лучше.
1.5	Степень подлинности объекта или ресурса (Authenticity) Оценка степени тождественности и подлинности объектов, ресурсов, процессов перед предоставлением доступа к данным	Способность проверки подлинности объектов, ресурсов, процессов перед предоставлением доступа к данным - определяют экспертным методом

Таблица 3 - Метрики характеристики «Защищенность (Security)» внутреннего качества ПСКН

№	Название и назначение метрики	Меры, оценочные элементы, интерпретация значений
2.1	Степень реализации требований к конфиденциальности (Confidentiality). Оценка степени реализации требований и функций по защите от НСД к ресурсам ПС	a) Уровень полноты реализации требований и функций контроля НСД: X = A/B, A - количество реализованных требований к управлению и контролю доступа к ресурсам ПП; B - количество требований к управлению и контролю доступа к ресурсам ПП, которые заданы в спецификациях; b) Уровень полноты реализации требований и функций контроля по типам доступа: X = A / B, A - число типов доступа, которые были зарегистрированы корректно, как определено в спецификации; B - число реализованных типов доступа, которые должны регистрироваться по спецификации; 0<=X<=1, чем ближе к «1», тем лучше.
2.2	Степень реализации требований к целостности (Integrity). Оценка степени реализации требований и функций по обеспечению предотвращения модификации ПС или данных	a) Уровень полноты реализации требований защищенности от искажения и потери данных: X = A/B; A - число реализованных механизмов защиты от повреждения данных; B - число механизмов защиты, требуемых по спецификации; b) Уровень полноты реализации функций защиты от искажения и потери данных: X = A / B, где A - количество типов искажения или потери данных, для которых реализован механизм выявления и восстановления; B - количество типов искажения или потери данных, для которых по спецификациям должен быть реализован механизм выявления и восстановления; 0<=X<=1, чем ближе к «1», тем лучше; c) Уровень полноты реализации функций защиты от перехвата данных: X = A / B, где A - количество реализованных механизмов шифрования для защиты данных от их перехвата; B – количество механизмов криптографической защиты данных, которые должны быть реализованы по спецификациям; 0<=X<=1, чем ближе к «1», тем лучше.

2.3	Степень реализации требований к обеспечению доказуемости действий (Non-repudiation) Оценка степени реализации требований и функций по обеспечению доказуемости действий, связанных с защищенностью	а) Уровень полноты реализации требований и функций по мониторингу текущего состояния - определяют экспертным методом или по формуле: X = A / B, где A - количество параметров, определяющих внутреннее состояние ПС, для которых реализована функция мониторинга; B - общее количество параметров, определяющих внутреннее состояние ПО, для которых должна быть реализована функция мониторинга; 0<=X<=1, чем ближе к «1», тем лучше; б) Уровень полноты реализации требований и функций к удостоверению доступа: X = A/B, где A - количество типов действий, для которых реализована функция удостоверения доступа; B - общее количество типов действий, для которых должна быть реализована функция удостоверения доступа; 0<=X<=1, чем ближе к «1», тем лучше.
2.4	Степень реализации требований к обеспечению учета действий по доступу к системе, данным (Accountability) Оценка степени реализации требований и функций по обеспечению прослеживаемости действий по контролю и регистрации доступа к системе, данным.	а) Уровень полноты реализации требований и функций по аудиту выполняемых действий - определяют экспертным методом или по формуле: X = A/B, где A - количество типов действий, для которых реализована функция аудита; B - общее количество типов действий, для которых должна быть реализована функция аудита; 0<=X<=1, чем ближе к «1», тем лучше; б) Способность учета доступа к системе, данным: X = A / B, где A - количество типов действий, для которых реализована функция учета доступа к системе, данным; B - общее количество типов действий, для которых должна быть реализована функция учета доступа к системе, данным; 0<=X<=1, чем ближе к «1», тем лучше.
2.5	Степень реализации требований к обеспечению подлинности объекта или ресурса (Authenticity) Оценка степени реализации требований и функций по обеспечению тождественности и подлинности объектов, ресурсов, процессов перед предоставлением доступа к данным.	а) Уровень полноты реализации требований и функций по проверке подлинности объектов, ресурсов, процессов перед предоставлением доступа к данным X = A / B; A - число реализованных механизмов проверки подлинности объектов; B - число реализованных механизмов проверки подлинности объектов, требуемых по спецификации; 0<=X<=1, чем ближе к «1», тем лучше.

На основе предложенных метрик можно с применением экспериментальных, расчетных или экспертных методов получить количественные оценки атрибутов защищенности.

Для оценки интегрального показателя уровня защищенности ПСКН может быть использован линейный функционал, составляющими которого являются нормированные значения атрибутов и метрик с соответствующими весовыми коэффициентами. Выбор величин весовых коэффициентов зависит от особенностей конкретной ПСКН и условий его применения. Интегральную количественную оценку уровня защищённости ПСКН следует вычислять с учетом категории его критичности и конкретных условий применения.

При использовании метрик защищенности ПСКН, приведенных в таблицах 2 и 3, необходимо обеспечить объективность и воспроизводимость измерений. Результаты же оценивания показателей защищенности должны обладать точностью и определенностью, которые достаточны для сравнения с требованиями технических заданий и спецификаций.

4. Выводы

Защищенность является одной из важных характеристик качества ПСКН, в то же время она является неопределенной, трудно формализуемой и оцениваемой характеристикой.

На основе анализа особенностей и требований к ПСКН идентифицированы основные объекты и факторы, влияющие на его защищенность, а также критерии их оценки. Определены базовые атрибуты и предложен комплекс метрик защищенности ПСКН, на основе которых предлагается вычислять количественные оценки атрибутов и далее через них вычислять интегральную количественную оценку уровня защищенности ПСКН.

Предложенные метрики могут быть измеряемы расчетными, экспериментальными или экспертными методами.

Для оценки интегрального показателя уровня безопасности ПСКН может быть использован линейный функционал, составляющими которого являются нормированные значения атрибутов и метрик с соответствующими весовыми коэффициентами. Выбор величин весовых коэффициентов зависит от особенностей конкретной ПСКН и условий его применения.

Полученные результаты создают предпосылки для формализации задачи количественной оценки уровня безопасности ПСКН.

Литература

1. ISO/IEC 25010:2011 Systems and software engineering. Systems and software Quality Requirements and Evaluation (SQuaRE). System and software quality models.- (http://www.iso.org/iso/home/search.htm?qt=ISO%2FIEC+25010%3A2011+&sort=rel&type=simple&published=on)

2. ISO/IEC 9126-1:2001. Software engineering – Software product quality – Part 1: Quality model. – 2001. – 32 p.

3. Жоголев Е.А. Технология программирования. – М., Научный Мир, 2004. - 216 с.

4. Полаженко С., Вариант определения понятий защищённости и безопасности программных продуктов.- (https://software-testing.ru/library/testing/security/87-defining-security)

5. ГОСТ 28806-90 Качество программных средств. Термины и определения. - М.: Стандартинформ, 2005.- 23 с.

ЛЕГКОВЕСНЫЕ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Капалова Н.А., Хаумен А., Сулейменов О.Т.
e-mail: kapalova@ipic.kz, haumen.armanbek@gmail.com, suleimenov97@gmail.com
Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *В работе рассматриваются основные направления легковесной криптографии и современные требования к алгориттом, осуществляющие шифрования на ее основе. Приводятся характеристики реализации наиболее известных блочных шифров, а также обзор проводимых исследований по разработке СКЗИ и созданию легковесного алгоритма шифрования.*

Введение

Основные направления развития криптографии во многом связаны с развитием средств связи, информационных технологий и вычислительной техники. Именно прогресс в этих областях сделал возможным повсеместное использование компактных устройств с малой вычислительной мощностью, имеющих доступ к сети Интернет и реализующих концепцию «Интернета вещей». Интернет вещей представляет собой беспроводную самоконфигурирующуюся сеть между объектами типа бытовых приборов, транспортных средств, различных сенсоров и датчиков, а также меток радиочастотной идентификации (Radio Frequency IDentification - RFID). Жёсткие ограничения на внутренние вычислительные ресурсы таких устройств делают затруднительным или невозможным использование классических криптографических алгоритмов. Это привело к возникновению нового раздела криптографии - **«легковесной» криптографии (lightweight cryptography)**, задачей которой является создание стойких криптографических алгоритмов и протоколов с приемлемой стойкостью в условиях ограниченных ресурсов [1-2].

Наряду с эффективной реализацией известных алгоритмов блочного шифрования актуальными является разработки по созданию новых блочных шифров, ориентированных на оптимальную реализацию на микропрограммном или аппаратном уровне для специализированного применения.

Большая часть научно-исследовательских работ по разработке легковесных криптоалгоритмов была проведена в области алгоритмов блочного шифрования. За последнее время было предложено множество легковесных решений. Значительный вклад в развитие направлений по созданию легковесных (малоресурсных) симметричных алгоритмов шифрования внесен такими учёными, как Д. Бернштайн, К. Паар, А. Богданов, А. Пошман и др. [3, 4].

В Республике Казахстан для защиты информации применяются в основном зарубежные аппаратно-программные средства, которые являются прозрачными для их разработчиков. Поэтому разработка отечественных средств криптографической защиты информации, в том числе отечественных легковесных алгоритмов шифрования на основе ранее разработанных алгоритмов шифрования, безусловно актуальна.

В лаборатории информационной безопасности (ЛИБ) Института информационных и вычислительных технологий (ИИВТ) КН МОН РК проводятся научно-исследовательские работы (НИР) по разработке и анализу новых систем шифрования, электронной цифровой подписи (ЭЦП), генерации криптографических ключей и аутентификации, а также созданию на их основе программных средств криптографической защиты информации (СКЗИ). В ЛИБ также проводятся НИР по криптоанализу разработанных и существующих алгоритмов шифрования и криптографическим атакам, основанным на статистических уязвимостях выходной последовательности.

В данной статье излагаются подходы построения легковесных шифров и планы работ по разработке отечественной легковесной системы криптографической защиты информации на основе ранее разработанных в ЛИБ алгоритмов шифрования.

Подходы к построению «легковесной» криптографии

Стандартными подходами к решению проблемы создания эффективных методов и средств «легковесной» криптографии являются [5]:

- использование классических криптографических алгоритмов, если это возможно;
- модификация классических алгоритмов с адаптацией к аппаратным особенностям и ограничениям систем с низкой стоимостью;
- разработка новых специализированных решений в методологическом, алгоритмическом и программно-аппаратном плане.

Каждый из этих подходов имеет свои недостатки. До сих пор большинство решений в этой области знаний относится к третьему подходу, и показывают неплохие результаты. При этой адаптации криптографического алгоритма к особенностям аппаратного базиса в условиях ограниченности ресурсов могут появиться дополнительные слабости алгоритма или ослабление общей стойкости.

К основным подходам, позволяющие криптографам создать нетребовательные к ресурсам и при этом относительно стойкие алгоритмы шифрования относятся:

- уменьшение размеров основных параметров алгоритма: блока шифруемых данных, ключа шифрования и внутреннего состояния алгоритма;
- попытки компенсации вынужденной потери стойкости алгоритмов за счет проектирования на основе хорошо изученных, широко применяемых операций, осуществляющих элементарные линейные/нелинейные преобразования. Такие операции можно представить как детали некоего конструктора, из которых криптографы «собирают» алгоритм, обладающий нужными качествами;
- уменьшение размеров данных, используемых в конкретных операциях. Например, в алгоритмах шифрования часто применяются таблицы замен; чтобы хранить таблицу, заменяющую 8-битовые фрагменты данных, необходимо 256 байт, но такую таблицу можно составить из комбинации двух 4-битовых таблиц, требующих всего 32 байта в сумме;
- использование «дешевых» с точки зрения ресурсоемкости, но эффективных преобразований, таких как управляемые битовые перестановки, сдвиговые регистры и пр.;
- применение преобразований, в отношении которых возможны варианты реализации в зависимости от ресурсов конкретного шифратора.

В Национальном институте стандартов и технологий (NIST) США публично и на конкурентной основе проводится отбор одной или нескольких аутентифицированных схем шифрования и хеширования, подходящих для использования в ограниченных средах. NIST после проведения первых двух этапов в июле 2020 г. объявил о старте третьего этапа [6].

Отметим, что основные ограничения вычислительных ресурсов выражаются в:

- для аппаратной реализации – размере микросхемы, потребляемой энергии;
- для программной реализации – размерах программного кода и оперативной памяти.

Для обоих видов реализации также важным является время, затраченное на исполнение процедуры шифрования-расшифрования. Структурные решения в классе малоресурсных шифров часто являются результатом компромисса между эффективностью реализации, производительностью и криптографической стойкостью.

Согласно стандарту ISO/IEC 29192-1[7] малоресурсная криптография классифицируется на основании таких характеристик, как ограничения на размер чипа, энергопотребление при аппаратной реализации, размера программного кода и размера ОЗУ при программной

реализации, полосы пропускания связи, время выполнения. Для симметричных блочных шифров данный стандарт определяет два основных алгоритма шифрования: PRESENT – длина блока 64 бит и длина ключа 80 или 128 бит [3]; CLEFIA: длина блока 128 бит и длина ключа 128, 192, или 256 бит [8]. В 2014 году было предложено дополнение к данному стандарту с добавлением алгоритмов SIMON и SPECK, имеющих несколько комбинаций размеров блока данных и ключей [9].

Учитывая особенности реализации и применения малоресурсных шифров, в данном классе криптографических средств нет одного оптимального решения, подходящего для использования в различных приложениях и встроенных системах. Это связано в первую очередь с тем, что при реализации таких криптографических алгоритмов необходимо принимать во внимание свойства целевой системы и условия, в которых алгоритм будет функционировать.

Требования, предъявляемые к легковесным алгоритмам шифрования, закреплены в международном стандарте ISO/IECFDIS 29192-2:2019 Информационная безопасность – легковесная криптография [10]. Этот документ определяет три легковесных блочных шифра: PRESENT, CLEFIA, LEA. Как нам известно, все чаще проводятся успешные атаки на фаворитов среди имеющихся алгоритмов легковесной криптографии. Всё это делает применение легковесных алгоритмов на практике довольно узкоспециализированной и сложной задачей.

Технические требования к создаваемому легковестному алгоритму должны соответствовать типичным ограничениям для программной реализации на размеры программного кода и оперативной памяти, а также на время исполнения программы. Могут появляться и другие ограничения. Каждый разработчик (проектировщик) в области легковесной криптографии должен стремиться найти баланс между безопасностью, ценой и производительностью. Обычно проще оптимизировать любые две из трёх целей разработки – безопасность и стоимость, безопасность и производительность, или стоимость и производительность; однако, довольно сложно оптимизировать эти три параметра одновременно[1]. А эффективность реализации того или иного преобразования на программном или аппаратном уровне оценивается по-разному. Для сравнения программных реализаций принято рассматривать требования к размерам программного кода и оперативной памяти, а также времени, затраченного на исполнение программы(Таблица 1).

Таблица 1.Программная реализация наиболее известных блочных шифров

Алгоритм	**Nb длина блока (в битах)**	**Nk длина блока (в битах)**	**R число раундов**	**Размер кода в байтах ROM**	**SRAM в байтах RAM**	**Encrypt (cycle/byte)**	**Decrypt (cycle/byte)**
AES-128	128	128	10	2606 1912	224 432	415 125	464 181
IDEA	64	128	8.5	596	0	338	1924
DES	64	56	16	4314	0	1079	1019

PRESENT	64	80	31	936	0	1340	1405
PRINT	48	80			490	10415	10575

Технические требования создаваемого малоресурсного алгоритма при программной реализации:

- длина информационного блока (в битах): $Nb \geq 128$;
- длина ключа (в битах): $Nk \geq 128$;
- число раундов: $R \geq 10$;
- размер кода (в байтах): $ROM \leq 1500$;
- SRAM (в байтах): $RAM \leq 200$;
- Шифрование (cycle/byte): ≤ 400;
- Дешифрование (cycle/byte): ≤ 400.

Разработка легковесного алгоритма шифрования на основе ранее разработанных алгоритмов шифрования

Разработанный алгоритм будет осуществовлять оптимальный баланс между временем, затрачиваемым на процесс шифрования, потребляемой энергией и оперативной памятью. Планируется осуществление программной реализации разработанного легковесного шифра и проведение анализа и оценки его надежности, а также подготовка рекомендаций и расчетов для аппаратной реализации.

Для достижения поставленной цели определены следующие основные задачи:

- исследование современных тенденций развития легковесных систем криптографической защиты информации;
- разработка и исследование легковесного алгоритм шифрования для вышеуказынных систем защиты информации;
- исследование и оценка надежности разработанного легковесного алгоритма шифрования методами криптоанализа;
- программная реализация разработанного легковесного алгоритма шифрования.

Проводимы НИР являются продолжением работ, проведенных в 2018-2020 годах в рамках проекта программно-целевого финансирования (ПЦФ) «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» (научный руководитель – д.т.н., ассоциир. проф. С.Е.Нысанбаева, ответственный исполнитель – к.т.н. Н.А.Капалова).

Научный задел ЛИБ ИИВТ и результаты этой программы будут использованы для разработки легковесной системы криптографической защиты информации с целью их применения на практике.

В этом проекте ПЦФ проведены НИР по разработке, анализу, программной и программно-аппаратной реализации симметричных блочных алгоритмов шифрования с использованием разных подходов, и в том числе непозиционных полиномиальных систем счисления. Основными результатамиэтих НИРявляется создание новых СКЗИ, таких систем, как Qamal, BC-2, AL01 и другие [11].

Алгоритм шифрования Qamal. При его разработке применены обратимые преобразования открытого текста для трех длин блоков файлов и ключей в 128, 192 и 256 бит. Ключам длиной в 128, 192 и 256 бит соответствуют число раундов шифрования 6, 8, 10.

Процесс зашифрования состоит из разработанных процедур наложения ключас помощью операции побитового сложения, блока замены и процедур перемешивания. В процессе расшифрования те же самые криптографические преобразования инвертируются и применяются в обратном порядке. Проведен криптографический анализ алгоритма «Qamal» атакой методом бумеранга [12].

Алгоритм шифрования BC-2. В нем длина блока составляет 256 бит. Для шифрования используется ключ длиной 512 бит. Получение зашифрованного файла реализуется за 10 раундов. Зашифрование производится путем последовательного выполнения четырех криптографических преобразований, а расшифрование – в последовательном, но строго обратном их выполнении. Проведено исследование на надежность с использованием методов криптоанализа. Изучены дифференциальные свойства S-блока подстановок данного алгоритма. Полученные результаты показали, что разработанный S-блок является стойким к дифференциальному криптанализу.

Эти разботанные системы симметричного блочного шифрования программно реализованы. На компьютерных программах исследованы свойства этих двух предложенных криптоалгоритмов [13].

Создана система симметричного блочного шифрования «AL01», число раундов в которой равно 4. Длина блока шифрования равна длине базового ключа K и составляет 16 байт. На основе базового ключа К с использованием алгоритма генерации псевдослучайных последовательностей ПСП_1 формируются промежуточные 16-байтовые ключи K_1, K_2, K_3 и K_4. Далее с использованием разработанных алгоритмов генерации ключей (или псевдослучайных последовательностей) ПСП_2 и ПСП_3 с помощью промежуточных ключей K_i (i=1,2,3,4) определяются раундовые ключи R_i и Q_i длиной 256 и 16 байт соответственно. Предложена модель программной реализации для разработанной системы симметричного блочного шифрования «AL01» [14].

Модель алгоритма легковесного шифрованиябудет разработана на основе приведенных выше разработанных алгоритмов шифрования и отвечать техническим требованиям создаваемого малоресурсного алгоритма при программной реализации. Поскольку «легковесные» алгоритмы разрабатываются под конкретные требования, то из них напрямую следуют все преимущества и недостатки данного семейства алгоритмов. При этом главным преимуществом является крайне низкие требования как к ресурсам, так и к энергопотреблению, что делает «легковесные» алгоритмы крайне быстрыми в работе и «неприхотливыми» к среде, в которой будет осуществляется их работа. Кроме того, это делает «легковесные» алгоритмы крайне дешевыми во внедрении и использовании.

Следует отметить, что легковесные алгоритмы шифрования создаются либо для систем с низким или средним уровнем безопасности, либо для систем, где будет учтена специфика используемых алгоритмов и будет найдено решение, позволяющее сделать реализацию алгоритма максимально безопасной для его уровня стойкости.

Заключение

Дальнейшая работа заключается в разработке надежного отечественного легковесного алгоритма шифрования на основе ранее разработанных в ЛИБ алгоритмов шифрования, который будет осуществовлять оптимальный баланс между временем, затрачиваемым на процесс шифрования, потребляемой энергией и оперативной памятью. Этот легковесный шифр будет программно реализован для анализа и оценки его надежности, и будет также подготовлены рекомендации и расчеты для аппаратной реализации.

Благодарность

Научно-исследовательская работа выполнена в рамках проекта AP09259570 «Разработка и исследование отечественного легковесного алгоритма шифрования при ограниченности ресурсов»в Институте информационных и вычислительных технологий КН МОН РК.

Литература

1. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. 2015. № 1.- С. 26–43.

2. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. 2015. № 2. - С. 2–10.

3. Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J. B., Seurin Y., Vikkelsoe C. PRESENT: An Ultra-Lightweight Block Cipher. in CHES. – Springer-Verlag, 2007. – P. 450–466.

4. Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J. & Biryukov, A. Design Strategies for ARX with Provable Bounds: SPARX and LAX. - In Advances in Cryptology–ASIACRYPT 2016. – Springer Berlin Heidelberg, 2016. – P. 484-513.

5. «Облегчённые» шифры – CryptoWiki [Электронный ресурс]. URL: https: //cryptowiki.net/index.php?title.

6. NIST. Lightweight Cryptography [Электронный ресурс]. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

7. ISO/IEC 29192-1:2012: Information technology – Security techniques – Lightweight cryptography.

8. Shirai T., Shibutani K., Akishita T., Moriai S., Iwata T. The 128-Bit Blockcipher CLEFIA (Extended Abstract). - In: Biryukov A. (eds) Fast Software Encryption. FSE 2007. -Lecture Notes in Computer Science, vol 4593. - Springer, Berlin, Heidelberg.

9. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers. Simon and Speck: Block Ciphers for the Internet of Things // NIST Lightweight Cryptography Workshop (9 July 2015).

10. Международный стандарт «Lightweight cryptography» – ISO/IEC 29192-2:2019.//https://standards.iteh.ai/catalog/standards/iso/5f0d0670-2efa-43fa-96a4-aa83042e0b11/iso-iec-29192-2-2019.

11. Отчет о научно-исследовательской работе по проекту программно-целевого финансирования «Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения». - 2018 г. - № гос. регистрации 0118РК01064.

12. Бияшев Р.Г., Смоларш А., Алгазы К.Т., Хомпыш А. Алгоритм шифрования "QAMAL NPNS" с использованием непозиционной полиномиальной системы счисления. Journal of Mathematics, Mechanics and Computer Science, «Вестник» КазНУ, № 1 (105). // Алматы, 2020 г. –С. 198-207.

13. Капалова Н.А., Хаумен А. Симметричный блочный алгоритм шифрования данных «ВС-2» // «Безопасные информационные технологии». Сборник трудов Десятой международной науч-но-технической конференции – М.: МГТУ им. Н.Э. Баумана, 2019. - С. 161-166.

14. 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». -Ч.2. – Алматы, 2019. – С. 602-607.

К ВОПРОСУ О СОСТОЯНИИ И ПЕРСПЕКТИВАХ РАЗВИТИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Метелев В.Н., Кожахметов К.Б.
e-mail: svo5858@mai.ru
Национальный университет обороны имени Первого Президента Республики Казахстан-Елбасы

Аннотация. *Перечислены криптографические методы преобразования информации, методы шифрования информации в компьютерных сетях. Изложены недостатки криптографических алгоритмов шифрования с открытым и закрытым ключом. Перспективы развития современной криптографии. Рассмотрены вопросы подготовки специалистов по информационной безопасности в органах управления Вооруженных Сил. Оценена возможность разработки в республике программно-технических продуктов и средств криптографической защиты информации. Предложены варианты решения проблем в этой сфере деятельности, используя опыт зарубежных государств и государственно-частного партнерства. Дан взгляд на состояние законодательной базы в области криптографии в республике, странах ближнего зарубежья и Китае. Отражена позиция Министерства обороны и Комитета национальной безопасности в отношении изменения законодательства в области криптографии и переработки государственного стандарта СТ РК 1073-2007.*

Современная криптография позволяет решать проблемы, которые ранее считались в принципе неразрешимыми. Многие такие возможности криптографии используются в реальных компьютерных системах. Это и заключение коммерческих сделок в режиме удаленного взаимодействия участников, и осуществление денежных расчетов по сети, и проведение выборов по компьютерным сетям, и многое др.

Рисунок 1 – Криптографическое закрытие информации

Криптографические алгоритмы не просто предоставляют новые возможности пользователю - можно произвести все необходимые операции со своего домашнего

компьютера. Важно то, что они способны обеспечивать надежность значительно более высокую, чем традиционные механизмы. Если бумажную банкноту можно подделать, и случаи подделок весьма многочисленны, то электронную банкноту, созданную при помощи криптографических методов, подделать практически невозможно.

Открытие 2-х-ключевой (асимметричной) системы (метода) шифрования американскими исследователями Диффи и Хеллмана в середине 1970-х годов явилось блестящим достижением многовекового эволюционного развития криптографии.

Так началось и продолжается до настоящего времени бурное развитие наряду с обычной классической криптографией и криптографии с открытым ключом. Метод шифрования с открытым и закрытым ключом привел к резкому росту числа открытых исследований в области криптографии и показал новые пути её развития, новые возможности и уникальное значение методов криптографии в современных условиях массового применения электронных информационных технологий.

Алгоритм RSA стал мировым стандартом для открытых систем. Алгоритмы криптосистемы с открытым ключом (СОК) используются и как самостоятельные средства защиты передаваемых и хранимых данных, и как средства для распределения ключей.

Алгоритмы СОК более трудоемки, чем традиционные криптосистемы. Поэтому часто на практике рационально с помощью СОК распределять ключи, объем которых как информации незначителен. А потом с помощью обычных алгоритмов осуществлять обмен большими информационными потоками.

Защита информации при передаче ее по каналам связи осуществляется средствами криптографической защиты: шифрованием, кодированием, стеганографией, сжатием и др.

Характерной особенностью этих средств является то, что они потенциально обеспечивают наивысшую защиту передаваемой информации от несанкционированного доступа и от модификации (использование цифровой подписи и имитовставки).

Рисунок 2 - ЭЦП с использованием симметричных криптосистем

В то же время применение средств криптографической защиты информации влечет ряд неудобств: стойкость этих средств является потенциальной, т.е. гарантируется при соблюдении ряда дополнительных требований. Реализация их на практике осуществляется

довольно сложно (создание и функционирование ключевой системы, распределение ключей, обеспечение сохранности ключей, необходимость в получении лицензии от государственного уполномоченного органа (КНБ) на право эксплуатации средств криптографической защиты информации (СКЗИ), планирование и организация мероприятий при компрометации ключевой системы); относительно высокая стоимость эксплуатация таких средств и др.

Решение проблем защиты электронной информации может быть получено только на базе использования перечисленных выше криптографических методов, которые позволяют решать важнейшие проблемы защищённой автоматизированной обработки и передачи данных. Современные скоростные методы криптографического преобразования информации позволяют сохранить исходную производительность автоматизированных систем, являются наиболее эффективным средством обеспечения конфиденциальности данных, их целостности и подлинности. Только их использование в совокупности с необходимыми техническими и организационными мероприятиями могут обеспечить защиту от широкого спектра потенциальных угроз.

Возрастание роли программных и криптографических средств зашиты проявляется в том, что возникающие новые проблемы в области защиты вычислительных систем от несанкционированного доступа требуют использования механизмов и протоколов со сравнительно высокой вычислительной сложностью и могут быть эффективно решены путём использования ресурсов мощных ЭВМ.

С другой стороны, в развитых странах наблюдается широкий спектр мнений в подходах к вопросу о регламентации использования алгоритмов шифрования. Высказываются предложения от полного запрета широкого применения криптографических методов до полной свободы их использования. Некоторые предложения относятся к разрешению использования только ослабленных алгоритмов или к установлению порядка обязательной регистрации ключей шифрования. Чрезвычайно трудно найти оптимальное решение этой проблемы.

Возможность широкого использования глобальных информационных сетей и криптографии является достижением и признаком демократического общества. Вместе с тем, надо понимать, что когда речь идет о защите информации в компьютерных сетях, содержащей сведения, относимые к государственным секретам, секретным (недоступным другим пользователям) должен быть не только ключ, но и сам алгоритм шифрования.

По мнению российских специалистов, владение основами криптографии в информационном обществе объективно не может быть привилегией отдельных государственных служб, а является насущной необходимостью для самих широких слоёв научно-технических работников, применяющих компьютерную обработку данных или разрабатывающих информационные системы, сотрудников служб безопасности и руководящего состава организаций и предприятий.

В то же время государственные органы, руководители которых наделены полномочиями по отнесению сведений к государственным секретам, должны обладать такими программно-аппаратными способами защиты информации, которые с гарантированной стойкостью обеспечивали бы безопасность передаваемой в информационных сетях секретной или служебной информации.

Рисунок 3 – Подразделение кибербразведки КНР

Не секрет, что разведывательные службы или другие инсайдеры (хакеры, злоумышленники), охотятся за такой информацией: первые – в интересах своих государств, вторые – в корыстных целях (информацию, в конце концов, можно выгодно продать под любым предлогом, включая шантаж).

Как считают зарубежные специалисты, отдельно взятая организация не может обеспечить достаточно полный и эффективный контроль за информационными потоками в пределах всего государства и обеспечить надлежащую защиту национального информационного ресурса. Однако, отдельные государственные органы могут создать условия для формирования рынка качественных средств защиты, подготовки достаточного количества специалистов и овладения основами криптографии и защиты информации со стороны массовых пользователей.

На рынке информационных технологий достаточно много предложений по закупу надежных средств криптографической защиты информации, включая аппаратные и программно-аппаратные средства. Для повышения криптостойкости шифров могут использоваться, к примеру, несколько ключей. Зашифрованная с помощью первого ключа информация подвергается шифрованию с помощью второго ключа и т. д. Предлагается также использовать переменные алгоритмы шифрования.

В этом случае ключ шифрования используется еще и для выбора конкретного алгоритма шифрования. Развитие этого направления шифрования сдерживает сложность строгого доказательства криптостойкости такого шифрования.

Привлекательность методов шифрования с использованием открытых ключей заключается, прежде всего, в отсутствии необходимости рассылки секретных ключей. Для распределенных на больших расстояниях объектов (пользователей) компьютерной сети рассылка секретных ключей становится довольно сложной и трудоемкой задачей. Распространение систем с открытыми ключами сдерживается отсутствием доказательств невозможности получения секретных ключей, кроме как путем их полного перебора [1-3].

Несмотря на то, что существующие криптографические алгоритмы способны обеспечить достаточно высокий уровень безопасности, чтобы защитить данные от любого противника на сотни лет, новые шифры продолжают появляться.

Иногда новые алгоритмы должны работать в специальных условиях (мало памяти, ограниченный набор команд), иногда требуется увеличить производительность без снижения стойкости. Работы по созданию новых симметричных шифров ведутся постоянно, но значительного изменения состава широко применяемых **с**имметричных криптографических алгоритмов, наверное, уже не произойдет. Все-таки симметричные шифры — одна из самых древних и хорошо изученных областей криптографии.

В криптографии с открытым ключом до сих пор много чего не сделано. Хорошо проверенные методы, такие как RSA, требуют выполнения значительных объемов вычислений и оперируют блоками большого размера. И с увеличением минимальной рекомендованной длины ключа вследствие прогресса вычислительной техники и методов взлома накладные расходы растут очень быстро. Так что поиск более технологичных решений, способных обеспечить высокий уровень безопасности, может, в конце концов, привести к появлению принципиально новых алгоритмов.

Это связано с оценкой требуемого уровня безопасности. Размеры ключей в симметричном шифровании остаются неизменными (128, 256 бит) всю жизнь системы, тогда как размеры открытого ключа всегда представляют собой переменную величину. Из-за очевидных проблем производительности, из-за того что в алгоритме Диффи-Хеллмана шифрование происходит значительно большим числом операций, требования к открытым ключам отличаются. Он остается действительным на протяжении одного года и защищает данные следующие 20 лет, т.е. в общей сложности используется 21 год. Ввиду его переменного размера ключ каждый год может изменяться и создаваться все более длинным, чтобы обеспечить требуемый уровень безопасности.

Таблица 1 - Показатели лучших оценок защиты данных

Ключ, длина	**Защита данных**
байт	**лет**
256	20
384	35
512	47

Число 6800 бит, гарантирующее, что злоумышленнику потребуется 2128 шагов для его взлома, получено из подобных оценок (Таблица 1). Можно достаточно точно предсказать развитие событий на 10 лет вперед, но на 50 – вряд-ли. Применение алгоритма Диффи-Хеллмана должно быть методичным и аккуратным ввиду наличия очевидных проблем и серьезных подводных камней.

Перспективным направлением развития криптозащиты информации является стеганография. Комплексное использование стеганографии и шифрования намного повышает криптостойкость закрытой информации.

Рисунок 4 - Обобщенная модель стегосистемы

В наше время встраивание скрытой информации, находятся в центре внимания многих исследователей и инженеров. Ежегодно проводятся многочисленные конференции по защите информации, где многие доклады посвящены стеганографии и стегоанализу, издаются

международные научные журналы, печатающие статьи о методах скрытой передачи информации и их применении. Стеганография — это искусство отправки скрытых или невидимых сообщений. Современная стеганография, как правило, имеет дело с информацией в электронной форме.

Размер информации весьма мал по сравнению с размером данных, в которых она должна быть скрыта (текстовый контейнер). Само извлечение может быть автоматизировано, когда данные в электронной форме, так как компьютеры могут эффективно обрабатывать их и выполнить алгоритмы, необходимые для получения сообщения. Электронные данные также часто включают в себя избыточные, ненужные и незаметные пространства данных, которые можно использовать, чтобы скрыть сообщения. Пустые пространства обеспечивают своего рода «скрытый отсек», в который могут быть вставлены секретные сообщения и отправлены принимающей стороне.

Стеганографическая информация может быть скрыта почти везде, и некоторые объекты контейнера больше подходят для скрытия информации, чем другие. Стеганография в изображениях стала более популярной в последние годы, чем другие виды стеганографии, возможно из-за большого потока изображений в электронном виде, доступного с появлением цифровых камер и высокоскоростной интернет-передачи.

Стеганография в изображении часто включает в себя скрытие информации в естественно возникающих «шумах» изображения и предоставляет хорошие наглядные примеры для таких методов.

Скрываемые сообщения теперь встраиваются в цифровые данные (изображения, видео и аудиофайлы). Также существуют методы по внедрению данных в текстовые файлы и даже в исполняемые файлы программ.

Стеганография – один из самых увлекательных и эффективных методов сокрытия данных, которые использовались за всю историю человечества. Развитие вычислительной техники в последнее время дало новый толчок в развитии компьютерной стеганографии. Исследуются новые области применения.

Главной причиной сдерживания этого процесса является лавинообразное развитие компьютерной сети общего пользования Internet, в т.ч такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов, принятые в ряде стран ограничения на использование сильной криптографии.

Существуют и другие проблемы, связанные с криптографией, как науки, к примеру, ограниченность рабочих схем с открытым ключом; увеличение размера шифруемых блоков данных и ключей к ним; ненадежность фундамента шифрования и др.

Современная криптография полностью основана на математике. Основная задача, которую преследует математика в криптографии — это криптографическая стойкость, т. е. способность противостоять теоретическому и практическому взлому ключа (шифра).

В самых распространённых криптографических системах сети Интернет (RSA, ElGamal, Shamir и др.) используются последние достижения теории чисел и алгебры. Взломать их — значит решить сложные математические задачи.

Некоторые проблемы имеющихся методов криптографии может решить, так называемая, квантовая криптография. Квантовая криптография — это сравнительно новое направление исследований, позволяющее применять эффекты квантовой физики для создания секретных каналов передачи данных. В квантовой криптографии используется фундаментальная особенность квантовых систем, заключающаяся в принципиальной невозможности точного детектирования состояния такой системы, принимающей одно из набора нескольких не ортогональных состояний

Технология квантового распределения криптографических ключей решает одну из основных задач криптографии — гарантированное на уровне фундаментальных законов природы распределение ключей между удаленными пользователями по открытым каналам связи.

Родившись около 30 лет назад на стыке квантовой механики и традиционной криптографии, квантовая криптография достигла наибольших результатов в плоскости практических приложений, имеющих непосредственное отношение к вопросам обеспечения информационной безопасности. Возможно, через десятилетие уже появятся новые виды вычислительной техники, а именно квантовые компьютеры. Классические методы криптографической защиты в таком случае станут уязвимы,

В основе метода квантовой криптографии лежит наблюдение квантовых состояний фотонов. Отправитель задает эти состояния, а получатель их регистрирует. Здесь используется квантовый принцип неопределенности Гейзенберга, когда две квантовые величины не могут быть измерены одновременно с требуемой точностью. Таким образом, если отправитель и получатель не договорились между собой, какой вид поляризации квантов брать за основу, получатель может разрушить посланный отправителем сигнал, не получив никакой полезной информации. Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа.

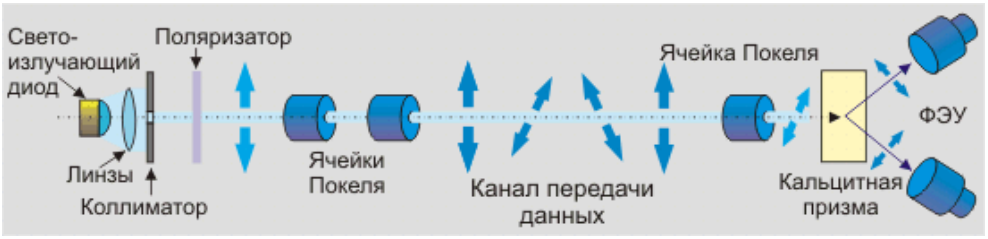


Рисунок 5 – Схема практической реализации квантовой криптографии

В настоящее время уже несколько фирм предлагают первые коммерческие системы квантовой криптографии. Но на пути практической реализации систем квантовой коммуникации возникает ряд технических трудностей. Очевидно, что квантовые системы еще не скоро войдут в массовое пользование, однако уже сейчас они могут найти свое применение для защиты особо важных каналов связи.

Ученые намерены продолжать испытания квантового компьютера и, возможно, попытаются запустить на нем квантовый алгоритм, позволяющий взламывать большинство существующих систем шифрования (в т.ч. считающийся самым стойким криптографический алгоритм RSA). Кубит - квантовый разряд или наименьший элемент для хранения информации в квантовом компьютере. Квантовый компьютер — вычислительное устройство, которое использует явления квантовой суперпозиции и квантовой запутанности для передачи и обработки данных [5].

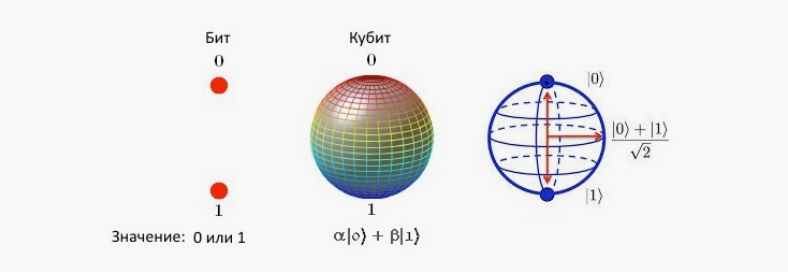


Рисунок 6 - Хранение информации в квантовом компьютере

Самая ценная информация — это шифровальные ключи. Если ключ имеет длину, равную самому сообщению или еще длиннее, то расшифровать послание, не зная ключа, в принципе невозможно. Остается организовать защищенную передачу ключей, а это как раз и обеспечивают квантовые линии связи.

Однако пока дистанция передачи данных для таких линий слишком коротка: из-за тепловых шумов, потерь, дефектов в оптоволокне фотоны не «выживают» на больших расстояниях.

По мнению российских исследователей, максимальная длина канала связи, позволяющего использовать метод квантовой криптографии, составляет всего лишь чуть больше сотни километров, а устойчивая работа на нормальных, не рекордных линиях вообще ограничивается 40 км.

Но ученые-физики продолжают исследования и, по мнению, российских экспертов, при благоприятных условиях первый прототип квантового повторителя может быть создан примерно через пять лет. А появление его на рынке может открыть дорогу действительно массовому применению квантовой криптографии, что серьезно изменит жизнь не только военных или банкиров [6].

Возможный подход к решению проблемы исследований в области квантовой физики - практикующееся во всем мире государственно-частное партнёрство в сфере противодействия киберпреступности. Необходимо сотрудничество в этой сфере на позициях лояльности и открытости с казахстанскими государственными органами и организациями, представителями ведущих ВУЗов республики, неформальное участие в различных мероприятиях, направленных на развитие кибербезопасности республики.

Проведение теоретических и экспериментальных исследований методов квантовой криптографии позволит в будущем реализовать абсолютно скрытую передачу данных в телекоммуникационных системах государства.

Если ученым удастся реализовать на практике идею квантового шифрования данных, информация, циркулирующая в компьютерных сетях, будет защищена с гарантированной стойкостью в не зависимости от того, интегрирована или нет компьютерная сеть в глобальную вычислительную сеть Интернет.

Исследования в этой области, несомненно, послужат мощным средством обеспечения информационной безопасности республики. Сдерживающим фактором, по мнению казахстанских специалистов, является то, что в Республике Казахстан нет соответствующих экспериментальных линий связи, научно-исследовательских центров физики и оборудования.

Учитывая некоторую общность в решении ключевых проблем информационной безопасности государств-участников Содружества Независимых Государств (СНГ), полагается целесообразным исследования в области квантовой криптографии проводить в сотрудничестве, к примеру, с российскими, белорусскими и украинскими коллегами.

Отличной платформой для исследований в этом перспективном разделе криптографии послужит возможность обучения в системе послевузовского образования казахстанских военнослужащих с соответствующим профильным образованием в военных ВУЗах Российской Федерации, республиках Беларусь и Украина.

Рисунок 7 - Меры информационной безопасности

Одно из основных направлений обеспечения информационной безопасности в Вооруженных силах, других войсках и воинских формированиях Казахстана - совершенствование существующих приемов и способов обеспечения информационной безопасности, включая и развитие криптографических методов защиты информации, и, конечно же, - подготовка специалистов по информационной безопасности, в т.ч. и в области криптографии.

Кафедрой информационной безопасности факультета цифровых технологий и безопасности информационных систем проанализирована ситуация по подготовке специалистов в области информационной безопасности и криптографии, в частности. Об этом информировалось на предыдущей конференции в Институте информационных и вычислительных технологий в январе 2020 г. Полагается возможным в Вооруженных Силах республики сохранить имеющийся опыт подготовки военных специалистов в том формате, который существует сейчас: кафедра защиты информации Военно-инженерного института радиоэлектроники и связи, кафедра информационной безопасности Национального университета обороны, военные ВУЗы Турции, России и Республики Беларусь, с учетом потребностей войск.

Рассматривается вопрос возможности подготовки/повышения квалификации указанных специалистов также и в гражданских (коммерческих) организациях республики и ВУЗах РФ.

В настоящее время и в дальнейшей перспективе продолжится обучение военнослужащих Вооруженных Сил по программам различных обучающих дисциплин известных компаний мирового уровня, специализирующихся на решении вопросов кибербезопасности, таких как, SAP, Cisco, Juniper, Tpales, Check Point и др.

Министерством обороны организован обмен опытом, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов в области информационной безопасности в рамках региональных (межправительственных)

актов о сотрудничестве, к примеру, - Шанхайская организации сотрудничества; Организация договора о коллективной безопасности и др.

В перспективе на основе имеющихся меморандумов (соглашений) о сотрудничестве в сфере высшего образования Национальный университет обороны может заключить договора с ведущими ВУЗами республики (в г. Нур-Султан) о привлечении их профессорско-преподавательского состава для преподавания дисциплин, связанных с информационной безопасностью и криптографическими методами защиты информации.

В докладе Международного исследования EY в области информационной безопасности отмечается: ключевыми составляющими устойчивости информационных систем к различного вида кибератакам являются такие традиционные средства, как антивирусные программы, системы обнаружения и предотвращения вторжений (IDS и IPS), регулярное обновление программного обеспечения, а также технологии шифрования, обеспечивающие целостность данных даже в том случае, если злоумышленникам удастся получить к ним доступ [7].

Казахстанскими специалистами отмечается, что разработки в области защиты информации напрямую связаны с деятельностью по обеспечению государственных и коммерческих секретов. Использование готового иностранного программного продукта небезопасно. Представляется крайне сложным проведение исследований по обнаружению наличия возможных незадекларированных программных и аппаратных закладок в данных готовых продуктах. Поэтому разработки средств защиты и иных программно-технических продуктов государственной важности должны выполняться в специализированных национальных лабораториях с привлечением отечественных ученых и специалистов.

К сожалению, Министерство обороны не располагает такими лабораториями. Здесь возможно сотрудничество с ведущими отечественными научными организациями и ВУЗами республики. Как отмечается казахстанскими специалистами, необходима организация сотрудничества с ведущими зарубежными вузами в части обучения и обмена опытом. К примеру, можно использовать потенциал ВУЗов и НИИ страны, в частности, потенциал Назарбаев университета, ЕНУ им. Л.Н. Гумилева, КазНУ им. аль-Фараби, КарГУ, КазНИТУ и др. ведущих ВУЗов Казахстана.

Возможное решение этих проблем – использование опыта других государств. Так, в Южной Корее, создан Исследовательский институт электроники и телекоммуникаций (Electronics and Telecommunications Research Institute) и собран квалифицированный штатный состав в единую организацию. Другой пример сильного научного объединения – это научно-исследовательский институт «Техническая защита информации» оперативно-аналитического центра при Президенте Республики Беларусь. Возможно, и в Казахстане создать аналогичный научно-производственный орган, в функции которого будет входить решение стратегической задачи поэтапного импортозамещения в сфере защиты информации. Его возможно создать на базе Международного технопарка ИТ-стартапов, который организуется по поручению Президента на одном из объектов ЕХРО-2017. Государственно-частное предпринимательство, привлечение инвестицийи трансферт технологий в сфере защиты информации – эти задачи были бы основными для такого центра [8].

О законодательстве в сфере криптографии. В Казахстане под термином «Средства криптографической защиты информации» понимаются криптографические средства для защиты сведений, не составляющих государственные секреты.

Рисунок 8 - СКЗИ в государственных органах

В государственных органах Республики Казахстан, в том числе в Министерстве обороны и Комитете национальной безопасности, для обеспечения конфиденциальности информации (сведений ограниченного распространения с пометкой «Для служебного пользования», а также электронных информационных ресурсов, содержащих персональные данные ограниченного доступа, применяются СКЗИ.

Также в указанных государственных органах СКЗИ применяются в качестве средств электронной цифровой подписи для обеспечения юридической значимости электронного документооборота [9, 10].

Как полагают казахстанские исследователи, на сегодняшний день требования к СКЗИ для защиты сведений, не составляющих государственные секреты, устарели и не учитывают актуальных угроз информационной безопасности [11, 12].

Рисунок 9 - Нормативные требования к СКЗИ

Обязательность применения норм СТ РК 1073-2007 государственными органами, местными исполнительными органами, государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры при обеспечении конфиденциальности с помощью СКЗИ нормативно закреплена постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Единые требования в

области информационно-коммуникационных технологий и обеспечения информационной безопасности».

В соответствии с пунктом 48 этого постановления с целью защиты служебной информации ограниченного распространения, конфиденциальных информационных систем, конфиденциальных электронных информационных ресурсов и электронных информационных ресурсов, содержащих персональные данные ограниченного доступа, применяются СКЗИ (программные или аппаратные) с параметрами, соответствующими требованиям СТ РК 1073-2007 [13].

Рисунок 10 – СКЗИ для обеспечения конфиденциальности и целостности

Ключевым отличием между СКЗИ, обеспечивающим конфиденциальность и средствами электронной цифровой подписи (ЭЦП), обеспечивающими целостность документов, являются последствия при компрометации. Так, компрометация СКЗИ, предназначенного для сохранения конфиденциальности данных при помощи алгоритмов шифрования приведет к нарушению конфиденциальности, т.е. к утечке информации, а компрометация средств ЭЦП приведет к возможности подделки документа и подписи.

Для удостоверения соответствия открытого ключа ЭЦП закрытому ключу ЭЦП, а также подтверждения достоверности регистрационного свидетельства в Республике Казахстан действуют удостоверяющие центры (УЦ).

Подпунктом 1) пункта 4 приказа Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ «Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре» определено требование для аппаратного криптографического модуля (Hardware Security Module) о соответствии хотя бы третьему уровню безопасности в соответствии с требованиями, установленными СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" [14].

Рисунок 11 – Стандартизация СКЗИ

Таким образом, в вышеуказанных нормативных правовых актах (НПА) приведены требования к безопасности применяемого СКЗИ в виде соответствия требованиям Государственного стандарта Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования", что делает стандартизацию СКЗИ обязательной. Указанный стандарт распространяется на СКЗИ отечественного и зарубежного производства и устанавливает общие технические требования к ним. Стандарт пригоден для целей подтверждения соответствия. При этом, стандарт не распространяется на СКЗИ, являющиеся государственными шифровальными средствами Республики Казахстан.

Рисунок 12 - Государственный стандарт СТ РК 1073-2007

Указанный стандарт стал основным казахстанским стандартом для оценки качества СКЗИ.

Рисунок 13 – Необходимость переработки СТ РК 1073-2007

В Республике Казахстан в соответствии Законом от 15 марта 1999 года № 349-1 «О государственных секретах» уполномоченным органом в вопросах криптографии является КНБ РК. Компетенция в области криптографии возложена на КНБ РК в Положении о КНБ РК, утвержденном Указом Президента Республики Казахстан от 1 апреля 1996 года № 2922.

КНБ в установленном законодательством Республики Казахстан порядке и в пределах своей компетенции:

организует сертификацию технических, в том числе криптографических средств защиты сведений, составляющих государственные секреты (подпунктом 35) пункта 12).

контролирует исполнение на территории Республики Казахстан системы правовых, административных, экономических, технических, программных и криптографических мер по защите государственных секретов (подпункт 64-18 пункта 12).

разрабатывает систему правовых, административных, экономических, технических, программных и криптографических мер по защите государственных секретов (подпункт 64-25 пункта 12).

КНБ для решения возложенных задач и выполнения функций в установленном законодательством порядке имеет право:

проводить технические исследования на предмет отнесения товаров к специальным техническим средствам для проведения оперативно-технических мероприятий и средствам

криптографической защиты информации, выдавать по ним соответствующие заключения (подпункт 31-1 пункта 13);

рассматривать заявления физических и юридических лиц о выдаче заключений (разрешительных документов) на ввоз или вывоз специальных технических средств и средств криптографической защиты информации, регистрации нотификаций о характеристиках товаров, содержащих криптографические функции, выдавать по ним соответствующие разрешения и регистрировать нотификации (п.п. 31-2 п. 13);

осуществлять согласование лицензий на импорт и экспорт средств криптографической защиты информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий (п.п. 31-3 п. 13).

В соответствии с пунктом 1 постановления Правительства Республики Казахстан от 27 июля 2015 года № 589 «Об определении лицензиара в сферах обеспечения информационной безопасности, специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, и органа, уполномоченного на выдачу разрешения второй категории в области криптографической защиты информации» КНБ определен лицензиаром
по осуществлению лицензирования деятельности по:

разработке средств криптографической защиты информации;

органом, уполномоченным на выдачу разрешения второй категории "Разрешение на реализацию (в том числе иную передачу) средств криптографической защиты информации" [18].

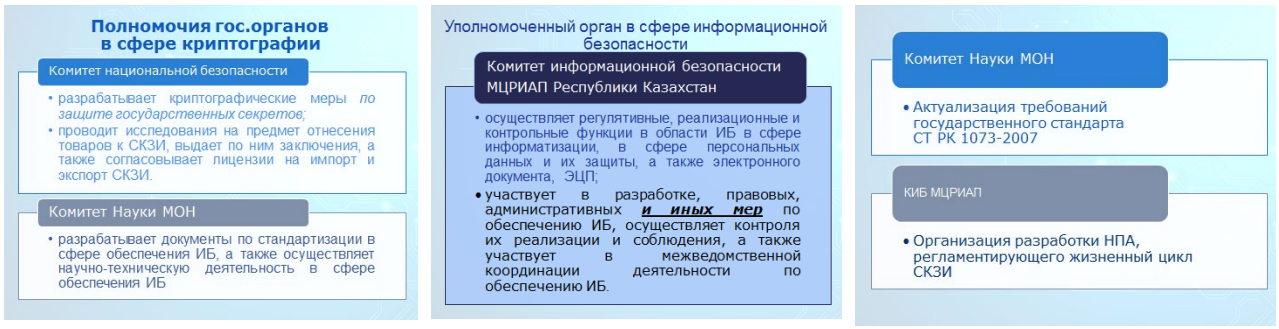


Рисунок 14 – Полномочия госорганов в сфере криптографии

Перечень компетенций и полномочий государственных органов республики в сфере информационной безопасности и криптографической защиты информации, переработки НПА в области криптографии, по мнению исследователей КНБ РК отражен ниже в таблице 2.

Касаясь компетенции государственных органов, казахстанские республики полагают:

Таблица 2 – Перечень компетенций и полномочий госорганов

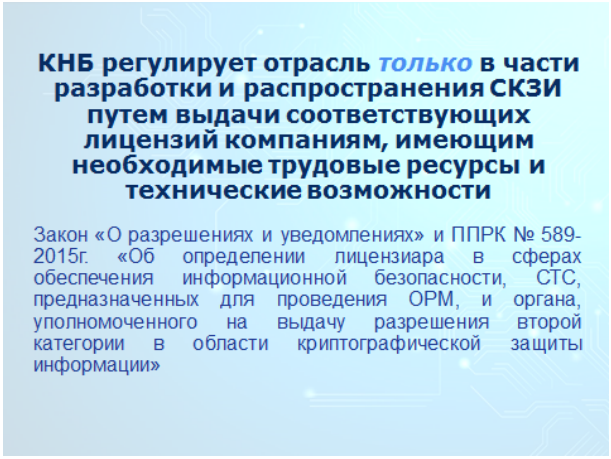
	К компетенции относится разработка правовых, административных, экономических, технических, программных и криптографических мер по защите государственных секретов, а также выдача лицензий на разработку и реализацию СКЗИ

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, ИННОВАЦИЙ И АЭРОКОСМИЧЕСКОЙ ПРОМЫШЛЕННОСТИ РЕСПУБЛИКИ КАЗАХСТАН

Организация разработки НПА, регламентирующего жизненный цикл СКЗИ, который устарел, относится к компетенции Комитета по информационной безопасности МЦРИАП

ИИСТ ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ

переработка государственного стандарта СТ РК 1073-2007 относится к компетенции Института информационных и вычислительных технологий Комитета науки МОН



Специалистами КНБ и МО РК проведен анализ законодательства в сфере криптографической защиты информации государств - участников СНГ и Украины. По результатам изучения установлено, что в целом, системы правового регулирования криптографической защиты на постсоветском пространстве выстроены схожим образом, что объясняется наличием специалистов старшего поколения «советской школы криптографии».

В то же время прослеживается следующая тенденция: чем менее развита в государстве электронная промышленность, разработка и производство собственных средств защиты информации, тем менее полным и детализированным представляется законодательство в области криптографической защиты информации. Так, например, в Украине, Беларуси и России при необходимости оценки соответствия СКЗИ требованиям, которые техническими нормативными правовыми актами не установлены, осуществляется экспертиза СКЗИ. В Кыргызской Республике, Республике Армения и Республике Казахстан указанные мероприятия не предусмотрены.

Рисунок 15 - Часть сравнительного анализа НПА стран СНГ в сфере криптографии

Примечательно, что в Российской Федерации, Кыргызской Республике и Республике Армения функции и задачи в области криптографической защиты информации отнесены к компетенции служб безопасности указанных государств, в то время как в Республике Беларусь и в Украине для этих целей созданы отдельные государственные органы (Оперативно-аналитический центр при Президенте Республики Беларусь (ОАЦ) и Государственная служба специальной связи и защиты информации Украины (ГСССЗИ), соответственно).

Особую позицию в этом отношении занимает Республика Казахстан, в которой часть функций (разработка криптографических мер по защите государственных секретов, лицензирование деятельности в области СКЗИ, ввоз шифровальных средств) осуществляет КНБ, разработка мер по обеспечению информационной безопасности относится к компетенции КИБ МЦРИАП. Национальным институтом развития в сфере обеспечения информационной безопасности определен "Институт информационных и вычислительных технологий" Комитета науки Министерства образования и науки Республики Казахстан, а разработка производство, ремонт и реализация СКЗИ переданы в конкурентную среду для обеспечения условий развития данной отрасли.

Уполномоченными структурными подразделениями МО РК для анализа ситуации в этой сфере рассмотрен вопрос о принятии в Китайской Народной Республике Закона «О криптографии». Указанным законом закреплена компетенция уполномоченного органа в области криптографии, установлена ответственность за нарушение требований Закона «О криптографии», а также определена классификация криптографии на три вида. Первые два вида криптографии (основная и общая), предназначены для защиты сведений, составляющих государственные секреты КНР, и строго регулируются со стороны государства, третий вид (коммерческая) – для защиты сведений, не составляющих государственные секреты. Уполномоченным органом в КНР в области криптографии определено – Государственное подразделение управления криптографией.

При этом, в законодательстве Республики Казахстан, в отличие от закона КНР «О криптографии», не определены виды криптографии (основная, общая и коммерческая), но в то же время имеется четкое разграничение криптографических средств по классу (степени) защищаемой информации – государственные шифровальные средства (далее – ГШС) и средства криптографической защиты информации (далее – СКЗИ).

Государственные шифровальные средства – средства криптографической защиты информации, предназначенные для защиты сведений, составляющих государственные

секреты с гарантированной криптографической стойкостью и специальной защитой от утечки информации по техническим каналам, разрешенные к применению в Республике Казахстан.

Средство криптографической защиты информации (СКЗИ) – средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами.

Рисунок 16 - СКЗИ и ГШС

Первый класс (ГШС) предназначены для защиты сведений, составляющих государственные секреты (по аналогии с Законом КНР – основная и общая криптография). Требования к ГШС, а также порядку их разработки и изготовления определяются Техническими регламентами, утвержденными приказами ПКНБ РК. Порядок использования ГШС на каналах связи определяется Правилами организации шифровальной работы в Республике Казахстан, утвержденных Указом Президента Республики Казахстан и правилами пользования (работы) определенным типом ГШС.

Второй класс (СКЗИ) предназначены для защиты несекретной, но в то же время критической по отношению к разглашению, информации (например, банковской или персональной информации), а также служебных сведений, имеющих ограничительную пометку «Для служебного пользования» (по аналогии с Законом КНР – коммерческая криптография). Требования к СКЗИ определяются стандартом Республики Казахстан «Средства криптографической защиты информации. Общие технические требования» (СТ РК 1073-2007). Порядок использования СКЗИ на каналах связи и в информационных системах определен различными нормативными правовыми актами Республики Казахстан, ведомственными нормативными документами государственных органов и инструкциями по их настройке и использованию.

Ответственность за нарушения в области криптографии, повлекшие разглашение передаваемых сведений, закреплена в Уголовном кодексе Республики Казахстан (статьи 185 и 186) и Кодексе об административных правонарушениях (статья 504), не повлекшие разглашения передаваемых сведений – в Дисциплинарном уставе и других нормативных правовых актах Республики Казахстан. Также законодательно определено, что криптография в Республике Казахстан является лицензируемым видом деятельности. Для законного использования на каналах связи или в информационных системах СКЗИ, в соответствии с требованиями нормативных правовых актов (НПА), должны пройти в сертификационных

органах сертификацию на предмет соответствия СТ РК 1073-2007, а ГШС – на предмет соответствия Техническим регламентам.

Однако необходимо отметить, что одним из пробелов в законодательстве и проблемным вопросом криптографии в Республике Казахстан, в целом, является отсутствие официально принятого национального алгоритма шифрования. В связи с чем, в СКЗИ и ГШС применяются алгоритмы шифрования, принятые в качестве стандартов в других странах (в основном российский ГОСТ или американский AES, либо их совмещенное использование). При этом разработка собственного (национального) алгоритма шифрования является трудоемкой задачей с научной точки зрения, по причине отсутствия достаточно сильной национальной школы криптографии.

Министерством обороны также проведен мониторинг НПА в области криптографии, опубликованных в открытых источниках и принятых в отдельных странах СНГ (Российская Федерация, Республика Беларусь, Украина, Республика Узбекистан, Кыргызская Республика). Установлено, что отдельного закона «О криптографии» ни в одной из рассматриваемых стран не принято, а законодательное регулирование отношений в области криптографии осуществляется в основном в аналогичном с Республикой Казахстан порядке, за исключением отдельных незначительных моментов (например: отличия в классификации СКЗИ, разные подходы к сертификации, в Российской Федерации и Республике Беларусь, Украине и Узбекистане официально приняты национальные алгоритмы шифрования и ряд других).

Министерство обороны полагает, что на данный период времени принятие в республике закона, аналогичного закону КНР «О криптографии» преждевременно по причине наличия достаточно отрегулированной нормативной правовой базы и отсутствия значительного производства собственных СКЗИ и государственных шифровальных средств.

Полагается, что, возможно другой взгляд на существующие и обозначенные в этом докладе проблемы информационной безопасности, связанные с криптографическими методами защиты информации, может быть дан и другими квалифицированными специалистами Комитета национальной безопасности и Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности и Института информационных и вычислительных технологий.

Литература

1. В. Ф. Шаньгин. Информационная безопасность компьютерных систем и сетей. Учебное пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. — 416 с.:ил. — (Профессиональное образование).

2. Н. Смарт. Криптография = Cryptography: An Introduction / пер. с англ. С.А. Кулешова под ред.С.К. Ландо. — М. : Техносфера, 2005. — 528 с.

3. Илья Ферапонтов. Квантовая криптография: что это такое? 29 мая 2018. По материалам Интернет-журнала «Популярная механика».

4. Дошина А. Д., Михайлова А. Е., Карлова В. В. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] // Современные тенденции технических наук: материалы IV Междунар. науч. конф. (г. Казань, октябрь 2015 г.). — Казань: Бук, 2015. — С. 10-13. — URL https://moluch.ru/conf/tech/archive/163/8782

5. По материалам сайта - http://www.tadviser.ru/a/53660 Квантовая криптография / шифрование.

6. По материалам сайта - https://www.securitylab.ru/news/487363.php?R=1 Физики создали первый в мире 51-кубитный квантовый компьютер.

7. Николай Самодаев. Кибербезопасность на новом витке: готовимся противостоять киберугрозам. 20-е международное исследование EY в области информационной безопасности за 2017-2018 годы.

8. Сейткулов Е.Н. Информационная безопасность Республики Казахстан: состояние и перспективы. 10 Октября 2016. Электронный ресурс - https://www.enu.kz/ru/info/novosti-enu/novosti-nauki/45582/.

9. Закон Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи».

10. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

9. Ибраев Р.Б., Горлов Л.В., Возный О.Э. Анализ полноты требований Государственного стандарта Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования». «Сатпаевские чтения 2020, том 2». Издательство КазНИТУ им. К. Сатпаева.

10. Абдрахманов А.Е. Безопасные пороги для параметров криптографических алгоритмов и стандарт СТ РК 1073-2007. «Известия». Серия физико-математическая N 5 (333). Издательство Национальной академии наук Казахстана.

13. Государственный стандарт Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

14. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 405/НҚ «Об утверждении Правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре».

15. Постановление Правительства Республики Казахстан от 27 июля 2015 года № 589 «Об определении лицензиара в сферах обеспечения информационной безопасности, специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, и органа, уполномоченного на выдачу разрешения второй категории в области криптографической защиты информации».

ЖЕЛІЛЕРДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БҰЗУ ҚАТЕРЛЕРІ МЕН ОСАЛДЫҚТАРЫН АНЫҚТАУ

Мухаев Д.К.
e-mail: daryn.mukhayev@gmail.com
Ақпараттық және есекптеуіш технологиялар институты, Алматы, Қазақстан

Аңдатпа. *Мақалада желілердегі ақпараттық қауіпсіздікті бұзу қатерлері мен осалдықтарын анықтау мәселелері қарастырылған. Ақпаратты қорғау үшін компьютерлік шабуылдарды анықтау жүйелерін құру қажет. Кибершабуыл ұғымына түсініктеме беріліп, олардың түрлеріне тоқталған. Қазіргі уақытта ешбір ұйым кибершабуылдан жеткілікте деңгейде қорғалмаған. Барлық ұйымдар киберқылмыскерлермен күресу мақсатында арнайы жоспар құруы керек. Арнайы жоспар төтенше жағдайларға дайын болып, туындайтын қатерлерге қарсы тұруға және шабуылдың әсерін жылдам қалпына келтіруге мүмкіндік береді. Кибершабуылдан қорғану үшін қауіп төндіретін факторларды біліп, олардың тактикасын, әдістері мен процедураларын түсіну қажеттілігі атап көрсетілген. Ақпаратты қорғау процесі деректерді өңдеудің автоматтандырылған құралдарын құру мен пайдаланудың барлық кезеңдерінде жүзеге асырылатын кешенді және үздіксіз болуы керек. Ақпаратты қорғаудың негізгі әдістері келтірілген.*

Негізгі сөздер. Ақпараттық қауіпсіздік, кибершабуыл, киберқылмыскер, ақпаратты қорғау, қауіптер, осалдықтар.

Ғылым мен техниканың қарқынды дамуына байланысты барлық өндіріс салаларына әлемдік ақпараттық технологиялардың әсері күшейіп келеді. Осыған орай қоғамда жаңа әлеуметтік топтар қалыптасып, адамдардың қалыпты өмір салты айтарлықтай өзгеруде. Қазіргі кезде жүзеге асырылып жатқан белсенді түрде ақпараттандыруға байланысты ақпараттық қауіпсіздік мәселелері аса маңызды. Олардың көпшілігі ақпараттың үлкен көлемін өңдеуді оңтайландыру, соның ішінде оның сенімді сақталуы және ақпарат алмасу үшін қолжетімділікті қамтамасыз ету мақсатында бірыңғай ақпараттық кеңістікті құруға бағытталған.

Осы мақсатты жүзеге асыру үшін қойылатын негізгі міндеттер - рұқсат етілмеген ақпаратты алуға немесе ақпараттық жүйелердің қалыпты жұмыс істеуін бұзуға әкеп соғуы мүмкін ақпараттық қауіпсіздік қатерлерін анықтау, талдау және жіктеу, қауіп-қатерлерге қарсы тұру және осалдықтарды жою үшін атқарылатын негізгі шараларды анықтау, қауіпсіздік критерийлері мен механизмдерін, сондай-ақ тиісті заңнамалық және нормативтік-құқықтық базаны әзірлеу.

Ақпараттық қауіпсіздікке төнетін қатерлерді анықтау мен талдауға арналған ғылыми зерттеулерді көптеген ресейлік және шетелдік ғалымдар жүргізді, олардың ішінде Я.Н.Алгулиев, И.Л.Альферов, А.А.Захаров, С.Л.Зефирова, Д.О.Карпеева, А.Г.Кащенко, А.А.Кононова, А.О. Сидорова, М.В.Тимонина және т.б.

Зерттеулер нәтижелері көрсеткендей, ақпарат саласындағы қылмыстардан келетін зиян жылына миллиардтаған долларға бағаланады. Қазіргі кезде компьютерлік технологияның даму қарқыны ақпараттық қауіпсіздік құралдарын құру үдерісінен едәуір озық. Сонымен қатар, әртүрлі пәндік салаларға қолданылатын қауіпсіз ақпараттық жүйелердің бірыңғай теориясы қалыптасқан жоқ.

Көрсетілген мәселелерді шешудің құралдарының бірі - ақпаратты қорғау үшін ұзақ уақыттан бері қолданылып келген компьютерлік шабуылдарды анықтау жүйелері. Заманауи жүйелердің көпшілігі компьютерлік шабуылдарды анықтау желілік ауытқуларды түзету және

қолтаңбаларды талдау әдістерін қолдана отырып жұмыс істейді. Бұл әдістердің оларды жүзеге асыруға арналған есептеу шығындарымен байланысты кемшіліктері бар, сонымен қатар компьютерлік шабуылдардың жаңа түрлерін табудағы тиімділігі төмен.

Ақпараттық қауіпсіздікті қамтамасыз етудің негізі шетелдік және отандық коммерциялық немесе мемлекеттік органдар құрған арнайы мәліметтер қоры мен интернет-ресурстар болып табылады. Мәліметтер қорын толтыру беделді ғылыми орталықтардың қатысуымен сараптамалық тәсілмен жүзеге асырылады. Алайда, мәліметтер қорында келтірілген ақпараттық қауіптер мен осалдықтардың тізімдері толық емес. Белгілі бір тақырыптық аймақтарда болып жатқан оқиғаларға қатысты пікірталас Интернет-платформаларын пайдаланушылардың арасында жиі болады. Тақырыптық талдау негізінде ақпараттық қауіпсіздік қауіптері мен осалдықтарының пайда болуын болжауға мүмкіндік туады.

Жоғарыда айтылғандарға байланысты, кезек күттірмейтін міндет - осалдықтар, компьютерлік шабуылдар мен вирустар туралы мәліметтер, сондай-ақ ақпараттық қауіпсіздікке төнетін қатерлерді анықтау бойынша мамандандырылған зерттеулер нәтижелері бар жалпыға қол жетімді ақпараттық ресурстарды анықтау. Ақпараттық қауіпсіздік маманы қауіптің немесе осалдықтың пайда болуын болжау нәтижелерін ала отырып, қорғалатын ақпараттық ресурстар үшін қауіптілік дәрежесін, қолданылып жүрген ақпараттық қауіпсіздік қатерлер моделінің дұрыстығын бағалай алады және осалдықтарды бейтараптандыру бойынша шаралар қолданады.

Кибершабуыл - бұл ұйымның немесе жеке тұлғаның басқа ұйымның немесе жеке тұлғаның жүйелерін бұзуға бағытталған қасақана және зиянды әрекеті. Шабуылшының мақсаты ақпаратты ұрлау, қаржылық пайда табу немесе тыңшылық болуы мүмкін. Қауіп-қатерлердің түрлері көбейіп келе жатқанына қарамастан, олардың кеңінен таралған түрлері бар. Соларға тоқтала кетейік.

Зиянды бағдарламалық шабуыл - бұл кибершабуылдың ең көп таралған түрі. Зиянды бағдарлама деп пайдаланушы қауіпті сілтемені немесе электрондық поштаны басқан кезде жүйеге орнатылатын зиянды бағдарламалар, оның ішінде шпиондық бағдарламалар, төлем бағдарламалары, вирустар мен құрттарды айтамыз. Жүйеге енгеннен кейін, зиянды бағдарламалық қамтамасыз ету, басқалармен қатар, маңызды желілік компоненттерге кіруді бұғаттауы, жүйені зақымдауы және құпия ақпаратты жинауы мүмкін.

Киберқылмыскерлер заңды ресурстардың атынан зиянды хаттарды жібереді. Пайдаланушы электрондық поштадағы зиянды сілтемені басу нәтижесінде зиянды бағдарлама орнатылады немесе несиелік карта және кіру деректері сияқты құпия ақпарат алынады. Фишингтік шабуылдар тіркелген кибер оқиғалардың 80% -дан астамын құрайды.

Бағытталған фишинг - бұл жүйелік ұйымдастырушылар мен басшылар сияқты артықшылығы барларға ғана бағытталған фишинг шабуылдарының анағұрлым жетілдірілген түрі. Мақсатты шабуылдардың 71%-дан астамы бағытталған фишингті қамтиды.

Ортадағы адам (MitM) шабуылы киберқылмыскерлер екі жақты байланыс арасында қалып қойғанда пайда болады. Ол құпия деректерді сүзіп, ұрлап, қолданушыға әр түрлі жауаптар қайтара алады. Netcraft деректері бойынша HTTPS серверлерінің 95% -ы MitM шабуылына осал.

Қызмет көрсетуден бас тарту түріндегі шабуылдар желілерді немесе серверлерді жаппай толтыруға бағытталған, бұл жүйенің заңды сұраныстарды орындауына жол бермейді. Осы мақсатта бірнеше зақымдалған құрылғыларды қолдана алады. Бұл «Қызмет көрсетуденбас тарту» (DDoS) шабуылы деп аталады. 2019 жылы 8,4 миллион DDoS шабуылдары болған.

Құрылымдық сұраныстар тіліне (SQL) енгізе отырып шабуыл жасау киберқылмыскерлер SQL сценарийлерін жүктеу арқылы дерекқорға қол жеткізуге тырысқанда пайда болады. Бұл

жағдайда шабуылдаушы SQL дерекқорында сақталған деректерді көре, өзгерте немесе жоя алады. SQL шабуыл барлық веб-қосымшаларға жасалған шабуылдардың шамамен 65,1% құрайды.

Нөлдік күндік шабуыл бағдарламалық жасақтаманың немесе аппараттық құралдың осалдығы туралы хабарланған кезде пайда болады және киберқылмыскерлер шешім табылғанға дейін осалдықты пайдаланады. 2021 жылға қарай нөлдік күндік шабуылдар саны күніне бір шабуыл жасалуға дейін өседі деп болжануда.

Жетілдірілген тұрақты қауіп шабуылдаушы жүйеге немесе желіге рұқсатсыз қол жеткізгенде және ұзақ уақыт байқалмай жүргенде пайда болады. Ұйымдардың 45% -ы осы шабуылдауға ұшырайды.

Бопсалаушы бағдарлама - зиянкестер жәбірленушінің деректерін блоктайтын немесе шифрлайтын және егер төлем төленбесе, деректерді жариялаймын немесе оған қол жеткізуді блоктаймын деп қорқытатын зиянды бағдарламалық шабуыл түрі. Болжам бойынша, мұндай шабуылдар әлемдік ұйымдарға 2021 жылы 20 миллиард доллар шығын әкеледі.

DNS шабуылы - бұл киберқылмыскерлер домендік атау жүйесіндегі (DNS) осалдықтарды пайдаланатын кибер шабуыл. Шабуылшылар сайтқа кірушілерді зиянды беттерге бағыттау үшін DNS осалдықтарын пайдаланады (DNS ұрлау) және бұзылған жүйелерден деректерді шығарып тастайды (DNS туннелі). DNS шабуылының орташа құны 2020 жылы $ 924,000 құрады.

Кибершабуылға тиімді жауап беру үшін қауіп төндіретін факторларды біліп, олардың тактикасын, әдістері мен процедураларын түсіну қажет.

Коронавирустық пандемия 2020 жылы бизнес пен АТ ұйымдары үшін ең үлкен проблемаға айналды. Пандемия жағдайында киберқауіптер мен деректердің бұзылуы күрделене түсті және ауқымды болды, ал бұзушылықтардың саны бірінші тоқсанда 2019 жылмен салыстырғанда 273% өсті. Майкрософттың мәлімдеуінше, пандемиямен байланысты фишингтік және әлеуметтік инженерлік шабуылдар саны тек АҚШ-та күніне 30 000-ға дейін өсті.

Киберқылмыскерлер коронавирустық пандемияны және онымен байланысты тақырыптарды өздерінің фишингтік және әлеуметтік инженерлік кампаниялары үшін тақырып ретінде қолдана береді. Олардың шабуылдары көбінесе COVID-19 жағдайларының кенеттен өршуі немесе жаңа вакцина туралы хабарлау сияқты маңызды оқиғалармен сәйкес келеді. Шабуылшылар пайдаланушыларға зиянды сілтемені немесе заңды COVID-19 тақырыптарының атын жамылған қосымшаны басуға шақырады.

Қашықтықтан жұмыс істеуді және бизнестің үздіксіздігін жеңілдету үшін көптеген компаниялар бұлтқа ауысқан кезде, киберқылмыскерлер дәл осы тенденцияны ұстанып, бұлтты нысанаға алуда. Бұлттық қауіпсіздіктің қаупі, соның ішінде бұлтты дұрыс конфигурацияламау, деректердің толық жойылмауы және осал бұлтты қосымшалар кибершабуылдардың жалпы көздері болады.

Пандемия жағдайында бизнестің үздіксіздігін қамтамасыз ету мақсатында барлық дерлік кәсіпорындар үйден жұмыс істей бастады. Байланыс жасаушылар смартфондар мен планшеттер сияқты құрылғыларды қауіпсіз қорғалмаған, патчпен жабылмаған немесе АТ қауіпсіздік бөлімі басқармайтын құралдарды пайдаланады. Өкінішке орай, олар ұйымдарға кибершабуыл жасау қаупін туғызатын АТ қауіпсіздігінің кейбір ерекше қатерлері мен осалдықтарын тудырады.

Қазіргі цифрлық дәуірде бірде-бір ұйым кибершабуылдан қорғалмаған. Осылайша, барлық көлемдегі ұйымдар киберқылмыскерлермен күресу үшін инциденттерге қарсы іс-қимылдың тиімді жоспарын әзірлеуі керек. Бұл кәсіпорындарға төтенше жағдайларға дайын

болуға, туындайтын қатерлерге қарсы тұруға және шабуылдың әсерін тез қалпына келтіруге мүмкіндік береді.

Деректердің сақтық көшірмесін үнемі жасап отыру деректердің ұрлану қаупін азайтуға көмектеседі. Веб-сайттың, қосымшалардың, мәліметтер қорының, электрондық поштаның, қосымшалардың, файлдардың, күнтізбелердің және т.б. сақтық көшірмесін тұрақты және дәйекті түрде жасап отыру керек.

Ақпараттық қауіпсіздіктің қазіргі кездегі қауіптері мен осалдықтарын талдау ақпаратты қорғаудың мақсаттары мен міндеттеріне қол жеткізу, сондай-ақ қауіпсіздіктің жоғары деңгейін қамтамасыз ету, қорғаудың қол жетімді әдістері мен құралдарын кешенді қолдануды қажет ететіндігін көрсетеді. Осы себепті ақпараттық қауіпсіздік тұжырымдамалары мен нақты ақпараттық қауіпсіздік құралдарын дамытуға негізделген негізгі қағидалардың бірі - бұл кешенділік.

Ақпаратты қорғауды қамтамасыз ету процесі деректерді өңдеудің автоматтандырылған құралдарын құру мен пайдаланудың барлық кезеңдерінде жүзеге асырылатын кешенді және үздіксіз болуы керек. Осы жағдайларда ақпараттық қауіпсіздік процесін іске асыру қауіпсіздік техникасының өндірістік тұжырымдамалық тәсілдеріне және өндірісіне негізделеді. Әдетте қорғау тетіктерін құру, олардың сенімді және тиімді жұмысын қамтамасыз ету үшін жоғары білікті ақпараттық қауіпсіздік мамандары тартылады.

Ақпаратты қорғаудың негізгі мақсаты - ақпаратқа келеңсіз әсер ету көздерін, сондай-ақ олардың себептері мен жағдайларын анықтау және жою немесе бейтараптандыру. Аталған ақпарат көздері ақпараттың қауіпсіздігіне қауіп төндіреді. Ақпаратты қорғаудың негізгі әдістеріне мыналар жатады:

- олардың пайда болу мүмкіндігін бейтараптандыру үшін ақпараттық қауіпсіздікті қамтамасыз ету бойынша белсенді шараларды қабылдау арқылы белгілі қауіптердің алдын алу;

- қорғалатын ақпаратқа қатысты зиянкестердің нақты қауіптері мен нақты рұқсат етілмеген әрекеттерін анықтау нәтижесінде қауіп-қатерлерді анықтау;

- нақты немесе мүмкін қауіптердің пайда болуын үздіксіз талдау және бақылау барысында жаңа қатерлерді анықтау, сондай-ақ белсенді шараларды уақтылы қабылдау.

Қауіп-қатер туралы ақпарат - ұйымға қауіп төндіруі мүмкін шабуылдар туралы алдын-ала талданған ақпарат. Қауіптерді талдау ұйымдарға әлеуетті немесе қазіргі кездегі киберқауіптерді түсінуге көмектеседі. Ақпараттық қауіпсіздік персоналы қауіп-қатер субъектілері, олардың мүмкіндіктері, инфрақұрылымы мен уәждері туралы неғұрлым көп болса, соғұрлым олар өз ұйымдарын қорғай алады.

Қауіпті талдау жүйелері әдетте басқа қауіпсіздік құралдарымен бірге қолданылады. Қауіпсіздік жүйесі қауіп-қатерді анықтаған кезде, ол қауіптің сипатын, оның қиындығын және қауіп-қатерді азайту немесе болдырмаудың белгілі әдістерін дереу түсіну үшін қауіп-қатер туралы ақпаратпен байланыстырылуы мүмкін. Көптеген жағдайларда қауіп-қатерді талдау қауіптерді автоматты түрде блоктауға көмектеседі - мысалы, бұзылған серверлерден трафикті автоматты түрде блоктау үшін белгілі IP-адрестерді брандмауэрге жіберуге болады.

Қауіп туралы ақпарат әдетте арналар түрінде беріледі. Коммерциялық қауіпсіздікті зерттейтін ұйымдар ұсынатын қауіп-қатер туралы ақпараттардың ақысыз арналары және басқалары бар. Кейбір бағдарлама құрушылар қауіп-қатер туралы ақпаратты басқа қауіпсіздік жүйелерімен басқаруға және интеграциялауға көмектесу үшін көптеген қауіпті барлау платформаларын ұсынады.

Аталған мақсатты жүзеге асыруға бағытталған алгоритмнің нәтижесі анықталған қауіптер мен ақпараттық қауіпсіздіктің осалдықтары туралы есептер болып табылады, олар мәтіндік хабарламалар ағынының талдау нәтижелерін бейнелейтін ақпаратты қамтуы мүмкін,

соның негізінде қауіптер немесе осалдықтардың пайда болуы туралы қорытынды жасалады. Мұндай ақпарат мыналар болуы мүмкін:

– тақырыптық интернет-ресурстарда қауіп-қатерлер мен ақпараттық қауіпсіздіктің талданатын кезеңіне қатысты хабарламалардың жасалу жиілігі;

– талданып отырған уақыт кезеңіндегі қауіп-қатерлер мен ақпараттық қауіпсіздіктің тақырыптық саласына қатысты хабарламалар авторларының орташа рейтингі;

– талданып отырған кезеңде тақырыптық интернет-ресурстардың хабарламаларында кездесетін қауіптер мен ақпараттық қауіпсіздік осалдықтарының жиіліктік сипаттамалары;

– талданып отырған кезеңде құрылған және ақпараттық қауіпсіздікке қатерлер мен осалдықтардың шарттарын қамтитын тақырыптық интернет-ресурстардың хабарлама мәтіндерін таңдау;

– хабарламаларда кездесетін қауіптер мен ақпараттық қауіпсіздік осалдықтарының онтологиясының тізбесі, бұл болжамды қауіптер мен осалдықтарды жіктеуге мүмкіндік береді.

Тәуекелді сандық бағалау зерттелетін қауіптер мен онымен байланысты тәуекелдерді ақшамен, пайызбен, уақытпен, адам ресурстарымен және т.б. көрсетілген соңғы сандық мәндермен салыстыруға болатын жағдайларда қолданылады. Әдіс ақпараттық қауіпсіздікке төнетін қатерлерді жүзеге асыру кезінде тәуекелдерді бағалау объектілерінің нақты мәндерін алуға мүмкіндік береді. Сандық тәсілде тәуекелді бағалаудың барлық элементтеріне нақты сандық мәндер тағайындалады. Осы мәндерді алу алгоритмі нақты және түсінікті болуы керек. Активтің ақшалай мәні, қауіптің жүзеге асу ықтималдығы, қауіп-қатерден келген залал, қорғаныс шараларының құны және басқалары бағалау объектісі бола алады.

Сапалы әдіс тәуекелдерді тезірек бағалауға мүмкіндік береді, бірақ бағалау мен нәтижелер субъективті болып табылады және ақпараттық қауіпсіздік жүйелерін енгізуден болатын зиян, шығындар мен пайда туралы нақты түсінік бермейді. Әдісті таңдау белгілі бір компанияның ерекшелігіне және маманға жүктелген міндеттерге байланысты.

Қорытынды. Мақалада ақпараттық қауіпсіздіктің қазіргі кездегі қауіптері мен осалдықтары талданды. Болашақтағы зерттеулер шеңберінде қауіптер мен ақпараттық қауіпсіздіктің осалдығы туралы болжамның сапасын жақсарту мүмкіндіктерін қарастыру жоспарлануда.

Әдебиеттер тізімі

1. Кирсанов, К.А. Информационная безопасность: Учеб. пособие К. А. Кирсанов, А. В. Малявина, Н. В. Попов; Моск. акад. экономики и права. – М.: МАЭП, 2000
2. Конеев, И.Р. Информационная безопасность предприятия: [Информ. безопасность. Классификация атак. Методика упр. рисками. Криптограф. средства и механизмы] Искандер Конеев, Андрей Беляев. – СПб.: БХВ-Петербург, 2003
3. Мельников, В.В. Защита информации в компьютерных системах: – М.: Финансы и статистика. Электроинформ, 2004
4. Шаковец, А.Н. Основы защиты компьютерной информации и информационная безопасность: Лекция А.Н. Шаковец, Н.В. Рымарева; М-во внутрен. дел России, Дальневосточ. юрид. ин- – Хабаровск: Дальневосточ. юрид. ин-т МВД РФ, 2003
5. Смагин А.А., Полетаев В.С. Алгоритм прогнозирования угроз информационной безопасности // Инфокоммуникационные технологии. 2018. Т. 16, №2. С. 192–198.

6. Yazan Alshboul, Kevin Streff. Analyzing Information Security Model for Small-Medium Sized Businesses: Twenty-first Americas Conference on Information Systems, Puerto Rico, 2015. DOI: https://core.ac.uk/download/pdf/301365935.pdf

7. Julian Jang-Jaccard, Surya Nepal. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, Volume 80, Issue 5, August 2014, Pages 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

8. Top cybersecurity threats on enterprise networks: https://www.ptsecurity.com/ww-en/analytics/network-traffic-analysis-2020/

9. Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri.2018. The Privacy Implications of Cyber Security Systems: A Technological Survey.ACM Comput. Surv.51,2, Article 36 (February 2018), 27 pages. https://doi.org/10.1145/3172869

10. B. A. Obotivere, A. O. Nwaezeigwe. Cyber Security Threats on the Internet and Possible Solutions, September 2020, IJARCCE 9(9): 92-97. DOI: 10.17148/IJARCCE.2020.9913

EVE-NG ПЛАТФОРМАСЫ НЕГІЗІНДЕ ЖЕЛІЛІК ШАБУЫЛДАРДЫ МОДЕЛЬДЕУ

[1,2]Ордабаева Г.К., [1]Еркін М., [1]Жылқаман Ф., [1]Оразалина Р.
E-mail: gulzi200988@mail.ru
[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан
[2]Қазақ ұлттық аграрлық зерттеу университеті, Қазақстан

***Аңдатпа**: Мақалада Emulated Virtual Environment - Next Generation (Eve-NG) эмуляторы негізінде желілік шабуылдарды модельдеу қарастырылды. Ақпараттық қауіпсіздік жүйесі мамандарын даярлау барысында шабуылдардың виртуалды түрде алдын-алу мақсатында Eve-NG эмуляторында желілік топология ұйымдастырылды. Шабуылдарды модельдеу барысында Kali Linux, Windows 7, Windows 10 операциялық жүйелері қарастырылды.*

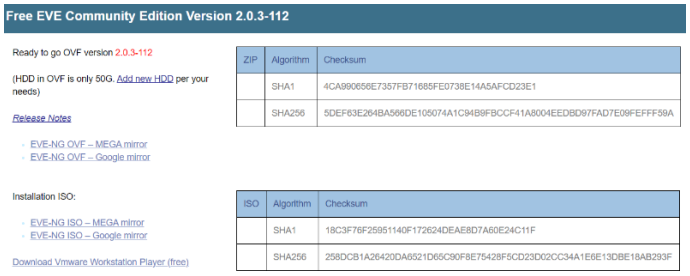
Жасалған жұмыстар ақпараттық қауіпсіздік саласына қызығушылар үшін өз біліктілігін көтеруге септігін тигізетініне сенімдіміз.

Emulated Virtual Environment - Next Generation (Eve-NG) - жетекші әлемдік өндірушілердің желілік жабдығы мен бағдарламалық қамтамасыз етуі бар толыққанды виртуалды зертхананы құруға мүмкіндік беретін келесі буынның эмуляцияланған виртуалды ортасы. Eve-NG сізге виртуалды құрылғылармен, желілерді құрумен, нақты жабдықпен жұмыс жасауға арналған құралдар жиынтығын береді. Бұл өнімнің мүмкіндіктері жабдықты пайдалануды, басқаруды, коммутацияны жеңілдетеді. Сонымен қатар, зерттеу топологияларымен, тұжырымдамалармен бөлісу, жай зертханалық жұмыстарды жасау, өндірістік міндеттерді дайындауға және шешуге кететін қаржылық, уақыттық шығындарды азайтуға мүмкіндік береді [1].

Eve-NG эмуляторын Windows немесе Linux жүйелеріне, сондай-ақ виртуалды Hyper-V, VMware және VirtualBox машиналарына орнату жолдары өнімнің арнаулы сайтында берілген [2].

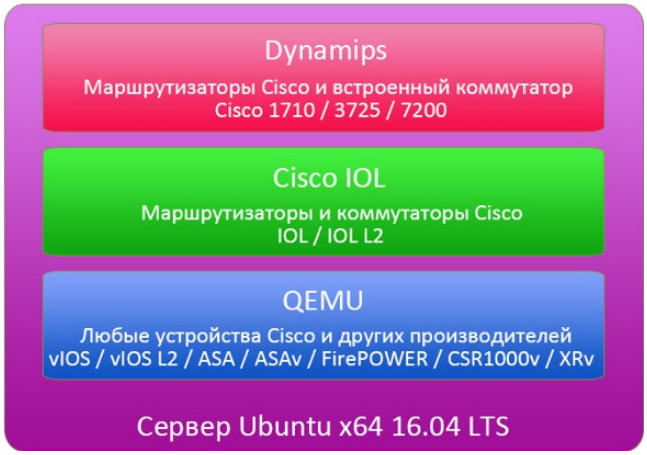
1 сурет. Эмулятор артықшылықтары [2]

Эмуляторды орнату барысында қажетті нұсқаны таңдау жолдары 2 суретте берілген.



2 сурет. Ақысыз нұсқалар [2]

Браузердің көмегімен Сіз визуалды режимде желілік топологияларды жасай аласыз, оның ішінде әртүрлі өндірушілер, эмуляцияланған құрылғыларды іске қосуға, оларға консольмен қосыла аласыз, сонымен қатар, Eve-NG есептеу ресурстарын бақылауға мүмкіндік бар. Eve-NG эмуляцияның үш негізгі ішкі жүйесін қамтиды: Dynamips, QEMUCisco, IOL (3 сурет).



3 сурет. Eve-NG архитектурасы

Эксперименталды бөлімде біз келесі мәселелерді қарастырдық:

- корпоративтік инфрақұрылым құру;
- серверлерді, машиналарды, желілік жабдықтарды және олардың байланыстарын конфигурациялау;
- корпоративтік инфрақұрылымға желілік шабуылдарды ұйымдастыру [3].

Бізге қажетті қарапайым инфрақұрылым – үш операциялық жүйеден: Kali, Windows7, Windows10; екі коммутатордан (switch), желіаралық экраннан (pfsense) және интернет желісінен (Internet) тұратын құрылым болып табылады. Негізгі мақсат –желілік жабдықтарды конфигурациялау.

Eve-NG платформасына келесі құрылғыларды жүктейміз:

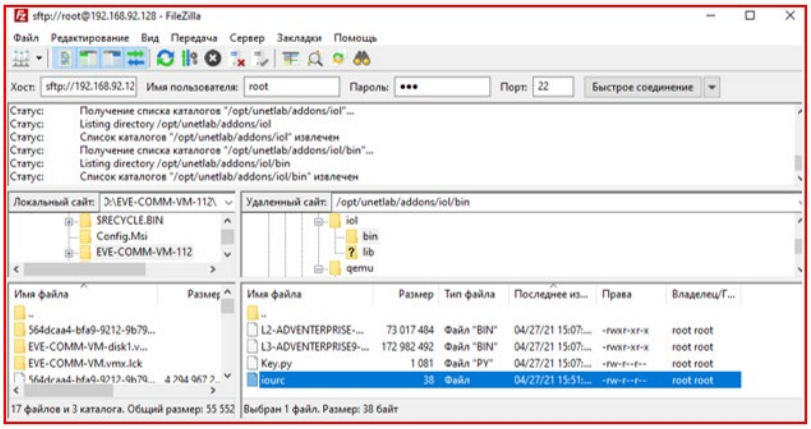
✓ CISCO IOL (switch, router);
✓ KALI-LINUX *iso немесе *vmdk;
✓ WINDOWS-7 ULTIMATE *iso немесе *vmdk;
✓ PFSENSE;
✓ Eve-NG Windows Client Side.

Eve-NG-да жұмыс жасау үшін ең алдымен Windows Client Side пакетін орнатамыз, мысалы, putty немесе ultravnc (4 сурет).

4 сурет. Eve-NG Windows Client Side бөлімі

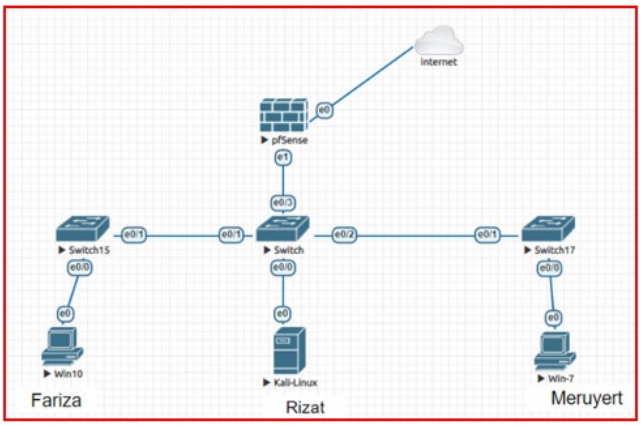
FileZilla*SFTP қосымшасын орнатамыз және хостқа Eve-NG IP адресін: 192.168.92.128, қолданушы аты: root , құпия сөз: eve, порт номері: 22 (SFTP байланыс орнату үшін қажетті порт) енгізе отырып виртуалды машинаға қосыламыз [4-6].

«Удаленный сайт» бөлімінде /opt/unetlab/addons/iol/bin файлына кіріп «Локальный сайт» бөлімінен қажетті файлды көшіреміз және Eve-NG-да коммутатор, роутер құрылғыларын қолдана аламыз (5-сурет).



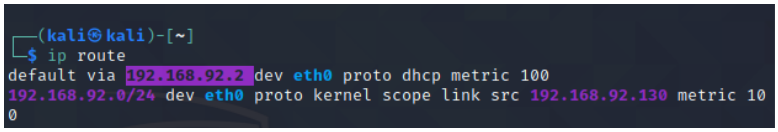
5-сурет. Cisco iol файлын қосу

Kali-Linux, Windows 7 және брандмауэрді Eve-NG –да қолданып, жүктейміз (6-сурет).



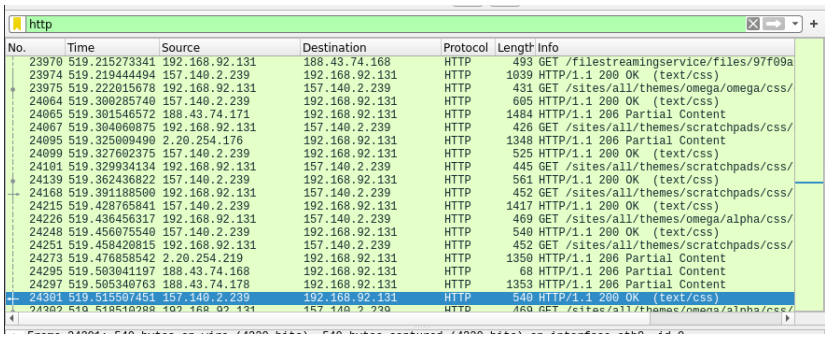
6-сурет. Эксперименталды инфрақұрылым

Келесі кезекте Kali арқылы ARPSPOOF енуін іске асырамыз. Осы мақсатта Kali терминалына - root атынан қосыламыз. Терминалда ip route командасын жазу арқылы eth0 интерфейсін анықтаймыз (7-сурет).



7-сурет. Интерфейсті анықтау

Windows10 – да Http сұраныстарын тізім ретінде де көре аламыз, яғни нақты қандай веб-беттерге кіргеніміз көрініп тұрады (8-сурет).



8-сурет. Http сұраныстарының тізім ретінде көрінісі

Орындалған жұмыстар негізінде корпоративтік инфрақұрылымға желілік шабуылдарды ұйымдастыру жүзеге асырылды [4-6].

Қорыта келгенде, Eve-NG-де желілік инженерлерді даярлау үшін барлық қажетті құралдар қамтылған. Eve-NG-ді қолдана отырып күрделі виртуалды зертханаларды құруға мүмкіндік бар. Бұл ретте әрбір студент үшін зертхана жеке эмуляцияланады. Физикалық жабдықта әрбір студент үшін осындай зертханалық стендтерді қалыптастыру іс жүзінде мүмкін емес.

Eve - NG Pro негізгі мүмкіндіктері:

* Қол жеткізуді рөлдер бойынша бөлу;
* Зертханаға нақты Интернет арнасын қосу;
* Әр түрлі қолданушылардың зертханалары арасында желілерді біріктіру;
* Түйіндер арасындағы байланыс арналарының сапасын реттеу;
* Wireshark интеграциясы;
* Docker контейнерлерін қолдау;
* Әкімшілерді пайдаланушылардың консольдік сессияларына қосу мүмкіндігі;
* Конфигурацияларды түйіндерден конфигурациялар жиынтығына экспорттау;
* Web интерфейсі арқылы жұмыс.

Eve-NG ақпараттық технологиялар саласындағы барлық қолданушыларға пайдалы. Бұл ірі компанияларға, оқыту орталықтарына, провайдерлерге, интеграторларға, жаңа білім алғысы келетін қызығушылар үшін қажетті болатыны сөзсіз.

Әдебиеттер:

1. U. Dzerkals. EVE-NG Professional Cookbook, Version 4.11.

2. EVE-NG Professional Edition. - https://www.eve-ng.net (29.04.2021)

3. Онлайн Лаборатория EVE-NG проекта LearnCisco.Ru, Версия v1.1, 2018. - Онлайн Лаборатория EVE-NG проекта LearnCisco.Ru (29.04.2021)

4. Установка EVE-NG в VMware - 2 способа - https://www.youtube.com/watch?v=qP40VDqFF0M&t=309s (08.05.2021)

5. Установка образов Linux на EVE-NG [Развертывание EVE-NG] - https://www.youtube.com/watch?v=b0weYW5d-X0 (09.05.2021)

6. Create own Linux host image (eve-ng.net) - https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image (10.05.2021)

АУДИТ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Усатова О.А.[1,2], Адилев Е.С. [1]
e-mail: uoa_olga@mail.ru, adilev_yerlan@live.kaznu.kz
[1]Казахский Национальный Университет им. Аль – Фараби, Алматы, Казахстан
[2]Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Безопасности мобильных приложений имеет очень большое значение, так же как и то, что требования к ним в современно мире постоянно меняются. В статье рассмотрено воздействие безопасности на архитектуру, разработку и менеджмент, мобильных приложений то есть программного обеспечения, которое работает на мобильном телефоне. Ввиду того, что мобильные приложения работают на онлайн-устройствах, требуется защита кибер-безопасности. Безопасность мобильных приложений от начальной стадии планирования и проектирования до его обслуживания после запуска, будут проанализированы потенциальные угрозы безопасности мобильного приложения, а также будут предоставлены возможные способы устранения и решения этих проблем.*

Ключевые слова*: Безопасность мобильных приложений, аудит безопасности мобильного приложения, архитектура безопасности мобильного приложения, безопасность и конфиденциальность, ,мобильные устройства на платформе Андройд, мобильные приложения.*

Вступление

С появлением беспроводной технологии 5G мобильные приложения сделали повседневную жизнь гораздо более удобной, чем раньше. Мобильные приложения проникли практически во все сферы нашего общества (Образование, медицина, строительство и тд). Однако с развитием мобильных приложений их безопасность требует большого внимания. В случае если мобильное приложение подвергается атаке из-за того, что архитектура программного обеспечения содержит уязвимость, что в дальнейшем может привести к значительным потерям. Разработчики мобильных приложений несут ответственность за безопасность разработки программного обеспечения, и его задача обеспечить безопасность качества мобильных приложений.

Угроза безопасности мобильных приложений

Платформа Android стала самой распространенной операционной системой (ОС) для мобильных телефонов и планшетов. Ей принадлежит более 71% рынка. В настоящее время зарегистрировано более 3 миллионов приложений (рис 1.). Открытый исходный код ОС Android, разнообразие (неофициальных) платформ для приложений и легкость с помощью которых можно создавать эти приложения, все это повлияло на популярность этой ОС, но эти особенности также повлияли на ее аспекты безопасности. В случае взлома, информация может быть выпущена в сеть, что приведет к большим потерям. Доступность личной информации и увеличившаяся денежная выгода привлекла вредоносное ПО разработчикам причинять вред, создавая трояны, ботнеты, шпионское ПО и другие подобные вредоносные программы для Android.

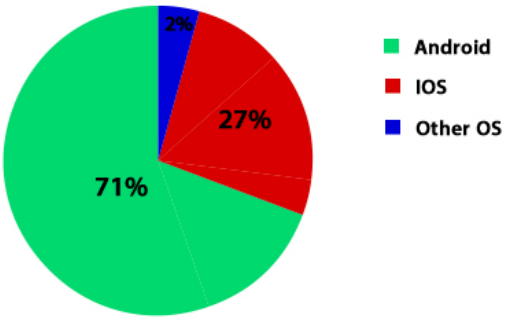


Рисунок 1- ОС мобильных приложений на 2021 г.

Для обычных пользователей мобильных приложений важны качество, удобство, безопасность и надежный сервис – это основные вещи на которые смотрит пользователь [1,2,3] Текущие тенденции ориентированы на пользователя. Основная задача разработчиков мобильных приложений заключается в том, чтобы их разработка удовлетворяла потребности пользователей. Архитектура мобильного приложения ограниченна мобильной системой: с одной стороны, разработчик не может делать все как хочет из-за ограничений, с другой стороны, это ограничение защищает безопасность мобильной системы.

Проверка на безопасность мобильных приложений

С развитием мобильных приложений возросли так же случаи атак на них, особенно в мобильных приложениях на платформе Android, которые будет рассмотрено позже. Потенциал риска безопасности мобильных приложений, связанный с высокой эпохой технологий, со смартфонами, планшетами и т. д. умный мобильные устройства становятся популярным, люди постепенно привыкают к онлайн-сервисам. С большим приростом количества приложений, приложения могут столкнуться с такими угрозами, как «Троянский конь», различные вирусы, несанкционированное изменение данных, фишинг, кража идентификаторов, SMS-троянцы, мобильное рекламное ПО, вредоносное ПО и так далее. Киберпреступник может внедрять вредоносные программы, а вредоносная программа может: повредить систему, украсть конфиденциальные данные, удаленный контроль, киберзапугивание, кибер-преследование, кибер-мошенничество, кибер-чит и так далее. Она может прямо или косвенно повлиять на пользователя, чтобы тот мог причинить вред другим пользователям [2] Поскольку опытные злоумышленники могут легко найти уязвимость и использовать ее, не будучи обнаруженным. Разработчики мобильных приложений должны знать, как работают атаки на приложения, и уметь создавать программные средства защиты от них у себя в приложениях.

Недостатки мобильного приложения. Из-за некоторых нерешенных проблем с безопасностью качество службы мобильных приложений может сильно пострадать. Рассмотрим несколько таких примеров:

- Появление аномальных исходов, в результате чего мобильное приложение не может работать стабильно
- Скорость работы, и объем памяти замедляют работу приложения.
- Не доступность сервера или ошибка на серверной части.
- Ошибка при предоставлении услуг внутри приложения.

Тестирование мобильного приложения обязательно должно включать тестирование безопасности.

Угрозой в безопасности мобильного приложения может быть:

- Раскрытый исходный код.
- Открытость платформы Android.
- Разработанная поддержка пользовательского интерфейса UI имеет скрытые уязвимости

Обеспечение безопасности - задача разработчиков приложений.

Причина проблем

На начальном этапе разработки, если разработчик мобильного приложения не принял во внимание угрозу безопасности достаточно серьезно, в дальнейшем это может повлиять на архитектуру безопасности всего мобильного приложения [4].

Архитектура мобильного приложения. На этапе проектирования, архитектура безопасности мобильного приложения должна учитывать многие аспекты кодирования. Основные два типа безопасности мобильных приложений это: погрешность и брак. Погрешности безопасности - обычно бывают тогда, когда не рассматриваются все возможности и вариации ошибок. Этот вид проблемы можно легко найти и очень быстро решить [5] Погрешности безопасности мобильных приложений могут быть более серьезными. Они могут быть проблемой функциональной архитектуры приложения на ранней стадии разработки, а не только вопрос программного кода.

Источник проблем с безопасностью мобильных приложений. Поскольку большинство мобильных приложений представляют собой дополнительные услуги (VAS), то есть используют сторонние приложения или платформы, возникает риск безопасности, что может привести к финансовым потерям, потерь в бизнесе или угрозы интеллектуальной собственности и т. д. Есть вероятность, что может произойти злоумышленная атака. Другая возможная ошибка – это ошибки в мобильном приложении, которые не были обнаружены при разработке программного обеспечения, архитектуре, программировании, тестировании и в период эксплуатации. В итоге мобильное приложение становиться не безопасным. Эти ошибки могут быть вызваны не соблюдением строгих правил безопасности программного обеспечения во время разработки мобильного приложения; или методология кодирования не была правильно подобранна. Еще одна возможность – это то, что тестирование мобильного приложения не было выполнено должным образом. Это также может быть связано с любым изменением требований к мобильному приложению, с игнорированием требований потенциальных угроз безопасности. Более того, непредсказуемость проблем безопасности мобильного приложения, такие как упрощенные функции мобильного приложения, вывод, состояние рабочей среды, ожидаемый ввод, интерактивные компоненты и т. д. так же могут быть потенциальной угрозой безопасности [6].

Безопасность при программировании мобильных приложений

Безопасный жизненный цикл мобильного приложения должен быть гарантирован разработчиками мобильных приложений. Обязательно должно проводиться тестирование безопасности мобильного приложения. Если позволяют условия, нужно провести профессиональное ручное тестирование безопасности мобильного приложения. Эксперт по безопасности должен объяснить мобильному разработчики приложений характеристики оценки безопасности, точки оценочного осмотра, подробности оценки по каждому случаю, предложения по исправлению перед тестированием безопасности.

Текущая тенденция дизайна (UX/UI) продукта ориентирована на пользователя. То же самое и с мобильными приложениями. Центрированная безопасность пользователя

мобильного приложения включает: безопасность памяти. Может классифицироваться как: безопасность в онлайн-программировании, управление приоритетами, удаленное использование и безопасность каждого элемента [2] Есть три этапа в дизайне и разработке мобильных приложений:

Стратегия и анализ пользователей. Что включает в себя: описание профиля пользователя, ожидания пользователей, список требований и анализ, определение цели дизайна. Разработать иерархическую структуру, как для пользовательских, так и для коммерческих целей.

Оценить: емкость, удобство использования, производительность, надежность, возможность установки и обслуживания.

Дизайн и определение качества.

Разработка оригинального дизайна включает в себя:

- Объектное моделирование прототипа различной лояльности
- Пользовательское тестирование и экспертная оценка.

Реализация и определение качества. Оценить: вместимость, удобство использования, производительность, надежность, возможность установки и обслуживания, удовлетворенность документацией.

Тестирование безопасности мобильных приложений. Перед запуском мобильного приложения существует много разных типов тестирования. Например, тестирование черного ящика и тестирование белого ящика. Что еще более важно, необходимо провести тестирование безопасности мобильных приложений на относительно ранней стадии жизненного цикла разработки приложения.

Улучшение тестирования безопасности мобильных приложений. Основной целью тестирования безопасности мобильного приложения выяснить, есть ли ошибки в программном обеспечении приложения. Что касается безопасности мобильного приложения, может быть проведен тест на проникновение, чтобы выяснить, работает ли архитектура безопасности. Это тестирование является процессом попытки получить доступ к ресурсам без знаний имен пользователей, паролей и других обычных средств доступа [2,5] Если упор делается на мобильные ресурсы, то примеры успешных проникновений – это получение конфиденциальных документов, прайс-листы, базы данных, личные данные пользователя, данные о конфиденциальности и другая защищенная информация.

Оценка тестирования безопасности включает:

- Доступность ресурсов
- Безопасность конфиденциальной информации
- Функция защиты от реверс-инжиниринга
- Сертификаты аутентификации
- Сканирование уязвимостей.
- Имитационный тест, используя приложения на проникновение.

Для того чтобы повысить качество безопасности мобильного приложения, при разработке мобильного приложения, на этапе кодирования исходного кода, на этапе реализации тестирования и этапе передачи данных, должно быть выполнено приемочное тестирование безопасности. Это тестирование позволяет эффективно использовать анализ потока данных, механизм семантического анализа для проверки были ли в итоге доставлены данные. После тестирования уязвимости безопасности, и получении соответствующих результатов, должны быть представлены предложения по модификации, чтобы разработчики системы могли исправить исходный код.

Решение проблем

Решение проблем по защите мобильных приложений включает в себя: безопасность памяти, проблему переполнение буфера; безопасность угроз и безопасность процессов, таких как, решения для синхронизации, совместной работы и блокировки; и безопасность входных данных [6].

Рисунок 2. Фреймворк безопасности мобильного приложения

Разработчики приложений играют ключевую роль в создании мобильных приложений, безопасность в жизненном цикле разработке. Вначале на этапе разработки приложения разработчики должны провести аналитические тесты, для своевременного обнаружения дефектов и уязвимостей безопасности, уменьшить ненужные риски безопасности. Улучшения по безопасность мобильных приложений должны выполняться на этапе выпуска приложения, чтобы повысить интенсивность безопасности приложений и предотвратить любые попытки взлома. Обязательно должен быть круглосуточный мониторинг (с мобильного оператора сетевой системы) на этапе эксплуатации, для защиты законных прав и интересов пользователей от злонамеренных повреждений и кражи личных данных.

- Небезопасный ключ шифрования и слабый пароль
- Несанкционированный доступ к данным
- Ошибки, вызывающие уязвимость конфиденциальных данных
- Наличие бэкдора и опции отладки.

Как показано на рисунке 2, для периода разработки мобильного приложения безопасность вовлечена на каждом этапе, дизайна, кодирования, реализации и тестирования. Финальное тестирование перед запуском очень важно, это для того чтобы была гарантия качества. На самом деле существует более одного метода выполнения аудита безопасности мобильного приложения, аудит безопасности - больше важен при разработке мобильных приложений, можем только предложить фреймворк который можно использовать, и который является лишь одним из инструментов по внедрению аудита безопасности.

Выводы

Были исследованы незаурядные проблемы в безопасности мобильных приложений. Поскольку разработка мобильных приложений связана с разными операционными системами и многими языками программирования, безопасность в мобильных приложениях проблема довольно сложная. Тем не менее, рассмотрены основные проблемы безопасности на этапе разработки мобильных приложений, программировании, тестировании и менеджмента. Были проанализированы потенциальные угрозы безопасности приложения, также были предоставлены способы устранения и решения проблем. Данная исследовательская работа, применима лишь при ранней разработке.

Список литературы

1. Antoine Olivier, et al 2013. ISO/IEC 27018: The Future Standard for Personal Data Protection in Public Cloud, EBRC.

2. Feng, X. and Zhang X. 2015. Personally Identifiable Information Security in Cloud Computing. International Conference on Computing and Technology Innovation, UK.

3. ICO .2016. Overview of the General Data Protection Regulation (GDPR).https://ico.org.uk/for-organisations/data-protection-reform/overview-of-thegdpr/ (Accessed 14/3/2017)

4. Anderson R. .2008. Security Engineering. 2nd Ed. Wiley,

5. Feng, X, and Conrad M. 2017. Security at the Design Stage. Accepted by ACE-2017, FL. USA.

6. Cole E. 2009. Network Security Bible. John Wiley & Sons; 2nd ed.

7. Aliyun. 2017. Mobile Security. https://cn.aliyun.com/product/mobsec

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ ҚАУІПТЕРІ ЖӘНЕ ОЛАРДАН ҚОРҒАНУ ҚАЖЕТТІЛІГІНІҢ МАҢЫЗДЫЛЫҒЫ

[1]Шайкулова А.А., [2,3]Калижанова А.У., [1]Искакова А.Т.,
[1,2]Козбакова А.Х., [4,5]Айткулов Ж.С.
e-mail: shaikulova_ak_al@mail.ru, kalizhanova_aliya@mail.ru, iskakova.1977@mail.ru
2 [1]Алматы технологиялық университеті, Қазақстан
[2]ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институты,Қазақстан
[3]Алматы энергетика және байланыс университеті, Қазақстан
[4]Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан
[5]Логистика және көлік академиясы, Қазақстан

Аңдатпа. *Мақалада ақпарат қауіпсіздігін қамтамасыз етудің Үкіметтік деңгейде көтерілуіне себеп болып отырған жағдаяттар талданады. Қазіргі қоғамда кең етек алып отырған әлеуметтік инженерия шаубуылдарына талдау жасалып, одан қорғанудың алғы шарттары ұсынылады.*

Кілттік сөздер: *Ақпараттық қауіпсіздік, Фишинг, әлеуметтік инженерия, DdoS шабуылдар, кибершабуылдар.*

2017 жылғы 12 желтоқсанда Қазақстан Республикасы Үкіметінің № 827 қаулысымен "Цифрлық Қазақстан" мемлекеттік бағдарламасы бекітілді». Мақсаты - Орта мерзімді перспективада цифрлық технологияларды пайдалану есебінен республика экономикасының даму қарқынын жеделдету және халықтың өмір сүру сапасын жақсарту, сондай-ақ республика экономикасының ұзақ мерзімді перспективасында Болашақтың цифрлық экономикасын құруды қамтамасыз ететін түбегейлі жаңа даму траекториясына бет бұру. Бағдарламаның негізгі міндеттері - халыққа көрсетілетін қызметтердің барлығын дерлік цифрландыру технологиясына көшіру. Осы бағытта халықтың цифрлық сауаттылығын арттыру және АКТ саласында ақпарат қауіпсіздігін қамтамасыз ету міндеттері анық көрсетілген.[1]

Бұған себеп те жоқ емес. Соңғы онжылдықта әлем цифрлық технологиялар оны қалыптастырудың негізгі құралына айналатын жаңа типтегі экономикаға бет бұруда. Қазіргі жағдайда ақпараттық технологиялар мен цифрлық трансформация технологиялық өзгерістердің негізгі факторы және барлық экономикалық және өндірістік процестерді қайта құруға, өнімділікті түбегейлі арттыруға, тауарлар мен қызметтердің сапасын арттыруға және өзіндік құнын төмендетуге әкелетін жекелеген кәсіпорындар деңгейінде де, елдер мен ұлттықтан жоғары бірлестіктер деңгейінде де бәсекеге қабілеттілікті қамтамасыз етудің шарты болып табылады.

Жеке және мемлекеттік секторлардың жұмысында ақпараттық технологиялардың рөлін кеңейту ақпараттық қауіпсіздік саласында кадрлар мәселесін тудырып отыр және бұл әлемдік мәселе болып табылады. Жыл сайын АҚ нарығы ондаған пайызға өсіп отыр, олай болса АКТ-ны қоғам өмірінің барлық салаларына енгізумен байланысты ақпарат қауіпсіздігіне төнетін қауіптердің де соншалықты көлемде өсіп отырғанын білдіреді.

Президенттің 2017 жылғы 31 қаңтардағы Қазақстан халқына Жолдауында Ел Президенті Үшінші жаңғырудың бесінші басымдығында киберқылмыспен, діни экстремизммен және терроризммен күрестің өзектілігін атап өтті. Мемлекет басшысының Жолдауында Үкімет пен Ұлттық қауіпсіздік комитетіне «Қазақстан киберқалқаны» тұжырымдамасын әзірлеу тапсырылды, оның мақсаты - ақпараттандыру және байланыс саласында қоғам мен мемлекеттің ақпараттық қауіпсіздігін қамтамасыз ету, сондай-ақ ақпараттық-

коммуникациялық инфрақұрылымды пайдалану кезінде азаматтардың жеке өміріне қол сұғылмаушылықты қорғау болып табылады, делінген болатын.

Бұл елімізде ақпарат қауіпсіздігіне төнетін қауіптер мәселесінің мемлекеттік деңгейде көтеріліп отырғанын білдіреді.

Ақпараттық қауіпсіздікті қамтамасыз етудің алғы шарты алдымен қауіп төнетін нысандарды анықтап алу, сонан соң оған төнетін қауіп түрлерін болжау. Қауіп төнетін нысандар – әрине, кез келген ақпараттық ресурс (ол қолданушының компьютері, мекеме сервері немесе желілік жабдықтар болуы мүмкін). Қауіптерді жүзеге асыру келесі әрекеттер мен оқиғалардың бірінің салдары болып табылады: құпия ақпаратты жария ету, құпия ақпараттың сыртқа байланыс арналары арқылы ағып кетуі және қорғалатын ақпаратқа рұқсатсыз қол жеткізу. Жария ету немесе ақпараттың сыртқа кетуі кезінде қол жетімділігі шектеулі ақпараттың құпиялылығын бұзуға әкеледі.

Сурет 1. Ақпаратты қауіпсіздікке себеп

Жариялап жіберу – қызметкерлердің қасақана немесе абайсызда құпия ақпаратты бөгде адамдардың қол жеткізуіне жағдай туғызуы.

Ағып кету - түрлі арналар бойынша ақпараттың сыртқа бақылаусыз таралып кетуі.

Рұқсатсыз қатынас құру - рұқсат етілмеген адамдардың КИ-мен заңсыз қасақана танысуы, қорғалған ақпараттың тұтастығы мен қол жетімділігін бұзу.

Жариялап жіберу және ақпараттың сыртқа ағуы қаскүнем тарапынан ең аз күш жұмсап, құпия ақпаратпен заңсыз танысуға алып келеді. Бұған компания қызметкерлерінің жеке кәсіби емес сипаттағы әрекеттері, яғни адами фактор ықпал етеді.

Соңғы кезде әлеуметтік инженериядан қауіп күшейіп тұр. KZ-CERT хабарламасы бойынша 2020 жылдың бірінші жартыжылдығында ақпараттық қауіпсіздіктің 8 300 инциденті анықталған. 2019 жылмен салыстырғанда фишингтік шабуылдар саны 25% - ға, ал DDoS шабуылдар саны 42%-ға артқан**.**

2020 жылдың бірінші жартыжылдығында ИҚБШ-ға қосылған телекоммуникация желілеріне 568,5 млн. шабуыл тіркелген. Бұл 2019 жылдың сәйкес кезеңімен салыстырғанда 4,8 есе көп.

KZ-CERT сарапшыларының пікірінше, себептердің бірі COVID-19 пандемиясымен байланысты жағдай болған. Азаматтардың табыс деңгейінің төмендеуіне байланысты зиянкестер күрделі емес сауалнамадан өту және ақшалай сыйақы алу ұсынылған фэйк Telegram-боттарын, сауалнама-сайттарды белсенді түрде таратып отырған. Алаяқтық схемалар зиянкестерге пайдаланушының деректерін иеленуге мүмкіндік беріп, соның ішінде банктік деректермен де аляқтық әрекеттер анықталған. KZ-CERT сарапшылары тіркеген оқиғалардың ішінде фишингтік шабуылдарға ұшырап, алаяқтықтың қақпанына түскен жайттар көп тіркелген, мысалы:

- Ағымдағы жылдың 5 қаңтарында Youtube-те таратылған фишингтік интернет-ресурс анықталған.

- 6 қаңтарда «Kaspi Bank» АҚ-нан сауалнама жүргізілген, шын мәнінде банк тарапынан ешқандай сауалнама жүргізілмегені дәлелденген.

- 10 қаңтарда төлем ресурсы түрінде жасырылған интернет-ресурс анықталған.

- Үстіміздегі жылдың 27 қаңтарында KZ-CERT қызметінің қызметкерлері Нұр-сұлтан қаласы әкімдігінің Instagram-дағы @akimat_nur_sultan аккаунтын қалпына келтіргенін мәлімдейді.

- Сәуір айында сауалнама сайттарымен және «үйдегі әлеуметтік табыс» фишингін тарату орын алған.

- Мамыр айында қазақстандықтар тегін сыйақы алу мүмкіндігін ұсынған компаниялардың әр түрлі акциялары туралы хабарламаларды жаппай ала бастаған фактілер тіркелген, Adidas атынан жіберілімдер қайталанған.

- Magnum Cash & Carry және DHL сауда-бөлшек сауда желісі атынан бірқатар фишингтік формалар таратылған.

- маусым айында Birtanov.e@dsm.gov.kz электрондық мекенжайдан зиянды фишингтік жіберілімдер таралған.

Ranking.kz сайт деректері бойынша ағымдағы жылдың қаңтар-тамыз айларында Қазақстанда 11 мың кибершабуыл тіркелген - өткен жылдың сәйкес кезеңімен салыстырғанда 23,4%-ға аз (14,4 мың кибершабуыл). Фишингтік шабуылдар қарастырылып отырған кезеңде ҚР—да 853 рет жасалған - бір жыл бұрынғыға қарағанда 12,1% - ға артық (761 кибершабуыл).

Сонымен қатар, DDoS шабуылдары санының айтарлықтай өскенін білдіретін фактылар жетерлік. Бұл ең көп таралған және қауіпті желілік шабуылдардың бірі болып табылатын қызмет көрсетуден бас тарту. Шабуыл нәтижесінде заңды пайдаланушыларға, желілерге, жүйелерге және өзге де ресурстарға қызмет көрсету бұзылады немесе толық бұғатталады. Ағымдағы жылдың сегіз айында осындай 206 кибершабуыл тіркелген — бұл өткен жылдың сәйкес кезеңімен салыстырғанда 39,2% - ға көп (148 шабуыл). Соңғы уақытта хакерлер шабуылдың бұл түрін шабуылды тоқтату үшін ақша талап етіп, бопсалау үшін қолдануда.[7] Төмендегі суреттегі Ranking.kz сарапшыларының құрастырған «Қазақстан республикасындағы қауіпсіздікке қарсы жасалған инциденттері санының өзгеріс динамикасы» жоғарыда аталған келеңсіз жайттардың қаншалықты дәрежеде орын алғандығының айғағы.

Сурет 2. KZ-CERT деректері негізіндегі Ranking.kz көрсеткіштері

Ағымдағы жылдың қыркүйек айында ақпараттық қауіпсіздік инциденттерінің қатарына ҚР мемлекеттік органдарының интернет-ресурстарының мониторингі барысында анықталған білім беру платформаларына бағытталған нысаналы DDoS-шабуылдар тіркелген. Оған kundelik.kz және bilimland.kz іліккен, - деп хабарлайды KZ-CERT. KZ-CERT қызметінің сарапшылары шабуылдар өзара байланысты және қашықтықтан оқыту кезеңінде жоғарыда көрсетілген білім беру порталдарының жұмысқа қабілеттілігін бұзуға бағытталған деген қорытынды жасаған.[8]

Сурет 3. KZ-CERT деректері негізіндегі Ranking.kz көрсеткіштері

Мұндай шабуылдарға тек жекелеген азаматтар емес, шағын және ірі компаниялар да ұшыраған, олардың кейбіреулерін алаяқтар торларына түсірген де.

Қарапайым қолданушы ақпарат қауіпсіздігіне төнетін қауіптерді, олардың сипаттамаларын білмеуі мүмкін. Ал, банктер немесе түрлі үкіметтік және үкіметтік емес кәсіпорындарда ақпарат қауіпсіздігін қамтамасыз ету шаралары қарастырылған. Соған қарамастан ақпаратқа қауіп төндіру фактілері орын алып отырған. Банктер тұтынушылары алдында өз имидждерін сақтау үшін мұндай оқиғаларды көп жариялай бермейді, дегенмен өткен жылы Каспий банкте шоттардың бұғатталып, бір күн клиенттердің банк қызметін қолдана алмағаны ақпарат көздерінде тараған болатын, бұл - факт.

Осындай орын алып отырған келеңсіз құбылыстарды қалай азайтуға болады (мүлдем жоқ қылу мүмкін емес), олардың алдын алау шаралары қандай?-деген сұрақтар туындаған жағдайда, мәселені шешудің бір жолы - ақпарат қауіпсіздігін қамтамасыз ету саласында мамандарды көптеп дайындау, олардың біліктілігін арттыру, үнемі тәжірибелерін жетілдіріп отыру механизмі. Қарапайым қолданушыларға ақпарат қауіпсіздігін қамтамасыз етудің жолдарын, әдістерін түсіндіру. Ал мекемелерде барлық жерде қызметкерлерге қойылатын талап бір, ол – АҚ қамтамасыз ету әдістерін, технологияларын білу. Ақпараттық қауіпсіздік талаптарын сақтамаған жағдайда өздерінің құқықтық жауапкершіліктерін білу.

Кәсіпорынның немесе компанияның қауіпсіздік мәслелерін кешенді қамтамасыз ету аса маңызды. Оның ішінде ақпарат қауіпсіздігіне жауапты мамандардың жауапкершіліктерін ұғындыратын, міндеттерін айқындайтын басқа да шаралар бар. Ол – жоғарыда мысалдар келтіріп өткен фишингке, яғни әлеуметтік инженерия шабуылдарына қарсы тұра білу.

Сонымен қатар, АҚ маманы әлеуметтік жауапты болуы керек: егер ол компанияның жұмыс процестерін жүзеге асырудағы ықтимал мәселені көрсе (ол оның тікелей қызметімен тікелей байланысты болмаса да), онда ол кем дегенде жолдауға жауапты қызметкерге өзінің күмәндері туралы хабарлауы керек. Кез-келген ықтимал мәселе нақты тәуекелдерге әкелуі

мүмкін. Егер бар тәуекелдер нақты емес болса және ешқандай әрекет жасалмаса, мәселені жоғары деңгейдегі көшбасшылық деңгейіне шығару керек

Зиянды бағдарламалық қамтамалар мен фишингтік интернет-ресурстардың өсуіне назар аудара отырып, мынадай ережелерді сақтық шарасы ретінде ұстану ұсынылады:

1. Егер сіз күдікті интернет-ресурстарға тіркемесі немесе сілтемесі бар белгісіз адресаттан хат алсаңыз, онда мұндай хаттарды елемеу керек немесе incident@kz-cert.kz мекен-жайына жолдау керек.

2. Белгісіз жіберушілердің күдікті хаттарында салынған файлдарды ашпау ұсынылады.

3. Қажетті бағдарламалық жасақтаманы тек ресми интернет-ресурстардан жүктеп алу, себебі ресми емес веб-беттер сияқты басқа сілтеме көздерін зиянды бағдарламаларды тарату үшін пайдалануға болады.

4. Жұмыс станциясында орнатылған бағдарламалық жасақтаманы қосымшалардан тікелей немесе бағдарламалық жасақтама әзірлеушілері ұсынатын құралдардың көмегімен жаңарту.

5. Сенімді антивирустық немесе тыңшылыққа қарсы бағдарламалық жасақтаманы қолдана отырып, ақпараттық қауіпсіздікке төнетін қауіп-қатерлерге операциялық жүйені үнемі тексеріп отыру өте маңызды.

6. Егер сіздің компьютеріңіз қазірдің өзінде жұқтырылған деп ойласаңыз, зиянды бағдарламаны автоматты түрде жою үшін антивирустық сканер немесе антивирустық бағдарламалық жасақтама арқылы сканерлеуді бастау ұсынылады.

Ең бастысы ақпараттық қауіпсіздікті қамтамасыз етудің заманауи шараларын зерттеп, тиімді қолдана білу қажет.

Қорытынды

Фишингтік шабуылдар жасау заңмен қудаланады. Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V Қылмыстық кодексінде (30.12.2020 ж. жағдай бойынша өзгерістермен және толықтырулармен) 7-тарау тұтастай ақпараттандыру және және байланыс саласындағы қылмыстық жауапкершіліктерге арналған.

Заң алдындағы жауапкершілікті сезіне отырып, Ақпаратқа қасақана рұқсатсыз қол жеткізу, оның мазмұнын бұрмалау, ұрлау, таратып жіберу сияқты заңсыз әрекеттер бүгінгі таңда әлеуметтік инженерия деп аталатын шабуылдармен жасалуда. Одан қорғану әр қолданушының өз қолында.

Әдебиеттер

1.Государственная программа «Цифровой Казахстан». https://zerde.gov.kz/activity/management-programs/the-state-program-digital-kazakhstan/

2. Проект Государственной программы «Цифровой Казахстан – 2020». http://primeminister.kz/ru/news/industrializatsiya/v-2017-godu-startuet-pervaja-pjatiletka-programmy-«tsifrovoj-kazahstan-2020».

3. Концепция информационной безопасности Республики Казахстан до 2016 года. Указ Президента Республики Казахстан от 14 ноября 2011 года № 174.

4. В.Н. Ясенев. Конспект лекций по информационной безопасности. http://www.iee.unn.ru/wp-content/uploads/sites/9/2017/02/konspekt-lektsij-po-IB.pdf

5. Под общей редакцией проф. Ясенева В.Н. Информационная безопасность: Учебное пособие..– Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. – 198 с.

6. Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V Қылмыстық кодексі (30.12.2020 ж. жағдай бойынша өзгерістермен және толықтырулармен) https://online.zakon.kz/document/?doc_id=31575252#pos=237;-96

7. Источник: Sputnik.kz, (новости источника) https://news.mail.ru/society/43576181/

8. Инциденты нарушения информационной безопасности. Январь–август 20207 http://www.ranking.kz/ru/a/infopovody/ostorozhno-kiberprestupniki-v-rk-zametno-uchastilis-fishingovye-i-ddos-ataki

9. https://www.tbforum.ru/blog/podgotovka-kadrov-po-ib-vzglyad-koda-bezopasnosti

10. https://habr.com/ru/post/306336/

11. https://news.mail.ru/society/43576181/

12. http://primeminister.kz/ru/news/industrializatsiya/v-2017-godu-startuet-pervaja-pjatiletka-programmy-«tsifrovoj-kazahstan-2020».

13.https://bluescreen.kz/digital-kazakhstan/v-kazahstane-snova-uvelichilos-kolichestvo-kiberatak/

УМНОЖИТЕЛИ ПОЛИНОМОВ ПО МОДУЛЮ ДЛЯ КРИПТОСИСТЕМ НА БАЗЕ НПСС

[1]Калимолдаев М.Н., [1]Тынымбаев С.Т.
e-mail: s.tynym@mail.ru
[1]Институт информационных и вычислительных технологий КН МОН РК, Казахстан

Аннотация. *Рассматриваются схемные решения для аппаратной реализации умножителей полиномов по модулю неприводимых полиномов, которые могут быть базовыми блоками при построении криптосистем на основе непозиционной полиномиальной системы счисления. В таких умножителях двоичное изображение полинома-множимого могут служить фрагментами шифруемого текста, а двоичное изображение полинома-множителя является секретным ключом. Модулем служит двоичное представление неприводимого полинома этих двух полиномов.*

Ключевые слова: *непозиционная полиномиальная система счисления, формирователь частичных остатков, сумматор по модулю два, неприводимые полиномы, матричная и конвейерные умножители.*

Введение. На базе непозиционных полиномиальных систем счисления (НПСС) можно построить быстродействующее устройство для шифрования и расшифровывания данных. Это объясняется тем, что НПСС относится к системе остаточных классов [1], где число А представляется в виде последовательных остатков или вычетов, полученных делением числа А на заданные положительные простые целые числа P1, P2, … , Pn, которых называют основаниями системы. Основным преимуществом такой системы счисления заключается в отсутствии переносов между остатками при выполнении различных арифметических операции над одноименными остатками по их основанию. Это дает возможность параллельно обрабатывать данные по каждому из основания, что существенно ускоряется процесс вычисления.

Однако, если остатки и основания системы представляются в позиционной системе счисления, то при выполнении арифметических операций над одноименными остатками будут вырабатываться внутренние межразрядные переносы, что замедляет процесс вычисления. Для устранения последнего недостатка в работах [2-4] предлагается обрабатываемые остатки и основания системы представлять полиномами, а в качестве основании (модуля) выбирать неприводимые полиномы. При этом полиномы обрабатываются по правилам модулярной арифметики. В такой системе счисления обработка полиномов по каждому основанию (модулю) и внутри модуля выполняются параллельно.

Криптосистем на базе НПСС можно реализовать программно, программно-аппаратно и аппаратно. Главным преимуществом программно-аппаратной и аппаратной реализации является быстродействие.

Центральным блоком криптосистемы при аппаратной реализаций являются умножители полиномов по модулю неприводимых полиномов, посредством которых осуществляются скоростное шифрование и расшифровывание данных.

В работах [5-7] были рассмотрены умножители полиномов по модулю последовательного действия и умножители полиномов по матричной структуре.

Умножитель полиномов по модулю последовательного действия

Основная идея ниже рассматриваемых умножителей состоит в том, что на каждом шаге умножения удвоенный предыдущий частичный остаток ($2r_{i-1}$) приводится по модулю P(x), формируя следующий частичный остаток r_i. Затем частичный остаток r_i логический умножается на младший бит b_i полинома-множителя B(x) и суммируется по модулю 2 с предыдущим промежуточным остатком R_{i-1}, формируя промежуточный остаток R_i. Число таких шагов определяется числом битов в двоичных представлениях полинома-множителя.

На рисунке 1 приведена функциональная схема умножителя полиномов по модулю последовательного действия. В состав устройства входит блоки логических схем $И_3 \div И_{10}$, регистр сдвига на один разряд вправо РгВ, регистр неприводимого модуля РгР, накапливающий формирователь частичных остатков (НФЧО), а также накапливающий сумматор по модулю два НСМ М2. В состав устройства также входят схемы, обеспечивающие управлением выполнения операций: элементы задержки ЭЗ.1, ЭЗ.2 и ЭЗ.3, триггер Т, вычитающий счетчик тактовых сигналов СчТИ, логическая схема $И_1$ и блок логических схем $И_2$.

РгВ служит для хранения множителя в виде двоичных коэффициентов полинома B(x), а РгР - двоичных коэффициентов полинома неприводимого модуля. НФЧО формирует частичный остаток r_i путем приведения по модулю P(x) удвоенного предыдущего частичного остатка $2r_{i-1}$. В НСММ2 формируются и временно хранятся промежуточные остатки R_i и результат вычисления $R=[A(x)\times B(x)]\mathrm{mod}P(x)$.

На рисунке 2 приведена структура НФЧО, который состоит из сумматора по модулю два (СММ2); мультиплексора MS, в состав которого входит инвертор НЕ, блоки схем И'1, И'2 и блок ИЛИ'1. ФЧО снабжен регистром частичного остатка РгЧО.

На рисункуе 3 приведена структура НСММ2, который состоит из сумматора по модулю 2, блока схем ИЛИ, выходы которого подаются на входы регистра промежуточного остатка РгR. На входы блока ИЛИ также подается значение r_0. В $РгR_i$ формируется R_i путем сложения по модулю 2 значений частичного остатка r_i с предыдущим значением промежуточного остатка R_{i-1}.

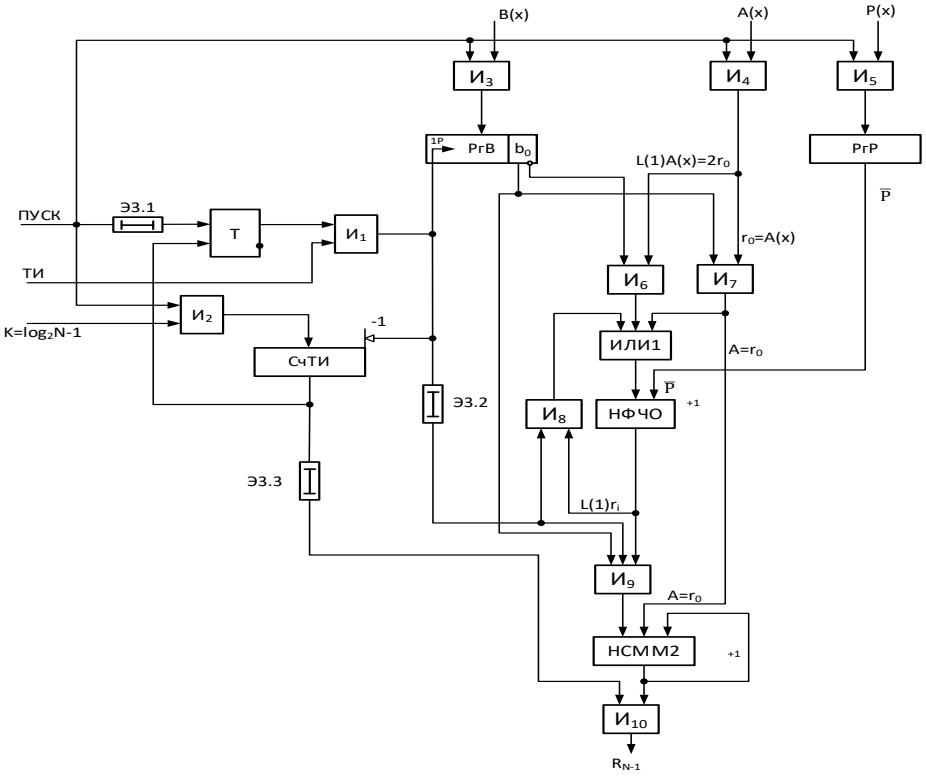


Рисунок 1. Функциональная схема умножителя полиномов по модулю последовательного действия с анализом младших разрядов множителя

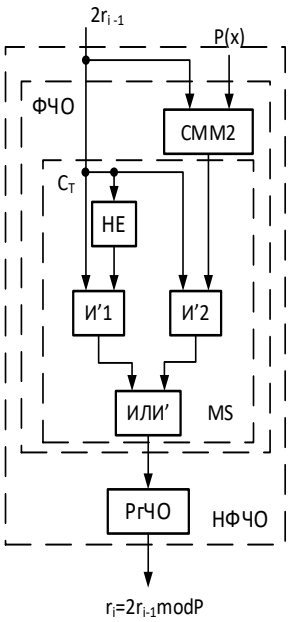


Рисунок 2. Состав ФЧО с регистром РгЧО

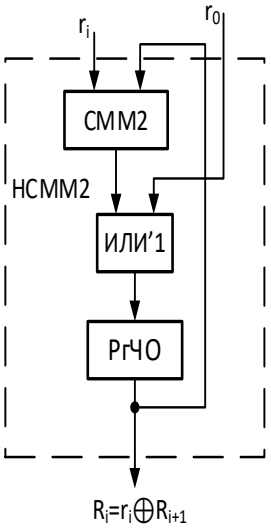


Рисунок 3. Структура формирователя промежуточного остатка на НСММ2

Матричная схема умножителя полиномов по модулю неприводимого полинома

В матричном умножителе полиномов по модулю выполняется за N-1 этапов по числу разрядов множителя. Каждый этап состоит из трех подэтапов. В первом подэтапе вычисляется частичный остаток r_i путем приведения удвоенного предыдущего частичного остатка $2r_i$ по модулю, т.е. $r_i=2r_{i-1} \mathrm{mod} P$. На втором подэтапе частичные остатки r_i логический умножаются на соответствующие биты b_i множителя начиная с младшего разряда. На третьем подэтапе формируется промежуточный остаток R_i путем приведения по модулю суммы $(r_i*b_i)+R_{i-1}$ по модулю.

На рисунке 4 приведена структурная схема матричного умножителя полиномов по модулю неприводимого полинома, где умножение начинается с анализа младших разрядов полинома-множителя со сдвигом частичных остатков на один разряд в сторону старшего разряда. Умножитель состоит из четырех блоков: 1 – блок это блок регистров, в состав которого входит регистр модуля P(x) и регистр множителя B(x), блок ФЧО 2 ($\Phi\text{ЧО}_1 \div \Phi\text{ЧО}_{N-1}$), блок схем И 3 ($И_1 \div И_{N-1}$), блок сумматоров по модулю два ($\text{СММ2}_1 \div \text{СММ2}_{N-1}$), линий задержки 5.

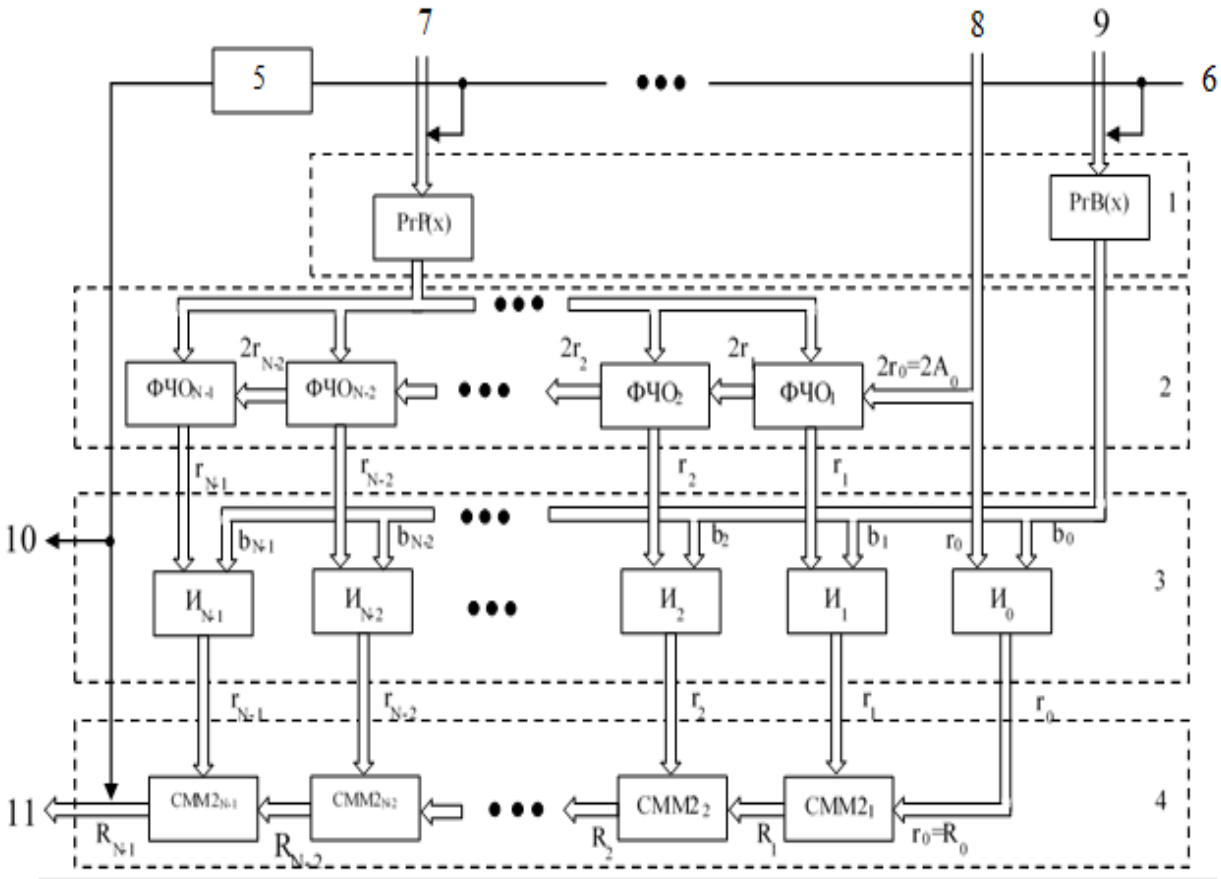


Рисунок 4. Структурная схема матричного умножителя полиномов по модулю неприводимого полинома

Конвейерный умножитель полиномов по модулю неприводимого полинома

При конвейерной организации весь процесс умножения полиномов по модулю разбивается на последовательность законченных шагов. Каждый из этапов процедуры умножения полиномов выполняется на своей ступени конвейера и эти ступени работают одновременно. Результаты, полученные на i-й ступени, передаются в (i+1) -ю ступени для дальнейшей обработки. Передача информации со ступени на ступень происходит через буферную память, которая размещается между ними.

Ступень, выполнившая свою операцию, запоминает результат в буферную память и может приступить к выполнению следующей порции данных операции, в то время как очередная ступень конвейера в качестве исходных использует данные, хранящиеся в буферной памяти на ее входе. Синхронность работы ступеней конвейера обеспечивается тактовыми сигналами, период которого определяется самой медленной ступенью конвейера и задержкой в элементе буферной памяти (рис. 5).

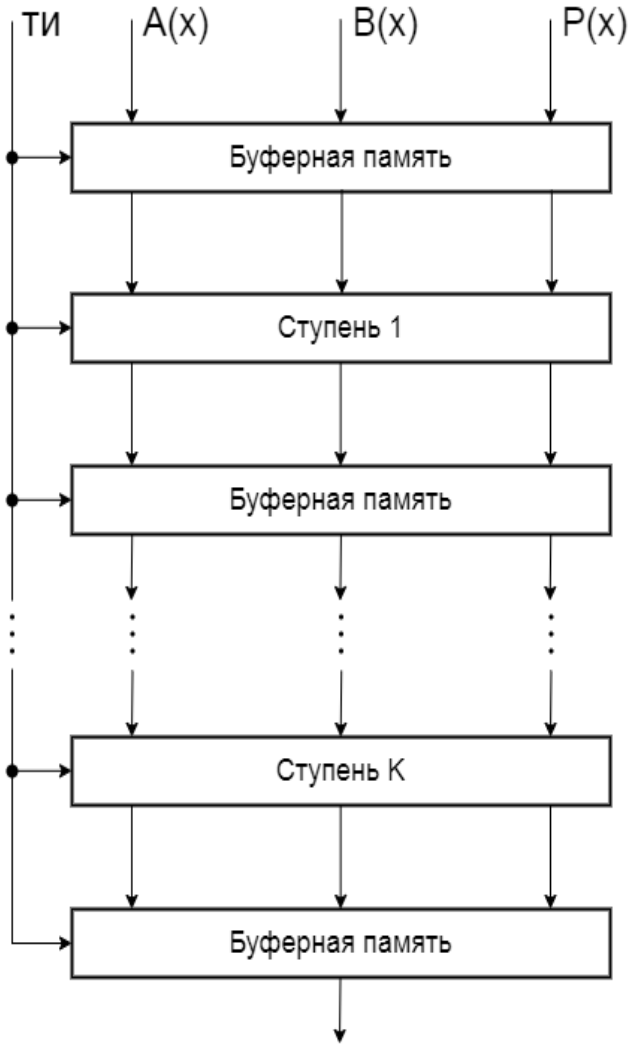


Рисунок 5. Структурная схема конвейерного умножителя

В конвейерном умножителе, состоящий из N ступеней операнды, участвующие в операции умножения могут подаваться на вход с интервалом N раз меньшим, чем в случае без конвейерного умножения.

На рисунке 6 приведена схема N-ступенчатого конвейера для умножения полиномов $A^1(x)$ и $B^1(x)$ по модулю неприводимого полинома $P^1(x)$, где умножение начинается с анализа младшего разряда. В процессе умножения в каждом такте коэффициенты полиномов $B^1(x)$, $B^2(x)$, …, $B^k(x)$ принимаются в N разрядный входной регистр РгВ(х). Двоичные коэффициенты неприводимых полиномов-модулей $P^1(x)$, $P^2(x)$, …, $P^k(x)$ принимаются в входной регистр РгР(х). Двоичные коэффициенты полиномов $A^1(x)$, $A^2(x)$, …, $A^k(x)$ в каждом такте принимаются в регистр множимого РгА(х).

Первая ступень конвейера состоит из блока схем И1, формирователя частичного остатка PRF.1 и буферных регистров РгВ(х).1, $Ргr_0$ и $РгR_0$.1, которые являются буферными регистрами I-ступени конвейера. Управляющий вход блока схемы И1 связан с младшим разрядом РгВ(х), где хранится младший разряд двоичных коэффициентов полиномов множителя В(х). Информационные входы блока схем И1 связаны с выходами регистра РгА(х) откуда тактовыми сигналами поступают двоичные коэффициенты полиномов $A^1(x)$, $A^2(x)$, …, $A^k(x)$. Удвоенные значения двоичных коэффициентов полиномов $2A^1(x)$, $2A^2(x)$, …, $2A^k(x)$ связаны со входами формирователя частичного остатка PRF.1. Другие входы PRF.1 связаны с выходами регистра РгР(х). Выходы регистра РгВ(х) также связаны со регистром РгВ(х).1. Выходы PRF.1 связаны с регистром $Ргr_1$. Выходы регистра РгР(х) также связаны со входами регистра РгР(х). Выходы блока схем И1 связан с регистром $РгR_0$ первой ступени.

Вторая ступень конвейера содержит блоки И2, PRF.2 и сумматор по модулю два (AddM2.1), буферных регистров II-ой ступени: РгВ(х).2, $Ргr_2$, РгР(х), $РгR_1$.

Управляющие входы блока схем И2 связаны с младшим разрядом регистра РгВ(х).1, а информационные входы блока схем И2 связаны с выходом $Ргr_2$.

Первые входы PRF.2 связаны также с выходами регистра $Ргr_2$. Вторые входы PRF.2 связаны с регистром РгР(х). Выходы блока схем И2 связаны с первыми входами AddM2.1. Вторые входы AddM2.1 связаны с выходами регистра $РгR_0$. Выходы регистра РгВ(х).1 связаны со входами буферного регистра РгВ(х).2, а выходы PRF.2 связаны с буферным регистром $Ргr_2$, выходы буферного регистра I-ступени РгР(х) связан буферным регистром РгР(х) второй ступени. Выходы сумматора по модулю два AddM2.1 связан со выходами регистра $РгR_1$ второй ступени.

Аналогичные блоки И, PRF, AddM2 и связи имеются в других ступенях конвейера. Исключением является N-ступень, где имеются блок логических схем И.N-1 и AddM2.N-1 и буферный регистр N-ступени – РгR.

На управляющий вход блока схем $И_{N-1}$ подается из регистра РгВ(х).N-1 старший разряд двоичного коэффициента множителя В(х) – b_{N-1}, на информационный вход подается частичный остаток r_{N-1} с выхода регистра $Ргr_{N-1}$.

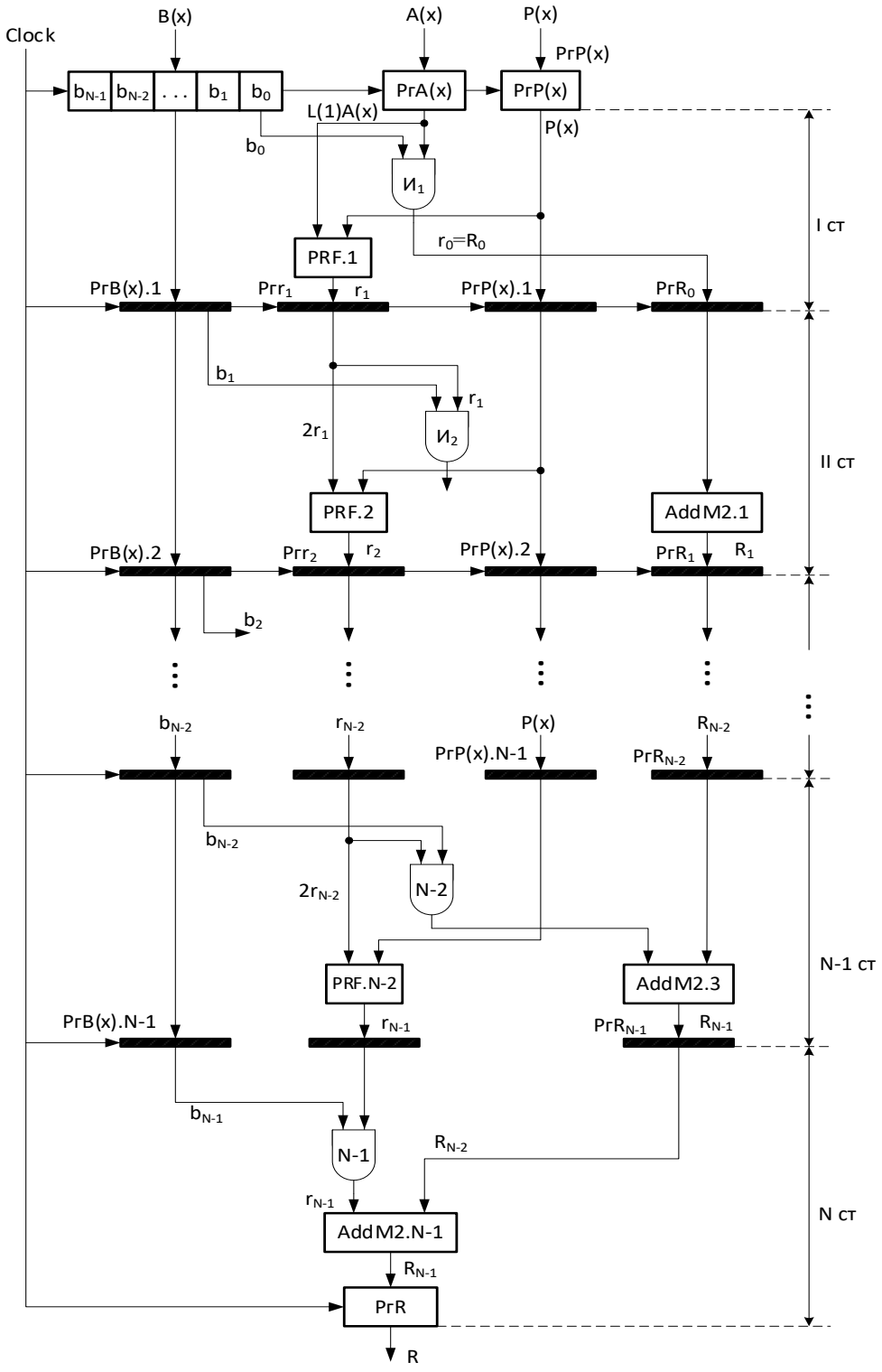


Рисунок 6. Конвейерный умножитель полиномов по модулю, где умножение начинается с анализа младших разрядов полинома-множителя

Выходы $И_{N-2}$ связан с первыми входами AddM2.N-1. Вторые входы связаны с выходами буферного регистра PrR_{N-2} N-1 ступени. Выходы AddM2.N-1 связаны с буферным регистром N-ступени PrR.

Логическими блоками ступеней конвейера является формирователи частичных остатков PRF и сумматоры по модулю два AddM2. Функциональная схема PRF приведена на рисунке 7 схема служит для формирования частичного остатка r_i-ой удвоенного значения от предыдущего частичного остатка r_{i-1} по модулю P(x). Удвоенное значение предыдущего остатка $2r_{i-1}$ получим путем сдвига r_{i-1} в сторону старшего на один разряд. В состав PRF входит N-разрядный сумматор по модулю два AddM2 и мультиплексор MS.

В данной схеме $2r_{i-1} \geq P(x)$, то в старший разряд ($C_т$) кода $2r_{i-1}$ принимается «1», который через блок схем И2 на выход передается результат сложения по модулю как результат, т.е $r_i=2r_{i-1} \oplus P(x)$.

Если старший разряд кода $2r_{i-1}$ принимает значение «0», т.е $C_т=0$, то это показывает на то, что $2r_{i-1}<P(x)$. В этом случае блок схем И1 выдает на выход значения $2r_{i-1}$. При этом $2r_{i-1}=r_i$.

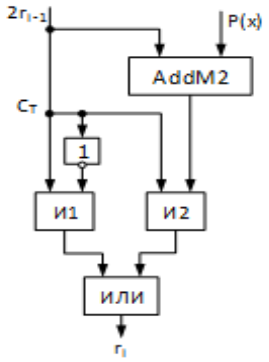


Рисунок 7. Структура PRF

Сумматор по модулю два AddM2 состоит из N-разрядного сумматора по модулю два. На входы подаются значения частичных остатков r_i и значения промежуточного остатки R_{i-1} и на выходах формируется значение

$$R_i = r_i \oplus R_{i-1}.$$

При переносе тактовыми сигналами двоичных коэффициентом полинома-множителя B(x) из буферного регистра i-ой ступени РгB(x).i в регистр i+1ступень РгB(x).i+1 передаются только те двоичные коэффициенты, которые еще не вступили в операцию. После подачи каждого тактового сигнала перенос двоичных коэффициентов модулю P(x) из буферного регистра i-ой ступени РгP(x).i в регистр i+1ступень РгB(x).i+1 передаются без изменения.

Параллельный перенос первой тройки полиномов $B^1(x)$, $A^1(x)$ и $P^1(x)$ на входы буферных регистров первой ступени осуществляется первым тактовым импульсом Clock.1. Во время действия этого импульса на управляющий вход блока схем И1 подается значение младшего бита b_0 полинома $B^1(x)$, а на информационные входы И1 подаются двоичные коэффициенты полинома A(x) из регистра A(x) и при $b_0=1$ на его выходах формируется промежуточных остаток $R_0=r_0$, который записывается в регистр $РгR_0$. Этим же импульсом двоичные коэффициенты полинома $A^1(x)$ со сдвигом на один разряд в сторону старших разрядов передается на первые входы PRF.1, а на его вторые входы передаются двоичные коэффициенты модуля $P^1(x)$. На выход PRF.1 формируется

частичных остатков r_1, который запоминается в регистре Prr_1 одновременно импульсом Clock.1 двоичные коэффициенты полиномов $B^1(x)$ без бита b_0 и двоичные биты полинома $P^1(x)$ переносятся в буферный регистр РгВ(х).1, а также содержимое регистра РгР(х) изменится РгР(х).1 первой ступени.

По заднему фронту импульса Clock.1 во входные регистры конвейера принимается вторая тройка полиномов $B^2(x)$, $A^2(x)$ и $P^2(x)$. После подачи второго тактового импульса Clock.2 по переднему фронту содержимые буферных регистров первой ступени переносится на буферные регистры второй ступени. При этом на блоке схем И2 выполняется операция b_1 r_1 и результат передается на первые входы сумматора по модулю два AddM2.1, а на вторые входы, которого передается содержимое PrR_0-R_0 и на выходе AddM2.1 формируется значение промежуточного остатка R_1, который запишется буферным регистром PrR_1 второй ступени. Вторым тактовым импульсом Clock.2 с выхода регистра Prr_1 со сдвигом на один разряд в сторону старшего передается значение $2r_i$ на первые входы PRF.2, а на вторые входы PRF.2 передается значения модуля Р(х) и на выходах PRF.2 формируется частичный остаток r_2, который запоминается в буферном регистре конвейера 2-ступени Prr_2. В буферный регистр РгВ(х).2 переносится содержимое от РгВ(х).1 без бита b_1 а в регистр РгР(х).2 переносится содержимое РгР(х).1. По заднему фронту импульса Clock.2 на входные регистры конвейера принимается третья тройка полиномов $B^3(x)$, $A^3(x)$ и $P^3(x)$. Полиномы $B^2(x)$, $A^2(x)$ и $P^2(x)$ по переднему фронту Clock.2 обрабатываются на логических блоках первой ступени и в результате формируются частичные остатки r_1 и R_0 по двоичным коэффициентом полиномов второй тройки, которые записаны в буферные регистры первой ступени.

После подачи третьего тактового импульса Clock.3 в буферных регистрах Prr_3 и PrR_2 пятой ступени запоминают остатки r_3 и R_2 первой тройки полиномов. В буферных регистрах второй ступени Prr_2 и PrR_1 запоминают остатки r_2 и R_1 второй тройки полиномов, а буферный регистр первой ступени запоминает r_1 и R_0 третьей тройки полиномов и по заднему фронту Clock.3 на входные регистры устройства принимается четвертая тройка полиномов $B^4(x)$, $A^4(x)$ и $P^4(x)$.

После подачи на конвейер тактового импульса Clock.4 четвертая тройка $B^4(x)$, $A^4(x)$ и $P^4(x)$ обрабатывается логическими блоками I-ступени третья тройка полиномов $B^3(x)$, $A^3(x)$ и $P^3(x)$ обрабатывается логическими блоками II-ступени, вторая тройка полиномов $B^2(x)$, $A^2(x)$ и $P^2(x)$ обрабатывается логическими блоками III-ступени конвейера, первая тройка полиномов $B^1(x)$, $A^1(x)$ и $P^1(x)$ обрабатывается логическими блоками IV-ступени конвейера.

После подачи тактового импульса Clock.N из регистра РгВ(х).N-1 значение бита b_{N-1} подается на управляющий вход блока схем И.N-1, а на управляющие входы его подается значение r_{N-1} из буферного регистра Prr_{N-1} ступени N-1. Результат с выходов блока схем N_{N-1} подается на входы сумматора по модулю два AddM2.N-1, а на его втором входе подается значение R_{N-1} из регистра PrR_{N-1} и на выходе AddM2.N-1 формируется результат $R=[A^1(x)\cdot B^1(x)] \bmod P^1(x)= R_{N-1}$, который фиксируется в регистре РгR.

После подачи N+1 тактового сигнала на выходах регистра РгR формируется результат умножения по модулю полиномов $[A^1(x)\cdot B^1(x)] \bmod P^1(x)= R_N$. Далее по мере подачи следующих тактовых сигналов на выходе схемы умножителя будет иметь значение остатков R_{N+1}, R_{N+2}, …, R_{N+K}.

Рассмотрим пример умножения полиномов по модулю на пятиступенчатом конвейере (K = 5) следующих полиномов:

$ТП_i$	Полиномы	Двоичные изображения

$ТП_1$	$A(x)_1=x^4+x+1$ $B(x)_2=x^4+x^2+1$ $P(x)_3=x^5+x^2+1$	10011_2 10101_2 100101_2
$ТП_2$	$A(x)_2=x^4+x^3$ $B(x)_2=x^4+x^3+x$ $P(x)_5=x^5+x^2+1$	11000_2 11010_2 100101_2
$ТП_3$	$A(x)_3=x^4+x^2+1$ $B(x)_3=x^4+x^2+1$ $P(x)_3=x^5+x^2+1$	10110_2 10111_2 100101_2

В таблице 1 приведены результаты потактного вычисления параметров троек полиномов $ТП_1 \div ТП_3$ по модулю на пятиступенчатом конвейере.

Таблица 1. Результаты потактного вычисления параметров полиномов $ТП_1$, $ТП_2$ и $ТП_3$ на пятиступенчатом конвейере.

ТИ / Полиномы	ТИ1	ТИ2	ТИ3	ТИ4	ТИ5	ТИ6	ТИ7
$A_1=10011_2$ $B_1=10101_2$ $P_1=100101_2$	$r_1=00011_2$ $R_0=10011_2$	$r_2=10110_2$ $R_1=10011_2$	$r_3=01101_2$ $R_2=10101_2$	$r_4=11000_2$ $R_3=10101_2$	$R_4=01101_2$		
$A_2=11000_2$ $B_2=11010_2$ $P_2=100101_2$		$r_1=10101_2$ $R_0=0_2$	$r_2=00011_2$ $R_1=10011_2$	$r_3=11110_2$ $R_2=10101_2$	$r_4=11001_2$ $R_3=01011_2$	$R_4=10010_2$	
$A_3=10110_2$ $B_3=10111_2$ $P_3=100101_2$			$r_1=01001_2$ $R_0=10110_2$	$r_2=10010_2$ $R_1=11111_2$	$r_3=00001_2$ $R_2=01101_2$	$r_4=00010_2$ $R_3=01101_2$	$R_4=01111_2$

Умножение полиномов матричной схемой определяется по формуле – NKT_k, где N – количество тройки полиномов, подлежащее к обработке, K – число ступеней конвейера, T_k – длительность тактового периода, который определяется по соотношению $T_k=T_{PRF}+T_{5P}$, где T_{PRF} – время формирования частичных остатков, T_{5P} – время записи результата обработки в буферные регистры.

Время выполнения операции над N выходными потоками полиномов (тройки полиномов) на K ступенях конвейере с тактовым периодом T_k можно определить соотношением:

$$T_{NK} = (K + (N-1))T_K$$

В этой формуле отражается, до появления на выходе конвейера результата вычисления первой тройки полиномов должно пройти K тактов, а последующие результаты будут следовать в каждом такте.

Ускорение вычислений S за счет конвейеризации можно формулой

$$S = \frac{NKT_K}{(K + (N-1))T_K} = \frac{NK}{K + (N-1)}$$

При $N \to \infty$ ускорение стремится к величине равный количеству ступеней в конвейере.

Для выше приведенного примера, где N=3 и K=5 время умножения по матричной и конвейерной схемы равно:

$$T_{\text{матрица}} = NKT_k = 15T_k$$

$$T_{\text{конвейер}} = \big(K + (N-1)\big)T_k = 7T_k$$

Тогда ускорения умножения равняется

$$S = \frac{T_{\text{матрица}}}{T_{\text{конвейер}}} = \frac{15}{7} \approx 2.14$$

Выигрыш во времени C можно вычислить по формуле:

$$\mathrm{C} = (NK - (K + (N-1)))T_K$$

Для нашего примера:

$$\mathrm{C} = (15 - 7)T_K = 8T_K$$

С увеличением значении N и K ускорение и выигрыш по времени умножения увеличивается. На пример, при N=50 и K=20:

$$T_{\text{матрица}} = NKT_k = 1000T_k$$

$$T_{\text{конвейер}} = \big(K + (N-1)\big)T_k = 69T_k$$

$$S = \frac{T_{\text{матрица}}}{T_{\text{конвейер}}} = \frac{1000}{69} \approx 14{,}49$$

$$\text{С} = (1000 - 69)T_K = 931T_K$$

Литература

1 Svoboda A. Valach M. Operatorove obvody // Stroje Na Zpracovani Informaci – 1955. – Vol 3. – P. 247-295.

2 Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Соаветское радио, 1968.

3 Бияшев Р.Г., Нысанбаева С.Е. Алгоритм формирования электронной цифровой подписи с возможностью обнаружения и исправления ошибки // Кибернетика и системный анализ. – 2012. – Т. 48, № 4. – С. 14-23.

4 Нысанбаев Р.К. Криптографический метод на основе полиномиальных оснований // Вестник Мин-ва науки и высшего образования и Нац. акад. наук Республики Казахстан – Алматы: Гылым, 1999. – № 5. – С. 63-65.

5 Kalimoldayev, M., Tynymbayev, S., Magzom, M., Ibraimov, M., Khokhlov, S., Abisheva, A., Sydorenko, V. Polynomials multiplier under irreducible polynomial module for high-performance cryptographic hardware tools / CEUR Workshop Proceedings. – 2019. – Vol. 2393.– P. 729-737.

6 Kalimoldayev, M., Tynymbayev, S., Gnatyuk, S., Magzom, M., Khokhlov, S., Kozhagulov, Y. Matrix multiplier of polynomials modulo analysis starting with the lower order digits of the multiplier / NEWS of the Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences. – 2019. – Vol.4.- P.181-187.

7 Калимолдаев М.Н., Тынымбаев С.Т., Ибраимов М., Мағзом М.М., Кожагулов Е.Т., Намазбаев Т.А. Конвейерный умножитель полиномов по модулю с анализом старших разрядов множителя/ Вестник НАН РК. – 2020. – Т. 4, №386, С. 13-18.

РАЗРАБОТКА УСТРОЙСТВА ДЛЯ ВЫЧИСЛЕНИЯ НОД НА ОСНОВЕ ВЫЧИТАТЕЛЯ

[1]Тынымбаев С.Т., [1]Мукашева А.К., [1]Шайкулова А.А.,
[2]Әділбекқызы С., [2]Жаксылыков З.Б.
e-mail: s.tynym@mail.ru
[1]Алматинский университет энергетики и связи имени Г. Даукева, Казахстан
[2]Satbayev University, Казахстан

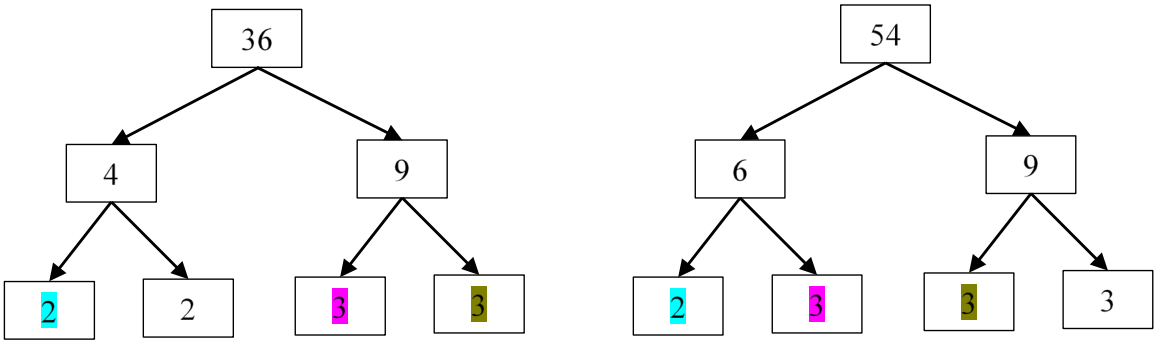
Аннотация. *Асимметричная криптография не требует физически защищенного канала передачи ключей, но имеет низкое быстродействие. Статья посвящена исследованию в области проблемы повышения низкого быстродействия асимметричных криптосистем. Аппаратная реализация асимметричных криптосистем позволяет повысить быстродействие. Нахождение наибольшего общего делителя (НОД) является одним важных этапов при формировании пары ключей в ассиметричных криптосистемах, поэтому аппаратная реализация вычисления НОД является одним из ключевых моментов для улучшения быстродействия криптоалгоритмов. Предлагается схемное решение вычисления наибольшего общего делителя двух чисел (a, b) на основе вычитателя, которое было реализовано на основе алгоритма Евклида. Также был предложена функциональная схема ускоренного варианта вычитателя НОД.*

Защита информации с помощью шифрования считается одним из наиболее надежных способов решения проблемы безопасности. Криптография является обязательным элементом безопасных экономических систем. При этом широко применяется асимметричная криптография, которая не требует физически защищенного канала передачи ключей. Это очень важно в современных условиях повсеместной цифровизации всех слоев общества. Применение асимметричных криптоалгоритмов сдерживается их низким быстродействием по сравнению с симметричными криптоалгоритмами, поскольку необходимо выполнить сложные математические операции из модулярной арифметики, как: умножение, возведение в квадрат и приведение по модулю.

Аппаратная реализация позволяет получить более быстродействующие асимметричные криптосистемы. К тому же аппаратуру легче физически защитить от проникновения извне. Аппаратура шифрования более проста в установке. Однако реализация математических вычислений на аппаратных платформах, таких как ПЛИС (FPGA), является более сложной задачей, чем выполнение их в программной среде, где само оборудование уже оснащено шиной данных вычислений и блоком управления для почти бесконечного числа алгоритмов и арифметических операций. За этой проблемой аппаратной реализации стоит бесценный выигрыш с точки зрения производительности, поскольку есть прекрасная возможность использовать меньшую площадь (аппаратные затраты), получить более высокую скорость, потреблять меньше энергии или получить разумную комбинацию всего этого. Вычисление наибольшего общего делителя (НОД) - одна из задач, для правильного решения которой требуется множество шагов. Эти шаги могут быть преобразованы в итерационный алгоритм, такой как алгоритм Евклида, который делает вычисления понятными и отслеживаемыми [1 ÷ 6].

Наибольший общий делитель (НОД) двух натуральных чисел - это наибольшее целое число, которое делит оба числа без остатка. НОД можно вычислить, определив простые множители обоих чисел, а затем умножив общие простые множители. НОД можно вычислить, определив простые множители обоих чисел, а затем умножив общие простые множители. На

практике для большинства людей этот метод сложен для расчета НОД. Рисунок 1 показывает пример того, как работает метод разложения на простые множители.



2) Общие: 2, 3, 3 3) Умножение: 2* 3*3 = 18 НОД(36, 54) = 18

Рис.1 Метод разложения на простые множители для нахождения НОД двух целых чисел

Эффективным методом решения задач НОД является алгоритм Евклида, который основан на том, что НОД двух чисел (a, b) делит остаток от деления (r) между ними (1):

$$\text{НОД}\ (a, b) = \text{НОД}\ (b, r) \quad (1)$$

где, $a = qb + r$, q – целая часть и r – остаток от деления.

Это итерационный процесс, который занимает несколько циклов для вычисления НОД. Деления выполняются итеративно до тех пор, пока не будет получено $r_n = 0$, тогда НОД = r_{n-1} (2).

$$\text{НОД}\ (a, b) = \text{НОД}\ (b, r_1) \quad (2)$$
$$\text{НОД}\ (b, r_1) = \text{НОД}\ (r_1, r_2)$$

Поскольку деление — это базируется на простом вычитание (3), было замечено, что НОД двух чисел также делит их разность, что упрощает разработку и реализацию схемы.

$$\text{НОД}\ (a,b) = \text{НОД}\ (b, (a - b)) = \text{НОД}(a, (b - a)) \quad (3)$$

На рис. 2 представлена функциональная схема вычислителя наибольшего общего делителя (НОД) чисел А и В основанного на простом алгоритме Евклида с использованием вычитателя и схемы сравнения (СС). Вычитатель реализован на основе двоичного сумматора (СМ), где операция вычитания заменяется операцией сложения в дополнительном коде: $A - B = A + \overline{B} + 1$.

Кроме сумматора и схемы сравнения вычислитель содержит регистры РгА и РгВ для хранения исходных числе соответственно А и В и промежуточных результатов. Элемент задержки ЭЗ.1, триггер Т и схема И3 служат для управления передачей тактовых сигналов ТИ на входы схемы. В состав вычислителя входят также блоки схем И1, И2, И4 ÷ И9 назначение которых рассмотрим в ходе описания работы вычислителя.

На рис. 3 приведен алгоритм Евклида – нахождение наибольшего общего делителя с учетом функциональной схемы приведенной на рис. 2.

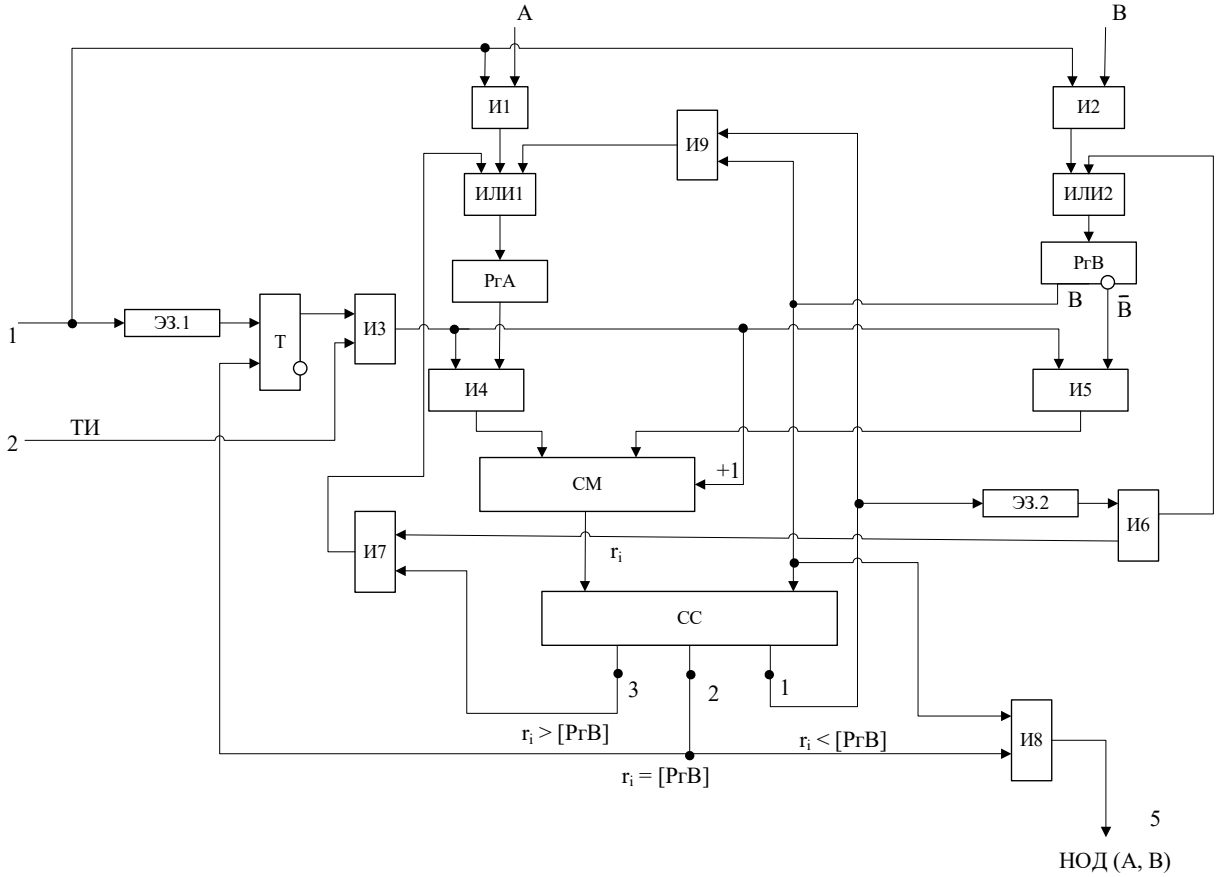


Рис. 2. Функциональная схема вычислителя НОД на основе вычитателя

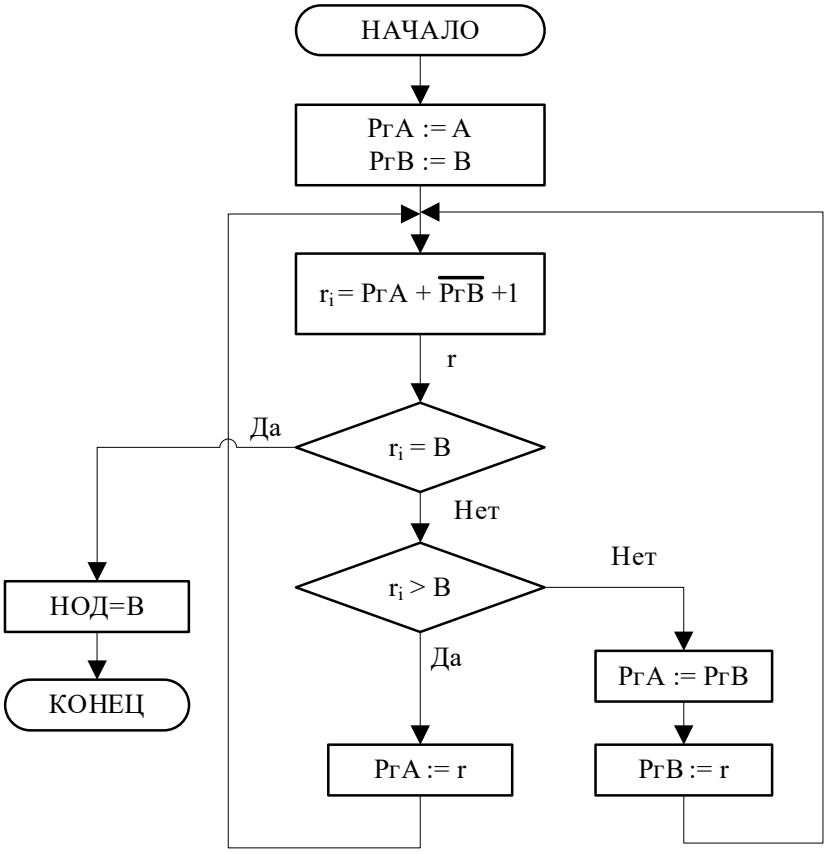


Рис. 3. Алгоритм вычисления НОД на основе вычитателя

Рассмотрим работу вычислителя НОД. По сигналу ПУСК (Вход 1) блоками схем И1 и И2 числа А (Вход 3) и В (Вход 4) через блоки схем ИЛИ1 и ИЛИ2 принимаются соответственно в регистры РгА и РгВ. На время записи в регистры РгА и РгВ чисел А и В сигнал «Пуск» задерживается на элементе задержки ЭЗ.1 и поступает в единичный вход триггера Т и переводит его в единичное состояние. Единичный сигнал с выхода триггера подается на первый вход схемы И3, что разрешает прохождение первого тактового импульса ТИ1 с выхода схемы И3 на управляющие входы блока схем И4 и И5. Кроме того единичный сигнал с выхода И3 подается в младший разряд сумматора СМ как сигнал «+1». Вторые входы блоков схем И4 и И5 связаны с выходами РгА и с инверсными выходами регистра РгВ ($Рг\overline{В}$). При этом сигналом ТИ1 в сумматоре выполняется операция $r_i = A + \overline{B} + 1$. Значение r_1 поступает на первые входы СС, на вторые входы которого подается из прямых выходов регистра РгВ. При этом осуществляется сравнение r_1 с В. При условий $r_1 > B$ на выходе 3 СС вырабатывается уровень «+1», при условий $r_1 = B$ на выходе 2 вырабатывается уровень «+1» и при условий $r_1 < B$, то на выходе 1 вырабатывается уровень «+1».

После сравнения r_1 с В, если $r_1 > B$, то блоком схемы И6 значение разницы r_1 передается через блока схем ИЛИ1 на вход РгА. Теперь в РгА фиксируется значение r_1 взамен исходного значение числа А.

Вторым тактовым импульсом ТИ2 вычисляется $r_2 = r_1 - B$. После сравнения r_1 с В, если выполняется условия $r_1 < B$, то до поступления тактового сигнала ТИ2 уровнем с третьего выхода СС число В из регистра РгВ блоком схемы И4 и ИЛИ1 перепишется в регистр РгА, задержанным сигналом с 1-го выхода СС посредством блока схем И6 значение r_1 перепишется в регистр РгВ. При этом тактовом сигналом ТИ2 формируется путем вычитания из В числа r_1.

После сравнения r_1 с В, если r_1 = В, то единичный сигнал с выхода 2 СС продается на нулевой вход триггера Т и переводит его в нулевое состояние, тем самым запрещает прохождение следующего тактового сигнала на выход схемы И3. Кроме того этим сигналом содержание регистра РгВ выдается на выход 5, что является наибольшим общем делителем чисел А и В.

Аналогично вычисляются другие разницы r_3, …, r_n до сформирования единичного сигнала на выходе 2 схемы сравнения СС.

Таким образом для определения очередной разницы r_i из содержимого регистра [РгА] вычитаются содержание регистра [РгВ] и r_i сравнивается с содержимым регистра [РгВ]. При этом если r_i > [РгВ], то r_i перепишем в регистр РгА, если r_i < [РгВ], содержимое регистра [РгВ] переписывается в регистр РгА, а разница r_i переписывается в регистр РгВ. При r_i = [РгВ] операция завершается и содержимое [РгВ] принимается за результат.

Рассмотрим пример на вычисления НОД для чисел А = 223 и В = 53. В таблице 1 приведена последовательность определения НОД чисел А и В, где для наглядности все вычисления выполняются в десятичной системе счисления.

Как видно из Рис. 1 и таблицы 1 для вычисления r_i= [РгА] – [РгВ] в операцию принимает участие только одинарное значение обратного кода содержимого регистра [Рг$\overline{B}$]. Для ускорения вычисления необходимо участие удвоенного значения содержимого 2 Рг$\overline{B}$, которого получаем со сдвигом содержимое [Рг$\overline{B}$] на один разряд влево. При этом выбор по сигналу на правый вход сумматора содержимого регистра РгВ [Рг$\overline{B}$] либо управляется дополнительной схемой схемы сравнения. При этом на правый вход этой схемы подаются содержимое [РгА], на вторые входы подается содержимое РгВ со сдвигом на один разряд в сторону старшего разряда. при этом на первом выходе схемы сравнения формируется сигнал 1, если [РгА] > 2[РгВ], а на втором выходе формируется единичный сигнал, если [РгА] ≤ 2[РгВ]. Эти сигналы используются для организаций передачи содержимого РгВ без сдвига или для передачи содержимого РгВ со сдвигом влево на один разряд.

Таблица 1. Последовательность вычисления НОД (223, 53)

№	Действия	№	Действия
ТИ1	223 [РгА] - 53 [РгВ] $170 = r_1 > 53$; РгА:= 170	ТИ8	20 [РгА] - 11 [РгВ] $9 = r_8 < 11$; РгА:= 11; РгВ:= r_8
ТИ2	170 [РгА] - 53 [РгВ] $117 = r_2 > 53$; РгА:= 117	ТИ9	11 [РгА] - 9 [РгВ] $2 = r_9 < 9$; РгА:= 9; РгВ:= r_9
ТИ3	117 [РгА] - 53 [РгВ] $64 = r_3 > 53$; РгА:= 64	ТИ10	9 [РгА] - 2 [РгВ] $7 = r_{10} > 2$; РгА:= 7

ТИ4	64 [РгА] - 53 [РгВ] $11 = r_4 < 53$; РгА:= 53; РгВ:= r_4	ТИ11	7 [РгА] - 2 [РгВ] $5 = r_{11} > 2$; РгА:= 5
ТИ5	53 [РгА] - 11 [РгВ] $42 = r_5 > 11$; РгА:= 42	ТИ12	5 [РгА] - 2 [РгВ] $3 = r_{12} > 2$; РгА:= 3
ТИ6	42 [РгА] - 11 [РгВ] $31 = r_6 > 11$; РгА:= 31	ТИ13	3 [РгА] - 2 [РгВ] $1 = r_{13} < 2$; РгА:= 2; РгВ:= r_{13}
ТИ7	31 [РгА] - 11 [РгВ] $20 = r_7 > 11$; РгА:= 31	ТИ14	2 [РгА] - 1 [РгВ] $1 = r_{14}$ НОД (223, 53) =1

Алгоритм ускоренного вычисления НОД приведена на рис. 4. На рисунке 5 приведена функциональная схема вычислителя НОД (А, В), позволяющий ускорить вычисления. Как видно из Рис. 2 в составе вычитателя включена схема сравнения СС-1 и блок схемы И6 для передачи обратного кода удвоенного значения содержимого регистра РгВ.

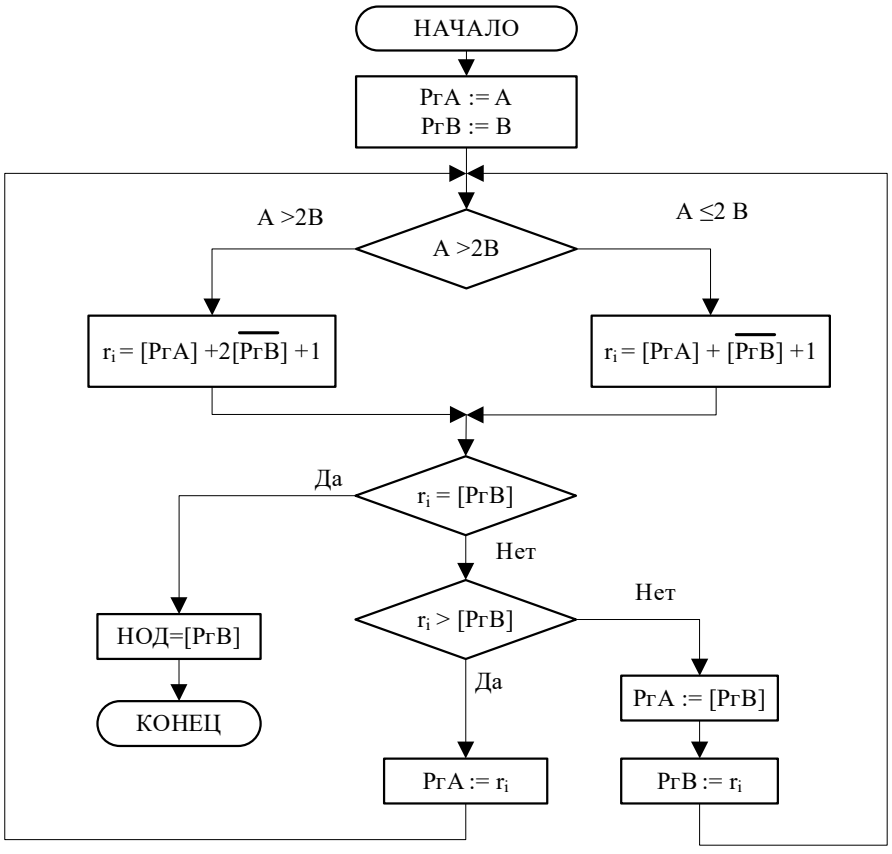


Рис. 4. Алгоритм ускоренного вычисления НОД

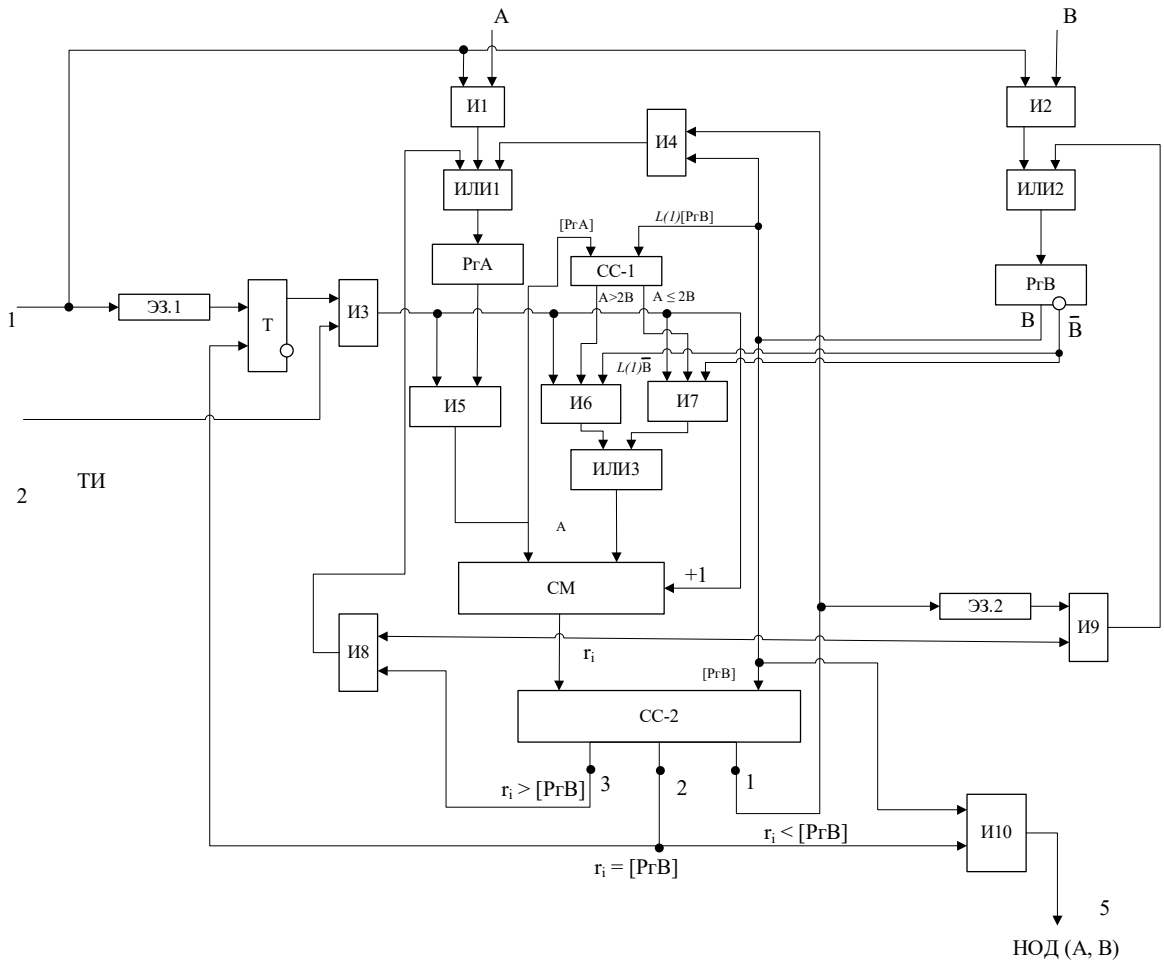


Рис. 5. Функциональная схема ускоренного вычислителя НОД на основе вычитателя

В таблице 2 приведен пример вычисления НОД (223, 53) на схеме ускоренного вычислителя.

Таблица 2. Последовательность вычисления НОД (223, 53) по схеме ускоренного вычислителя НОД

№	Действия	№	Действия
ТИ1	223 A>2B; СМ:=2$\overline{B}$ =106 - 106 [2B] 117 = r_1 > 53; РгА:= 117	ТИ5	11 11<9*2=18 - СМ:=18 9 [B] 2 = r_5 <9; РгА:= 9; РгВ:=2
ТИ2	117 A>2B; СМ:=2$\overline{B}$ =106 - 106 [2B] 11= r_2 < 53; РгА:=53; РгВ:=11	ТИ6	9 9>2*2=4 - СМ:=4 4 [2B] 5= r_6>2; РгА:= 5; РгВ:= 2

ТИ3	53 53>11*2=22 - СМ:=22 22 [2В] 31 = r_3 > 11; РгА:= 31	ТИ7	5 5>2*2=4 - СМ:=4 4 [2В] 1 = r_7 < 2; РгА:= 2; РгВ:= 1
ТИ4	31 31>11*2=22 - СМ:=22 22 [2В] 9 = r_4 < 11; РгА:= 11; РгВ:=9	ТИ8	2 2=2*1 - 1 [В] 1 = r_8 =1; НОД (223, 53)=1

Сравнивая таблицу 1 и таблицу 2 нетрудно заметить, что для нахождения НОД целых чисел (223, 53) с помощью схемы (Рис. 2) потребуются 14 тактовых шагов, а для схемы с ускорением вычисления (Рис. 5) потребуются 8 тактовых шагов.

Литература.

1. Hazmi, Ibrahim. (2015). Design and Implementation of the Euclidean Algorithm for Computing the Greatest Common Divisor using Xilinx Spartan6 FPGA. doi: 10.13140/RG.2.1.3669.3208.

2. Виноградов, И. М. Основы теории чисел: учебное пособие / И. М. Виноградов. — 12-е изд.,стер. — Санкт-Петербург: Лань, 2009. — 176 с. — ISBN 978-5-8114-0535-0.

3. Хассе Г. Лекции по теории чисел. Издательство иностранной литературы. Москова, 1953 - 258 с.

4. Сизый, С. В. Лекции по теории чисел: учебное пособие / С. В. Сизый. — 2-е изд., испр. и доп. — Москва : ФИЗМАТЛИТ, 2008. — 192 с. — ISBN 978-5-9221-0741-9.

5. Ахметов Б.С. Кузнецов А.А. Краснобаев В.А. Алимсеитова Ж.К. Кузнецова Т.Ю. Основы криптографии: элементы теории чисел, групп, полей, колец. Учебное пособие, Алматы, 2019. -320 с.

6. Лехин, С. Н. Схемотехника ЭВМ: Учебное пособие / Лехин С.Н. - СПб:БХВ-Петербург, 2010. - 663 с.ISBN 978-5-9775-0353-2.

ИССЛЕДОВАНИЕ И АНАЛИЗ РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ

[1]С. Тынымбаев, [2]А.Ж. Иманбаев
imanbaevazamat@gmail.com
[1]Алматинский университет энергетики и связи имени Гумарбека Даукеева, Алматы Казахстан
[2]Казахский Национальный Университет имени Аль-Фараби, Казахстанско-Британский Технический Университет, Алматы, Казахстан

***Аннотация**: ожидается, что достижения в области технологий вместе с более широким развитием сетей за пределами сотовой связью 5G окажут значительное влияние на безопасность, например, программно-определяемые сети (SDN), виртуализацию сетевых функций (NFV) и периферийные вычисления. Стандарт 5G 3GPP является независимым в том смысле, что он достаточно гибок, чтобы допускать различные типы физического и виртуального перекрытия между сетью радиодоступа и базовой сетью, например, от удаленного устройства до базовой сети. Разделение функций между сетью радиодоступа и ядром поднимает вопросы о конкурентоспособности и производительности. С точки зрения экономики, конкуренции и производительности, отказ от использования технологических достижений в конфигурации и развертывании коммерческих сетей 5G в итоге окажется контрпродуктивным для реализации уникальных сценариев использования 5G. В соответствии со структурой сети 5G, в данной статье проведен анализ рисков безопасности сети 5G, резюмированы четыре риска безопасности: конфиденциальность, целостность данных, аутентичность пользовательского оборудования и доступность сетевых функций. Так же предложены контрмеры и предложения по защите сетей 5G.*

***Ключевые слова**: 5G; Интернет вещей; Безопасность Интернета вещей; виртуализация; граничные вычисления.*

Введение. Как новое поколение технологии мобильной связи, 5G имеет характеристики более высокой скорости, более низкого энергопотребления, более короткой задержки и более широких соединений по сравнению с традиционными сетями. Более того, на основе значительного улучшения возможностей мобильного Интернета, 5G расширилась до области Интернета вещей, а ее цели обслуживания расширились с общения людей с людьми на людей с вещами и от вещей к вещам. Общение вещей, открывает новую эру взаимосвязи всего сущего. Три основных услуг для которых требуется создание сетей 5G включают расширенную мобильную широкополосную связь (eMBB), массовые коммуникации машинного типа (mMTC) и сверхнадежную связь с малой задержкой (uRLLC).

Тенденция развития сетей 5G, особенно новых услуг 5G, новых архитектур и новых технологий, ставит новые задачи в области безопасности и защиты конфиденциальности пользователей. В этой статье анализируются риски безопасности сетей 5G на основе сетевой архитектуры 5G и предлагаются контрмеры и предложения по трем аспектам: усиление построения сетевой безопасности 5G, создание механизма классификации рисков безопасности и улучшение системы безопасности стандартной системы безопасности 5G.

Анализ рисков

Общая архитектура

В целом новые риски, вызванные технологической революцией сетей 5G, в основном отражаются в распространенности устройств, виртуализации сетевых функций, сегментировании сети. По сравнению с сетями 4G объем информации, доступной для злоумышленников в сетях 5G, значительно увеличился и сталкивается с более высокими

рисками безопасности. Как показано на рисунке 1, на основе сетевой архитектуры 5G возможные риски безопасности сети 5G анализируются по уровням.

Рисунок 1. Общая схема архитектуры сетевой безопасности 5G

Уровень доступа

Безопасность оконечного оборудования. Риски безопасности, с которыми сталкивается оборудование, связаны с сетевым обменом данными и самим устройством. С одной стороны, для сетевой связи в беспроводной среде устройства сталкиваются с угрозами безопасности, такими как кража личных данных, сниффинг и спуфинг. В основном из-за уязвимостей в конструкции микросхемы устройства или недостаточной защиты аппаратной системы безопасности, что приводит к рискам безопасности, таким как утечка и подделка конфиденциальных данных; с точки зрения программного обеспечения устройства, также существует риск безопасности, когда кибер-злоумышленники запускают атаки через программное обеспечение устройства. Риски безопасности, связанные с сетевым обменом данными, с которыми сталкивается устройство, заключаются в следующем.

1) Аутентичность оборудования и конфиденциальность данных. Аутентичность оконечных устройств, особенно подлинность устройств IoT, является ключом к защите от атак безопасности. Идентификация и аутентификация устройств на уровне без доступа к сети 5G больше не основывается на SIM-картах, особенно на устройствах IoT, которые используют гибкие методы аутентификации, такие как приложения eSIM, которые создают проблемы для аутентификации оконечных устройств и влияют на подлинность устройства.

Кроме того, устройства с низкой аутентичностью также подвергаются атакам типа «человек по середине», в результате чего сторонние устройства перехватывают сообщения в сеансе, что создает угрозу конфиденциальности данных.

2) Наличие функций уровня доступа к сети. Некоторые оконечные устройства на уровне доступа, особенно устройства M2M, имеют значительно низкое энергопотребление и разные режимы передачи данных. Кроме того, оборудование уровня доступа имеет ограниченные

вычислительные ресурсы и низкую производительность, что затрудняет повышение доступности сетевых функций.

Безопасность радиоинтерфейса базовой станции. Риски безопасности радиоинтерфейса базовой станции в основном включают две основные категории [1, 2].

Первое, риски безопасности, вызванные внешними неконтролируемыми факторами в беспроводной среде: псевдобазовые станции в беспроводной среде, будут мешать беспроводным сигналам, что приведет к ухудшению доступа устройств 5G и подключению к небезопасным сетям 2G/3G/4G. Если атаковать широко распространенные устройства Интернета вещей с низким уровнем безопасности в беспроводной среде, они могут запустить DDoS-атаки на базовую станцию или базовую сеть, что снизит доступность функций сетевых устройств.

Второе, риски безопасности протокола радиоинтерфейса: лазейки в самом протоколе 3GPP могут столкнуться с такими рисками, как подделка, отказ в обслуживании и атаки повторного воспроизведения (replay attack), которые повлияют на аутентичность устройства; производители устройств должны улучшить качество обслуживания и уменьшить задержку.

Сетевой уровень

Сегментация сети. В соответствии с требованиями бизнес-логики сети 5G можно разделить на разные сегменты сети, которые, по крайней мере, разделены на три категории: расширенную мобильную широкополосную связь (eMBB), массовые коммуникации машинного типа (mMTC) и сверхнадежную связь с малой задержкой (uRLLC). Виртуализированная частная сеть формируется для каждой бизнес-организации посредством управления сегментацией сети [3].

В настоящее время сегментирование сети не получили широкого распространения в производственных системах 5G, и требует полной оценки безопасности. Потенциальные риски безопасности сосредоточены в общих сетевых интерфейсах, совместно используемых в сегментах, интерфейсах управления, интерфейсах между сегментами. Как только незаконный злоумышленник получает доступ к серверу сервисных функций через эти интерфейсы, злоупотребляет сетевым оборудованием, незаконно получает личные данные, включая идентификаторы пользователя, и нарушает доступность, конфиденциальность и целостность данных.

1) Безопасность идентификатора пользователя. Если реальный идентификатор пользователя напрямую используется для связи между пользователями или пользователем и платформой приложения после того, как к сетевой части системы или к интерфейсу между системами обращается незаконная программа, идентификатор пользователя, скорее всего, может быть перехвачена. Вместе с этим может просочиться личные данные пользователя и другая соответствующая информация. Если перехватить идентификатор пользователя весь контент пользователя может быть доступен злоумышленнику.

2) Конфиденциальность данных. С точки зрения безопасности, технология разделения сети стирает границы сети. Если домен управления сетевого сегмента не изолирован от домена, в котором хранится конфиденциальная информация, после атаки на сегмент сети конфиденциальная информация, хранящаяся в этом сегменте при аутентификации личности будет происходить утечка. С одной стороны, доступ к сегментам сети с неавторизованных устройств приведет к незаконному использованию сквозных приложений, а клиенты также рискуют стать жертвой хакерских атак, что может привести к утечке данных.

3) Целостность данных и доступность сетевых функций. Что касается качества обслуживания сервисов и приложений, каждый сетевой сегмент, реализующий 5G, имеет определенный набор параметров QoS. Конфигурация этих параметров тесно связана с качеством сетевых услуг и целостностью данных. Качество обслуживания пользователя должно быть гарантировано при условии обеспечения безопасности. В основных сценариях приложений 5G как сверхнадежная межмашинная связь с низкими задержками (uRLLC) и массовая машинная связь (mMTC) предъявляют высокие требования к качеству обслуживания. Если задержка значительно уменьшится, а скорость передачи увеличится, потеря пакетов данных увеличится, и будет трудно гарантировать целостность данных.

Что касается совместного использования инфраструктуры, несколько сегментов сети используют общие аппаратные устройства. При повреждении аппаратного устройства несколько сегментов, использующих устройство, будут функционально повреждены, и доступность сетевых функций будет серьезно нарушена [4].

Граничные вычисления (Edge computing). Граничные вычисления предназначены для передачи сетевых услуг и вычислительных возможностей стороне сети с беспроводным доступом ближе к пользователям, тем самым уменьшая нагрузку и накладные расходы базовой сети, а также уменьшая задержку обслуживания. Риски безопасности, связанные с граничными вычислениями для сетей 5G, заключаются в следующем.

1. Безопасность идентификации пользователя: граничные устройства сети имеют слабые возможности защиты и могут противостоять сетевым атакам. Трафик между пользовательскими и граничными устройствами легко перехватывается или отслеживается. Злоумышленники могут захватывать идентификаторы пользователей в трафике.
2. Конфиденциальность и целостность данных: граничные вычисления будут использовать открытый интерфейс прикладного программирования (API), открытую виртуализацию сетевых функций (NFV) и другие технологии. Внедрение открытых интерфейсов сделает граничные вычисления уязвимыми для внешних злоумышленников, которые будут использовать незаконный доступ для открытых интерфейсов, красть или незаконно вмешиваться в данные.
3. Подлинность устройства: из-за ограниченных ресурсов на границе сети, вычислительная мощность граничного узла ниже, чем у базовой сети, и возможность проверки идентичности устройства снижается.
4. Доступность сетевых функций: граничная вычислительная инфраструктура обычно развертывается на границе сети, такой как беспроводные базовые станции, и с большей вероятностью будет подвержена воздействию небезопасных сред, а оборудование сталкивается с риском функционального повреждения.

Программно-определяемая сеть (SDN). Наиболее характерной особенностью сети 5G является разделение плоскости управления и плоскости пользователя через программно-определяемую сеть (SDN), централизованное управление сетью с помощью сетевой операционной системы и сквозную маршрутизацию для каждый сервисный поток основан на больших данных и искусственном интеллекте. Более того, информация о маршрутизации встроена в заголовок расширения IPv6 исходного узла и передается каждому узлу в соответствии с исходным путем. Промежуточному узлу нужно только пересылать без маршрутизации, обеспечивая пересылку с малой задержкой, тем самым обеспечивая гибкое управление трафиком [5].

Внедрение технологии SDN создает риски безопасности для конфиденциальности и целостности данных в сетях 5G. В условиях постоянно меняющимися сетевыми ресурсами,

могут быть конфликты в маршрутах, рассчитанных SDN, особенно в сценарии межрегиональной маршрутизации, необходимость обмена данными о потоках услуг и сетевых ресурсах между SDN, прибавляет сложности и склонность к ошибкам расчета маршрутизации, потере пакетов данных или передаче данных по неправильному адресу назначения все это нарушает целостность передаваемых данных. Кроме того, API-интерфейсы устройств виртуализированной инфраструктуры также будут влиять на конфиденциальность и целостность данных, например как, кража данных, кража паролей пользователей, фальсификация данных [6].

Риски, связанные с технологией SDN для функциональной доступности сетей 5G, можно проанализировать с двух сторон: программного и аппаратного: во-первых, с точки зрения программного обеспечения, по сравнению с традиционными мобильными сетями, сети 5G в большей степени зависят от программного обеспечения, которое обеспечивает сетевые операции. Из-за новых угроз необходимо гарантировать, что это программное обеспечение не будет раскрыто или злонамеренно взломано; во-вторых, с точки зрения оборудования, контроллеры SDN и другие связанные аппаратные устройства также имеют риски для безопасности функционального повреждения. Кроме того, после отказов аппаратного оборудования восстановление системы должно автоматически восстанавливать функции взаимодействия между системами NFV, SDN и MANO.

Виртуализация сетевых функций. По сравнению с традиционными мобильными сетями технология виртуализации (NFV) основана на обычном оборудовании и индивидуальном программном обеспечении. Хотя эта технология дает сетям 5G множество преимуществ, существует также много рисков для безопасности.

1. С точки зрения программного обеспечения, если в системе виртуализации есть лазейки, и если она подвергается атаке со стороны программной сети, функциональность системы будет нарушена; если функциональный модуль, хранящий конфиденциальную или важную информацию, не изолирован надежно от поврежденной функции, это также повлияет на конфиденциальность данных.
2. Что касается аппаратного обеспечения, аппаратные устройства общего назначения имеют уязвимости в плане безопасности: во-первых, устройства могут быть физически повреждены из-за воздействия окружающей среды; во-вторых, восстановление после сбоя, может не быть быстрым; в-третьих, существует риск незаконного использования оборудования в общей инфраструктуре.

Технология виртуализации сопряжена с высокими рисками безопасности для доступности сетевых функций и конфиденциальности данных сетей 5G с точки зрения программного и аппаратного обеспечения. Поскольку сеть 5G принимает метод многоуровневой контекстной аутентификации и настраивает QoS с несколькими атрибутами для осведомленности о контексте, включая контексты нескольких пользователей (например, приложения и шаблоны использования) и контексты устройств (например, местоположение и скорость). Если в этих методах аутентификации есть лазейки, их легко взломать злоумышленники, что повлияет на аутентификацию оконечного оборудования и пользователей и снизит аутентичность устройства [7, 8].

Система эксплуатационной поддержки приложений. Система эксплуатационной поддержки приложений 5G не только включает в себя управление сбоями, управление конфигурацией, управление аварийными сигналами и управление производительностью, аналогичное традиционным сетям, но также включает управление виртуализированными сетевыми функциями, которое настраивает и регулирует сетевые функции в соответствии с потребностями пользователя.

Система эксплуатационной поддержки приложений обычно управляются иерархически. Системы нижнего уровня обычно развертываются более разрозненно, с распределенным хранилищем данных, слабыми возможностями управления безопасностью и защиты, а их функции могут использоваться незаконно и также могут вызывать утечку или потерю данных. Конфиденциальность и целостность данных сталкивается с проблемами.

Кроме того, если Система эксплуатационной поддержки приложений имеет лазейки в безопасности и подвергается атаке хакеров, сетевые функции могут быть разрушены, и доступность сетевых функций могут быть затронуты [9].

Прикладной уровень

Сети 5G работают с множеством отраслевых приложений, таких как умные города, умное здравоохранение, умные дома, умное сельское хозяйство, финансы и Интернет транспортных средств. Эти приложения настраиваются различными способами для обеспечения межсетевой работы с потенциальными рисками безопасности. Среди них финансовые услуги, интеллектуальные медицинские услуги и Интернет транспортных средств имеют более высокие риски.

Разнообразные приложения 5G показаны на Рисунке 2. Среди них отдельные ключевые отрасли предъявляют особые требования к безопасности. Например, отраслевые и ориентированные на пользователя приложения. К отраслевым приложениям относятся робототехника и автоматизация, автоматизированные сети транспортных средств и прикладные системы связи в чрезвычайных ситуациях на телемедицинском оборудовании; Приложения, ориентированные на пользователя, включают новые технологии, такие как дополненная реальность (AR) и виртуальная реальность (VR). По сравнению с традиционными сетями эти приложения 5G выдвигают более высокие и сложные требования к сетевой безопасности.

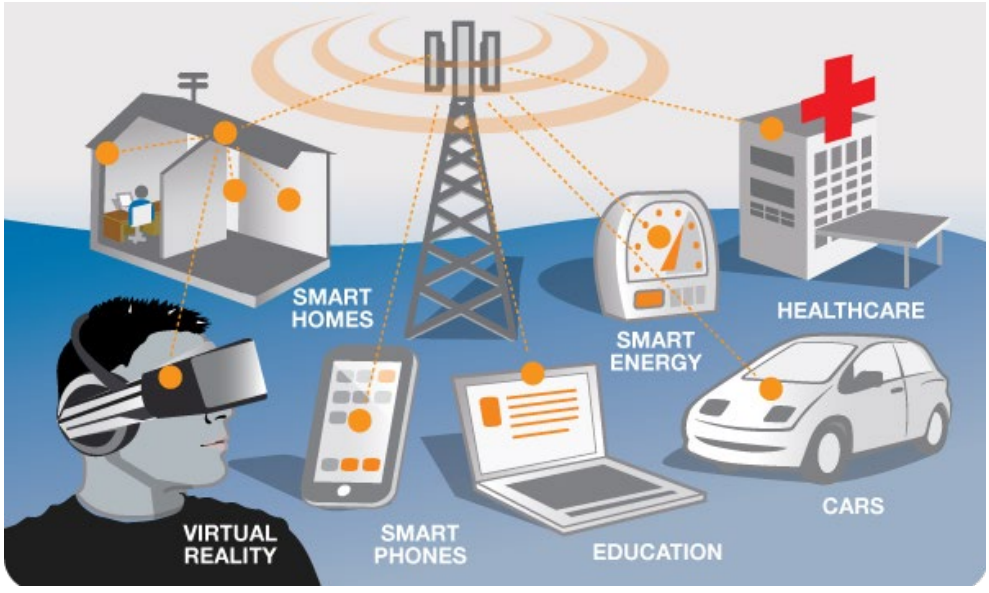


Рисунок 2. Разнообразные вертикальные приложения 5G [10]

Передача данных.

Анализируя риски безопасности при передаче данных, выяснилось, что, от уровня доступа до уровня приложений в сети 5G весь процесс передачи данных сталкивается с

рисками перехвата, подслушивания и подделки, и это все затрагивает конфиденциальность и целостность данных.

1. На уровне доступа могут быть атаки беспроводного доступа в форме подделки, модификации, пересылки и атаки повторного воспроизведения информационного содержимого с использованием беспроводных сигналов в качестве носителя, что серьезно повлияет на конфиденциальность и целостность данных.

2. На сетевом уровне линия передачи между устройствами базовой сети также подвержена риску кражи данных из-за повреждения или незаконной установки подслушивающего оборудования.

3. На уровне приложений, помимо создания собственных серверов во внутренней сети предприятия, различные поставщики услуг приложений также арендуют серверы и каналы связи в сети доставки содержимого (CDN). Передача данных также сталкивается с перехватом и риском кражи данных.

Обзор рисков безопасности.

Таким образом, риски безопасности, с которыми сталкиваются сети 5G на уровне доступа, сетевом уровне и уровне приложений, сосредоточены в четырех аспектах [11].

1. Безопасность идентификатора пользователя должна быть защищена с точки зрения конфиденциальности идентификатора пользователя. В мобильной сети анонимность идентификации может использоваться, чтобы не дать злоумышленникам идентифицировать отдельных пользователей, чтобы злоумышленники не могли отслеживать и анализировать трафик через базовую сеть и проникновение в сеть с беспроводным доступом.

2. Конфиденциальность и целостность данных требует шифрования данных, связанных с конфиденциальностью пользователей при передаче по сети, обработке на сервере и хранении базы данных, чтобы предотвратить утечку конфиденциальной информации.

3. Подлинность устройства. Чтобы злоумышленники не выдавали себя за законного пользователя для получения бесплатных услуг, мобильная сеть аутентифицирует каждое устройство, подключенное к сети, чтобы гарантировать подлинность и надежность идентификации пользователя устройства.

4. Доступность сетевых функций требует учета сетевых функций и требований к характеристикам оборудования при одновременном улучшении возможностей безопасности, чтобы гарантировать, что сетевые функции и производительность оборудования не будут значительно ухудшаться. Необходимо поддерживать баланс между сетевыми функциями, производительностью оборудования и требованиями безопасности.

Контрмеры и предложения

Общие рекомендации

Исходя из четырех основных рисков, с которыми сталкиваются сети 5G, предлагаются следующие рекомендации.

Во-первых, укрепление сетевой безопасности за счет четырех аспектов: безопасность идентификации пользователя, конфиденциальность и целостность данных, аутентичность устройства и доступность сетевых функций. В сочетании с новыми функциями сетей 5G меры защиты улучшаются уровень за уровнем [12, 13].

Второй - установить классификацию рисков безопасности и механизм гарантии классификации. Классифицируйте и расставьте приоритеты сторон, вовлеченных в риски безопасности, и предложите решения по различным категориям, а также уделите приоритетное внимание решению владельцев рисков с наибольшими потерями.

В-третьих, улучшить стандартную систему безопасности 5G. Предприятия в различных отраслях формулируют единые стандарты с помощью организации которые стандартизируют решений безопасности и улучшения возможностей защиты.

Укрепление построения безопасности сети 5G. В ближайшей перспективе следует увеличить инвестиции для создания безопасных сетей 5G, начиная с четырех аспектов: безопасность идентификации пользователя, конфиденциальность и целостность данных, аутентичность устройства и доступность сетевых функций. С точки зрения оборудования, виртуализации сети, с точки зрения разделения сети и граничные вычислений, приняты определенные технологии безопасности для обеспечения безопасности сетей 5G, и принимаются соответствующие меры для устранения рисков безопасности, для создания безопасной и стабильной сетевой архитектуры 5G и повышения общей безопасности сетей 5G. Рекомендуются следующие специальные меры безопасности [14].

Безопасность идентификатора пользователя. На уровне доступа должна быть усилена аутентификация и идентификации устройства, идентификаторы пользователя зашифрованы для хранения и передачи на сетевом уровне, а идентификация пользователя происходит на прикладном уровне, а преобразованные идентификаторы используется для сквозной и межплатформенной связи.

Конфиденциальность и целостность данных. Чтобы повысить конфиденциальность данных, во-первых, необходимо усилить аутентификацию безопасности интерфейса, включая эфирный интерфейс уровня доступа, интерфейс между системой виртуализации ядра сетевого уровня и открытый интерфейс API между сетевым и прикладным уровнем. Предотвращение получения данных через интерфейс незаконными приложениями, что может привести к утечке или подделке данных;

Во-вторых, необходимо хорошо выполнять зашифрованное хранение и передачу данных и применять различные методы шифрования для снижения риска взлома данных. Например, комбинация алгоритма симметричного шифрования (DES, AES) и алгоритма асимметричного шифрования (RSA) используя алгоритм хэширования MD5 или другой алгоритм хэширования с помощью соли, а также токены [15].

Для передачи данных мобильные сети особенно нуждаются в усилении шифрования данных, передаваемых по радиоинтерфейсу между пользовательским устройством и базовой станцией, чтобы предотвратить перехват и прослушивание злоумышленниками сигналов и данных, отправленных и полученных устройством.

Чтобы усилить защиту целостности данных, во-первых, с точки зрения передачи данных, настройте соответствующие политики безопасности для передаваемых сигналов и данных пользователя, а также установите приоритет различных алгоритмов. Сосредоточьтесь на повышении безопасности данных, передаваемых по радиоинтерфейсу.

Для услуг с малой задержкой, чтобы эффективно сбалансировать надежность и безопасность, может быть принята схема безопасности многопутевой избыточной передачи, чтобы повысить эффективность передачи данных при условии обеспечения безопасности данных; так же, с точки зрения хранения данных, используйте метод распределенного хранения данных с несколькими площадками и несколькими центрами, чтобы эффективно выполнять резервное копирование данных. С точки зрения обработки сбоев, восстановление системы после сбоя должно выполняться, так что гарантируют, что данные не будут потеряны особенно восстановление виртуализированных систем и интерфейсов.

Подлинность устройства. Создайте систему управления идентификацией в соответствии с единым стандартом, примените множество гибких методов аутентификационных и идентификационных меток, укрепите возможности аутентификации

устройства, обеспечьте легитимность всех устройств, подключенных к сети, и повысьте аутентичность устройства.

Доступность сетевых функций. Контролируйте баланс между энергоэффективностью оборудования и безопасностью при ограниченных вычислительных ресурсах на уровне доступа, а также улучшайте производительность и функциональную доступность оборудования в соответствии с предпосылкой обеспечения безопасности.

Используйте несколько устройств на сетевом уровне, чтобы повысить доступность сетевых функций: первое - создать полную вирусную базу данных, которую можно своевременно обновлять, чтобы повысить способность защиты от атак; второе - принять необходимые меры для обеспечения безопасной изоляции между уязвимыми устройствами и устройствами, хранящими конфиденциальную информацию; третье - это хорошо провести сертификацию безопасности интерфейсов между виртуализированными системами, чтобы предотвратить незаконный вызов системы и нарушение ее функций.

На уровне приложений сформулировано решение безопасности, подходящее для приложений M2M. Чтобы не оставлять лазейку, которая нарушает безопасность системы, к устройствам M2M можно применять алгоритмы безопасности, чтобы достичь баланса между высокой энергоэффективностью сети и высокой безопасностью.

Создание механизма классификации рисков безопасности и классификационных гарантий. Когда сеть 5G подвергается атаке безопасности, целостность, доступность и конфиденциальность ее системы ставятся под угрозу. В области безопасности эти организации или отдельные лица называются «владельцами рисков». Рекомендуется классифицировать и приоритизировать стороны, вовлеченные в риски безопасности, предлагать решения иерархически и категорично, а также отдавать приоритет решению владельцев рисков, которые несут наибольшие убытки. Рекомендации по классификации владельцев рисков показаны на рисунке 3. Пользователи на более высоких уровнях пирамиды на рисунке имеют более высокие риски, чем пользователи на более низких уровнях. По мере увеличения числа пользователей, пострадавших от атак на систему безопасности, риск будет увеличиваться еще больше, то есть, когда происходит инцидент безопасности, чем больше пользователей, тем сильнее воздействие.

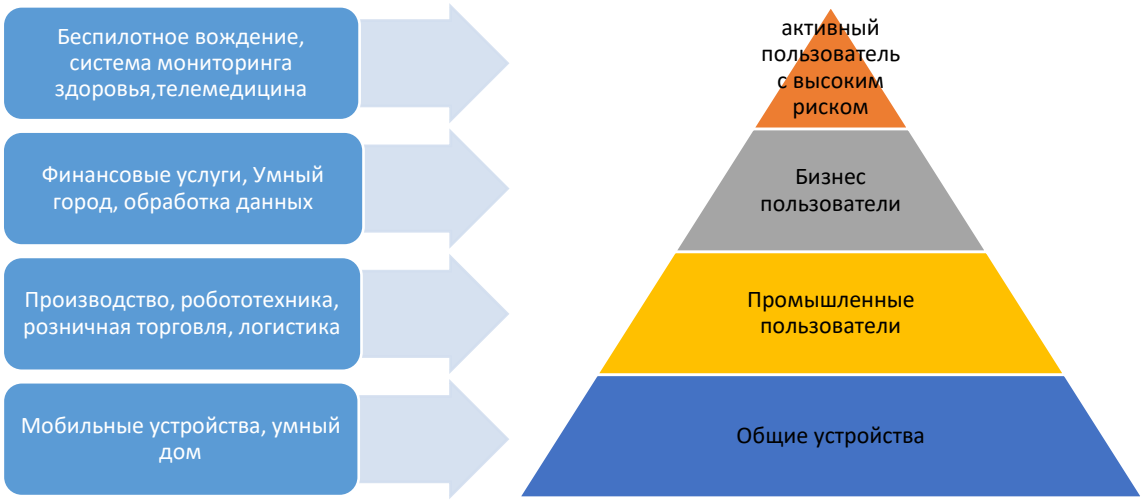


Рисунок 3. Классификация владельцев рисков 5G

При выполнении требований безопасности 5G следует учитывать потребности основных заинтересованных сторон сети и услуг 5G. В нормальных обстоятельствах между различными стратегиями возможны конфликты. Таблица 1 может предоставить рекомендации по выбору приоритетов в соответствии с различными стратегиями. В разных сценариях применения разные заинтересованные стороны будут определять приоритеты различных факторов в соответствии с потребностями.

Таблица 1. Заинтересованные стороны сетей и услуг 5G

Заинтересованные стороны	Основной спрос
Поставщики услуг (включая облачный сервис CaaS и инфраструктурный сервис IaaS)	Доступность, надежность, отказоустойчивость
Сетевые операторы и поставщики	Защита доходов и бренда, лицензирование, конфиденциальность данных
Государственные учреждения	Защита внутренней инфраструктуры, экономическое развитие, правоохранительные органы, аварийные службы
Предприятия и потребители	Защита конфиденциальности данных, производительность (качество обслуживания)

Улучшение стандартной системы безопасности 5G. В долгосрочной перспективе рекомендуется ускорить разработку стандартов. Предприятия в различных отраслях могут формулировать единые стандарты безопасности через организации по стандартизации, предоставлять стандартизированные решения для новых технологий и приложений 5G и улучшать возможности всесторонней защиты. С одной стороны, корпоративные организации в различных отраслях должны сотрудничать друг с другом через организации по стандартизации и промышленные форумы, чтобы сформулировать единые и стандартизованные стандарты безопасности; с другой стороны, все стороны в отраслевой цепочке 5G должны укреплять сотрудничество и сотрудничество для обеспечения безопасности всех звеньев и формирования всеобъемлющей системы управления безопасностью 5G, обладающей полным набором возможностей защиты безопасности.

Рекомендуется, чтобы ассоциации по стандартизации всех отраслей, участвующих в сети 5G, укрепляли координацию и сотрудничество, совместно формулировали спецификации и применяли межуровневый безопасный сквозной (E2E) подход для улучшения различных частей сети 5G (включая базовая мобильная сеть, передача, доступ, услуги и приложения) безопасность взаимодействия. В то же время следует гарантировать, что решения безопасности, предоставляемые единой организацией ассоциации стандартов, не имеют высокой специфичности в ограниченном диапазоне, чтобы оставить пробел в безопасности между всеми сетевыми системами 5G и обеспечить межсетевое взаимодействие.

Литература

1 3GPP TS 33.401, “Technical Specification Group Services and System Aspects: 3GPP System Architecture Evolution (SAE) Security architecture”.

2 3GPP TS 33.501, “Security architecture and procedures for 5G system”.

3 Anand R. Prasad, Sivabalan Arumugam, Sheeba B and Alf Zugenmaier, "3GPP 5G Security", Journal of ICT Standardization (River Publishers, Vol. 6, Iss. 1&2).

4 3GPP TS 33.401, "Technical Specification Group Services and System Aspects: 3GPP System Architecture Evolution (SAE) Security architecture", Release 15, v 15.3.0, March 2018.

5 3GPP TS 33.501, "Security architecture and procedures for 5G system", Release 15, v 15.0.0, March 2018.

6 3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS)", Release 15, v 1.0.0, March 2018.

7 3GPP TS 38.331, "NR-Radio Resource Control (RRC) protocol specification", Release 15, v 15.0.0, March 2018.

8 Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmWave) for 5G: opportunities and challenges," Wireless Networks, vol. 21, no. 8, pp. 2657–2676, 2015.View at: Publisher Site | Google Scholar

9 L. Gavrilovska, V. Rakovic, and V. Atanasovski, "Visions towards 5G: technical requirements and potential enablers," Wireless Personal Communications, vol. 87, no. 3, pp. 731–757, 2016.View at: Publisher Site | Google Scholar

10 "Setting the scene for 5G: opportunities & challenges," https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf.View at: Google Scholar

11 IMT Vision, Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, ITU-R M.2083-0, 2015.

12 European Commission, Commission Recommendation of 26.3.2019 Cybersecurity of 5G networks, European Commission, 2019.

13 Одарченко Р.С., Гнатюк В.А. Концептуальные основы повышения уровня кибербезопасности современных сотовых сетей. Защита информации. 2016. Вып. 22 (2). С. 143-149

14 Одарченко Р.С. Терентьева И.Е., Гнап Р.В., Михайленко К.А. Исследование перспективных технологических решений для сотовых сетей семейства стандартов 5G. Стандартизация, сертификация, качество. 2016. Вып. 6. С.14-19.;

15 Одарченко Р.С. Рост требований к обеспечению информационной безопасности новейших информационно-коммуникационных сетей. ITSEC: сб. материалов доп. учасн.V международной научно-технической конференции, 15-16 мая 2015 Киев. 2015 С. 103-105; 109.

Содержание

Ахметов Б.С., Лахно В.А., Картбаев Т.С., Алимсеитова Ж.К.	ОЦЕНИВАНИЕ ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	5
Ахметов Б.Б., Лахно В.А., Ягалиева Б.Е., Тынымбаев Б.А..	КИБЕРҚАУІПСІЗДІК ЖҮЙЕЛЕРІНЕ ИНВЕСТИЦИЯЛАУ ПРОЦЕСІНДЕ ШЕШІМДЕРДІ ҚОЛДАУДЫҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕСІНІҢ ТҰЖЫРЫМДАМАЛЫҚ ҮЛГІСІ	10
Бегимбаева Е.Е., Тұрғанбай А.Н.	АВТОМАТТАНДЫРЫЛҒАН АҚПАРАТТЫҚ ЖҮЙЕНІҢ ҚОЛЖЕТІМДІЛІКТІ ШЕКТЕУ ЖҮЙЕСІ	15
Бисалиев М.С.	СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ ВОПРОСОВ ОБЕСПЕЧЕНИЯ ПРАВОВЫХ НАЧАЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН	21
Д.С. Дюсенбаев, К.Т. Алғазы, Қ.С. Сақан.	СИММЕТРИЯЛЫ ШИФРЛАРДА ҚОЛДАНЫЛАТЫН СЫЗЫҚТЫ ЕМЕС ТҮЙІНДЕРДІ ЗЕРТТЕУ	34
Е.Е. Исмаил, Н.К. Утелиева, Р. Мулаев, Т.Ауельбеков, А. Кусаинов	ОСОБЕННОСТИ, ТРЕБОВАНИЯ, АТРИБУТЫ И МЕТРИКИ ЗАЩИЩЕННОСТИ ПРОГРАММНЫХ СРЕДСТВ КОСМИЧЕСКОГО НАЗНАЧЕНИЯ	39
Капалова Н.А., Хаумен А., Сулейменов О.Т.	ЛЕГКОВЕСНЫЕ СИСТЕМЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	48
Метелев В.Н., Кожахметов К.Б.	К ВОПРОСУ О СОСТОЯНИИ И ПЕРСПЕКТИВАХ РАЗВИТИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ	54
Мухаев Д.К.	ЖЕЛІЛЕРДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ БҰЗУ ҚАТЕРЛЕРІ МЕН ОСАЛДЫҚТАРЫН АНЫҚТАУ	74
Ордабаева Г.К., Еркін М., Жылқаман Ф., Оразалина Р.	EVE-NG ПЛАТФОРМАСЫ НЕГІЗІНДЕ ЖЕЛІЛІК ШАБУЫЛДАРДЫ МОДЕЛЬДЕУ	80
Усатова О.А., Адилев Е.С.	АУДИТ БЕЗОПАСНОСТЬ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ	85

Шайкулова А.А., Калижанова А.У., Искакова А.Т., Козбакова А.Х., Айткулов Ж.С.	ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ ҚАУІПТЕРІ ЖӘНЕ ОЛАРДАН ҚОРҒАНУ ҚАЖЕТТІЛІГІНІҢ МАҢЫЗДЫЛЫҒЫ	91
Калимолдаев М.Н., Тынымбаев С.Т.	УМНОЖИТЕЛИ ПОЛИНОМОВ ПО МОДУЛЮ ДЛЯ КРИПТОСИСТЕМ НА БАЗЕ НПСС	97
Тынымбаев С.Т., Мукашева А.К., Шайкулова А.А., Әділбекқызы С., Жаксылыков З.Б.	РАЗРАБОТКА УСТРОЙСТВА ДЛЯ ВЫЧИСЛЕНИЯ НОД НА ОСНОВЕ ВЫЧИТАТЕЛЯ	110
С. Тынымбаев, А.Ж. Иманбаев	ИССЛЕДОВАНИЕ И АНАЛИЗ РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ МОБИЛЬНЫХ СЕТЕЙ ПЯТОГО ПОКОЛЕНИЯ	118
Содержание		129

МАТЕРИАЛЫ

Международной научно-практической конференции "Актуальные проблемы информационной безопасности в Казахстане",

11 июня 2021, Алматы, Казахстан

Под редакцией М.Н. Калимолдаева

Подписано в печать 05.06.2020 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 13.76.
Тираж 100 экз. Заказ № 00441.
Отпечатано в ИИВТ МОН РК.
Алматы, ул. Пушкина, 125