ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

1

(136)

Подписывайтесь,

читайте,

пишите в наш журнал

Москва 2022

Все новейшие достижения и современные разработки предприятий оборонного комплекса — в научно-технических журналах ФГУП «НТЦ оборонного комплекса «Компас»

ФГУП «Научно-технический центр оборонного комплекса «Компас» является издателем следующих научных журналов:

Межотраслевой научно-технический журнал

Оборонный комплекс — научно-техническому прогрессу России
(4 выпуска)

Подписной индекс **79379**

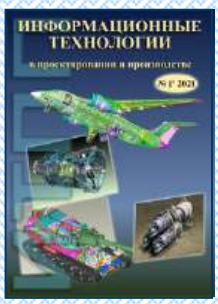
Издается с 1984 года

Межотраслевой научно-технический журнал

Конструкции из композиционных материалов
(4 выпуска)

Подписной индекс **80089**

Издается с 1981 года



Научно-технический журнал

Информационные технологии в проектировании и производстве
(4 выпуска)

Подписной индекс **79378**

Издается с 1976 года

Межотраслевой научно-практический журнал

Экология промышленного производства
(4 выпуска)

Подписной индекс **80090**

Издается с 1993 года

Научно-практический журнал

Вопросы защиты информации
(4 выпуска)

Подписной индекс **79187**

Издается с 1974 года

Все издания ФГУП "Научно-технический центр оборонного комплекса «Компас»:

✓ *включены решением ВАК Министерства науки и высшего образования России в перечень ведущих рецензируемых научных журналов и изданий, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата и доктора наук;*

✓ *метаданные выпусков включены в базу данных Российского индекса научного цитирования (РИНЦ).*

Более подробную информацию об изданиях, подписке, дополнительных услугах можно получить
по тел.: 8 (495) 491-43-17, 8 (495) 491-77-67, 8 (495) 491-77-20 (*подписка*);
факс: 8 (495) 491-44-80.
E-mail: izdanie@ntckompas.ru

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР ОБОРОННОГО КОМПЛЕКСА «КОМПАС»
(ФГУП «НТЦ ОБОРОННОГО КОМПЛЕКСА «КОМПАС»)

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

1 (136)

Москва 2022

Основан в 1974 г.

С О Д Е Р Ж А Н И Е

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2022.
Вып. 1 (136). С. 1—60.

Редактор *О. А. Константинова*
Компьютерная верстка: *Н. В. Ильина*, *К. В. Трыкина*

Подписано в печать 15.03.2022. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 7,0. Уч.-изд. л. 7,2.
Тираж 400 экз. Заказ 1990. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано: 101000, Москва,
Лубянский проезд, д. 15, стр. 4, офис 105.
ИП Кириченко Алексей Викторович.
Индекс 79187.

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004
DOI: 10.52190/2073-2600_2022_1_3

Использование доверительных систем в целях обеспечения информационной безопасности и ограничения несанкционированного доступа для информационных систем финансовых организаций

Д. П. Дубинин
Московский авиационный институт (национальный исследовательский университет),
Москва, Россия

Изучен вопрос обеспечения информационной безопасности для информационных систем финансовых организаций за счет интеграции доверительных систем и сред. Предпринята попытка систематизации знаний, касающихся темы представленного исследования. Преимущественная часть работа посвящена именно научному исследованию обеспечения информационной безопасности посредством доверительных сред.

Ключевые слова: информационная безопасность, информация, доверительная среда, финансовая система, несанкционированный доступ.

Посредством информационной безопасности (ИБ) производится ограничение несанкционированного доступа (НСД) и, как следствие, создается препятствие экономическим и материальным потерям организации. Без должного уровня обеспечения ИБ современные активно развивающиеся в аспекте информационных технологий организации имеют риски утери корпоративной информации, персональных данных и иной информации, имеющей ограниченный круг доступа [1].

Разработаны и активно интегрируются множественные способы обеспечения ИБ и поддержания стабильной работы информационных систем организаций. Так, к примеру, в электронных системах интегрируются различные методы шифрования данных, аппаратные и программные средства. Помимо этого на физическом уровне устанавливают различные средства контроля и управления доступом, датчики и иные технологии. В представленной работе автор подробно раскрывает вопрос, касающийся обеспечения информационной безопасности за счет доверительных сред в информационных системах финансовых организаций. Именно финансовые организации предъявляют наиболее жесткие требования к обеспечению уровня ИБ ввиду наличия множественной корпоративной и иной засекреченной информации, имеющей высокую значимость.

Методы

Автор использует теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных изучены научные работы отечественных и зарубежных авторов [1—3]. В каждой из данных работ затронуты фундаментальные вопросы, необходимые для воспроизведения общего анализа, касающегося обеспечения защиты информационных систем финансовых организаций за счет интеграции доверительных сред.

В используемой автором настоящей статьи литературе рассмотрены такие вопросы, как доверенные системы для разграничения доступа к информации в облачных инфраструктурах, описание подхода программной реализации модуля доверенной загрузки операционной системы, информационная безопасность в финансовом секторе (киберпреступность и стратегия противодействия), доверительные среды как инструмент информационной безопасности и другие.

Дубинин Дмитрий Павлович, преподаватель кафедры РВСН ВУЦ.
E-mail: dubinindp@yandex.ru

Статья поступила в редакцию 22 декабря 2021 г.

Актуальность и взаимосвязь киберпреступности и финансового сектора в современных реалиях

В целях повышения эффективности и производительности работы современные финансовые организации активно интегрируют передовые информационные и цифровые технологии. Именно данный фактор является основополагающим в аспекте нападения киберпреступников. На рис. 1 представлены основные киберугрозы, которым подвергаются современные финансовые организации [2].

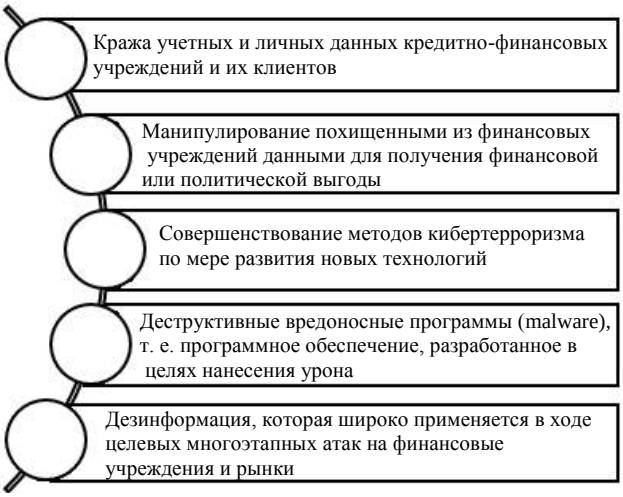


Рис. 1. Киберугрозы финансовых организаций

Информационные системы финансового сектора являются наиболее уязвимыми относительно кибератак. Данный фактор является следствием того, что финансовые организации — это достаточно привлекательный объект ввиду движения в их рамках денежных средств. Необходимо отметить, что успешная атака на одну из организаций способна быстро распространиться через множество взаимосвязей, объединяющих единую финансовую систему. Также одним из основных факторов является то, что современные финансовые системы все еще используют устаревшие системы информационной безопасности, что повышает шансы на успешность кибератаки, которая может вызвать существенные последствия в виде финансовых убытков и ухудшения репутации.

Доверительные системы в качестве основного инструмента для препятствия несанкционированного доступа к информационным системам

Для современных финансовых организаций критически важна надежная система информационной безопасности, обеспечивающая надежную защиту данных от НСД. Наряду с этим системы ИБ обязаны обеспечивать должный уровень конфиденциальности, целостности и доступности информации [3].

Одним из основных средств решения данной задачи является доверенная среда. Разработка доверенных систем для информационных систем финансовых организаций — это использование комплексов оборудования в целях обеспечения устойчивости критически важных информационных систем и защиты информации. Основными частями доверенной платформы выступают аппаратное обеспечение, программное обеспечение и элементная база.

На рис. 2 представлена функциональная схема принципа работы доверительной системы при установке нового программного обеспечения или обновлении старого.

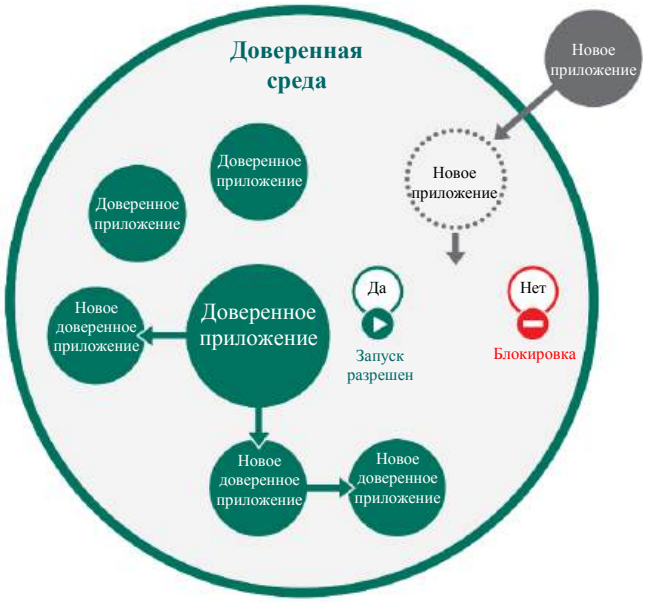


Рис. 2. Принцип работы доверительной среды при установке ПО

Видно, что если приложение уже установлено в систему и считается доверенным, то новая версия приложения, загруженная из доверенного источника, также будет считаться доверенной, поскольку она получена в доверенной среде. Это позволяет программам, уже установленным в систему, беспрепятственно обновляться, не нарушая доверенности системы. Таким образом, проблемы с обновлением установленного программного обеспечения отсутствуют [4].

Таким образом, меры для защиты безналичных расчетов должны быть направлены на:

- создание и поддержание вычислительной среды, в которой программы исполняются корректно;
- точную идентификацию, аутентификацию и авторизацию пользователя;

- разграничение доступа к ресурсам системы;
- реализацию тех участков ИТ, которые не могут контролироваться банком, с использованием технических средств, предназначенных для работы вне доверенной среды;
- надежную фиксацию событий в системе.

Доверенная среда Keystone в качестве инструмента обеспечения информационной безопасности в финансовых организациях

Keystone представляет собой open source компонент, способный организовывать доверенную среду для запуска программ на базе архитектуры RISC-V.

Данный компонент является изолированной областью главного процессора, имеющего набор механизмов безопасности. Необходимо отметить, что код и данные, имеющиеся в данной области, надежно защищены относительно изменений и вмешательства извне. Основной смысл в том, что в этих анклавах можно проводить операции над персональными и конфиденциальными данными, не боясь их компрометации, поскольку доступ к этим областям процессора не имеют ни операционная система, ни другие приложения.

Концепция Keystone базируется на технологиях SGX и анклав-платформе Sanctum Processor, разработанной в MIT. В общем виде схема реализации системы с анклавом на RISC-V показана на рис. 3.

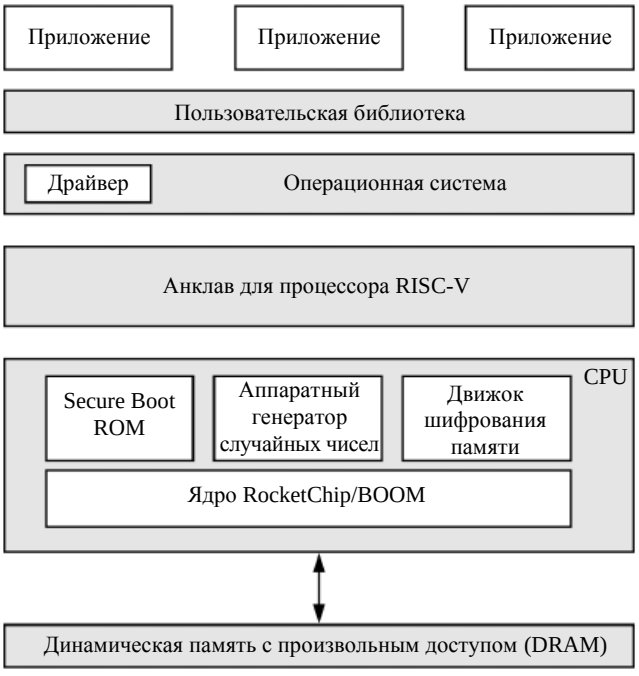


Рис. 3. Схема реализации доверенной системы с анклавом на RISC-V

Таким образом, Keystone представляет собой один из самых мощных инструментов для построения доверенной среды финансовых организаций. Уникальные алгоритмы работы данного компонента позволяют обеспечить должный уровень работы систем информационной безопасности и снизить риски несанкционированного доступа [5].

Заключение

Таким образом, в представленной работе изучены основные аспекты, касающиеся обеспечения информационной безопасности финансовых организаций на основе построения доверительной среды. Обозначены такие моменты, как актуальность обеспечения информационной безопасности в современных финансовых организациях, актуальность и взаимосвязь киберпреступности и финансового сектора в современных реалиях, киберугрозы финансовых организаций, доверительные системы в качестве основного инструмента для препятствия несанкционированного доступа к информационным системам, доверенная среда Keystone в качестве инструмента обеспечения информационной безопасности в финансовых организациях.

Необходимо отметить, что финансовый сектор является одним из самых актуальных в аспекте кибератак направлений, что связано с непрерывными денежными потоками и переводами в рамках информационных систем данных организаций. Исходя из этого, представители таких организаций обязаны вкладывать ресурсы и прилагать усилия для обеспечения должного уровня информационной безопасности в целях снижения рисков НСД и повышения уровня доверия к организации [6].

Литература

1. *Паращук И. Б., Саенко И. Б., Пантюхин О. И.* Доверенные системы для разграничения доступа к информации в облачных инфраструктурах // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 6. С. 68—75.

2. *Боровиков А. Ю., Новиков К. Б., Маслов О. А.* Описание подхода программной реализации модуля доверенной загрузки операционной системы // Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 1. С. 43—48.

3. *Капгер И. В., Журилова Е. Е., Миронова А. А.* О разработке учебно-лабораторного стенда для изучения аппаратного модуля доверенной загрузки "Аккорд" // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2016. № 17. С. 131—142.

4. *Семеко Г. В.* Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. 2020. № 1(1). С. 77—96.

5. *Кудрявцева Ю. В.* Инновационные финансовые технологии и операционные риски в сфере дистанционного банковского обслуживания // Финансовая аналитика: проблемы и решения. 2017. Т. 10. № 6(336). С. 647—662. DOI: 10.24891/fa.10.6.647

6. *Ревенков П. В., Бердюгин А. А.* Компьютерные атаки как источник операционного риска в условиях электронного банкинга // Финансы и кредит. 2018. Т. 24. № 3(771). С. 629—640. DOI: 10.24891/fc.24.3.629.

The use of trust systems in order to ensure information security and restrict unauthorized access to information systems of financial organizations

D. P. Dubinin
Moscow Aviation Institute (National Research University), Moscow, Russia

The presented article is devoted to the study of information security for information systems of financial organizations through the integration of trust systems and environments. The scientific significance of the work lies in the attempt to systematize knowledge related to the topic of the presented research. The predominant part of the article is devoted specifically to the study of the issue of ensuring information security through trust environments.

Keywords: information security, information, trust environment, financial system, unauthorized access.

Bibliography — 6 references. *Received December 22, 2021*

УДК 004.00
DOI: 10.52190/2073-2600_2022_1_7

Обеспечение информационной безопасности посредством построения комбинированных систем контроля и управления доступом

В. В. Кабаков
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Проведено изучение инновационного подхода к обеспечению информационной безопасности, связанного с построением комбинированных систем контроля и управления доступом. Решен ряд задач, посредством которых доказано гипотеза о том, что такие инструменты обеспечения информационной безопасности являются достаточно эффективными и качественными. Научная новизна заключается в методологическом изучении инновационного метода построения систем контроля и управления доступом.

Ключевые слова: информационная безопасность, система контроля, управление доступом, комбинация, информация.

Проблема обеспечения информационной безопасности продолжает иметь огромное значение. В большей степени данный фактор является следствием повсеместной цифровизации общества, а также бытовых и профессиональных сфер жизнедеятельности человека. Именно недостаточный уровень обеспечения информационной безопасности способен привести к колоссальным потерям материального и экономического характера [1].

Другой причиной необходимости развития систем информационной безопасности, в частности систем контроля и управления доступом (СКУД), является совершенствование алгоритмов и проводимых ими махинаций киберпреступников. Повсеместная цифровизация общества порождает различные кибернетические атаки. Исходя из этого для обеспечения должного уровня работы информационных систем на предприятиях необходимо повсеместное развитие и повышение уровня обеспечения информационной безопасности в специализированных системах.

Цель работы — решение проблемы необходимости разработки интеграции инновационных комбинированных СКУД. Рассмотрены отдельные аспекты, касающиеся темы исследования, а также сделаны уникальные выводы и умозаключения.

Методы

Автором использованы теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных использованы научные материалы отечественных и зарубежных авторов, таких, как Голубкин Н. Д., Терехов К. Г., Yeletskaya T. A., Balabanova T. N., Gakhova N. N., Марьенков А. Н., Кузнецова В. Ю. и другие [1—4]. В данных работах затрагиваются фундаментальные вопросы, необходимые для воспроизведения общего анализа, касающегося обеспечения информационной безопасности посредством разработки и интеграции инновационных СКУД. В них раскрываются такие вопросы, как тенденции развития систем контроля и управления доступом в помещение, направления совершенствования систем контроля и управления доступом для радиационно-опасных объектов, применение технологий распознавания лиц в системах контроля и управления доступом, комбинация технологий СКУД.

Обеспечение информационной безопасности за счет интеграции систем контроля и управления доступом

Системы контроля и управления доступом — это совокупность совместимых между собой средств аппаратного и программного уровня. Каждый из данных инструментов направлен на ограничение доступа людей, транспорта и иных объектов в те или иные помещения или на те или иные территории. Именно посредством СКУД происходит предупреждение несанкционированного доступа к засекреченной, корпоративной или иной информации на объекте.

Системы контроля и управления доступом имеют достаточно примитивный вид (считыватель, приемник, сервер и т. д.). На рис. 1 представлен пример СКУД на предприятии, основанный на пропусках и турникетах.

Кабаков Виталий Валериевич, старший преподаватель кафедры 104.
E-mail: ser-kvv73@mail.ru

Статья поступила в редакцию 26 декабря 2021 г.

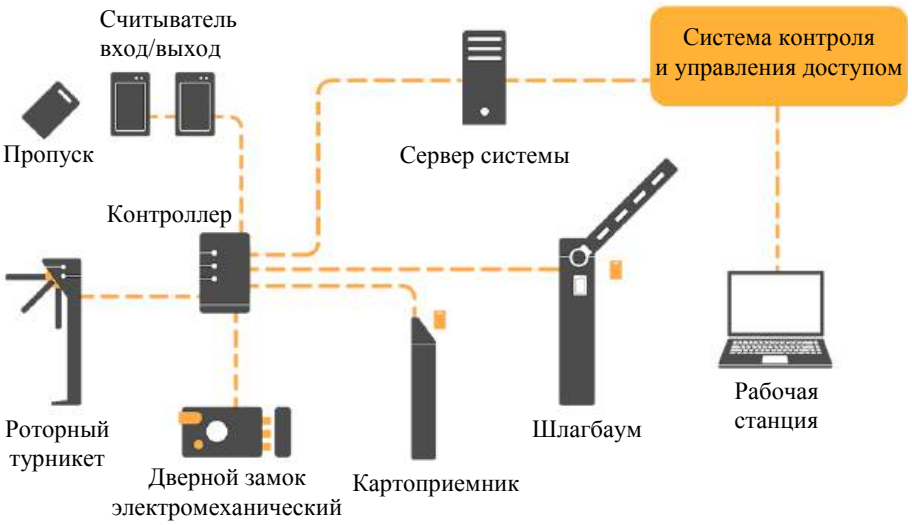


Рис. 1. Примитивная схема СКУД

СКУД устаревают ввиду интенсивного распространения и улучшения алгоритмов работы хакерских атак на информационные системы предприятия. Таким образом, необходимо незамедлительно развивать и совершенствовать, интегрируя инновационные алгоритмы и технологии [2].

Развитие систем контроля и управления доступом

Одним из наиболее актуальных и эффективных направлений инновационного развития СКУД является интеграция интеллектуальных технологий, в частности средств видеонаблюдения, в целях автоматического выявления несанкционированного доступа. Это стало возможным благодаря развитию фотокамер и переходу на цифровые аппараты, имеющие высокую четкость. Перспективные средства видеонаблюдения способны в автоматическом режиме детектировать движение в указанных областях кадра, а также выполнять многокамерное сопровождение объекта, измеряя статистические и биометрические признаки человека [3].

Другим перспективным решением для СКУД является нанесение на документы RFID-идентификаторов. Активный радиочастотный идентификатор, представляющий собой наклейку, позволит отслеживать местонахождение предметов и документов в реальном времени. Также является перспективным использование активных RFID-пропусков для бесконтактной идентификации. Преимущество этой технологии особенно проявляется в аварийных ситуациях в условиях свободного прохода, когда сохраняется возможность зарегистрировать всех лиц, покинувших охраняемую зону.

В целях защиты информационных активов в СКУД могут быть использованы направления, приведенные на рис. 2.

Также стоит отметить основные аспекты, характеризующие пути развития СКУД, которые, по-видимому, будут связаны с разработками, направленными на получение указанных на рис. 3 результатов.

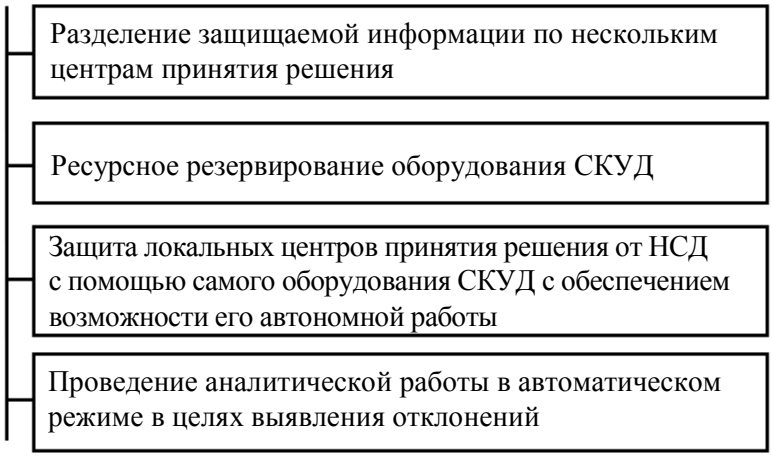


Рис. 2. Направления защиты информации в СКУД

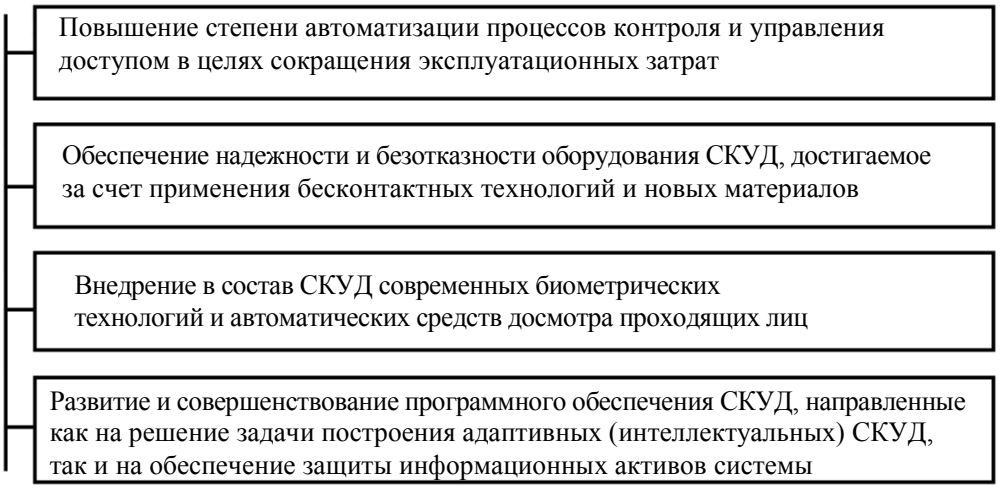


Рис. 3. Пути развития СКУД

Необходимо подчеркнуть, что наиболее перспективным вариантом развития СКУД является разработка комбинированных систем, имеющих множество специализированных программ и функций и наибольшую эффективность в отказе от несанкционированного доступа [4].

Комбинированные системы контроля и управления доступом как инновационная технология обеспечения информационной безопасности

Разработчики и производители комбинированных средств аутентификации предоставляют на рынок инновационные решения, включающие биометрические карты. Основным преимуществом данной технологии является возможность не устанавливать биометрические считыватели, а использовать установленные считыватели смарт-карт. На биометрической карте находятся 3D-сканер отпечатков пальцев и RFID-чип, посредством которого обеспечивается поддержка популярных технологий по стандарту ISO 14443. Такой способ обновления СКУД является весьма экономным способом перехода с устаревших технологий, использующих проксимити-карты, на биометрические технологии.

В комбинированных системах контроля и управления доступом (рис. 4) карта на только является носителем данных о доступе пользователя, но и выступает в роли флешки, посредством которой база данных СКУД и точки доступа обмениваются информацией в обоих направлениях. Для того чтобы этот обмен происходил максимально оперативно и комфортно, производится комбинация различных типов точек доступа в одной системе.

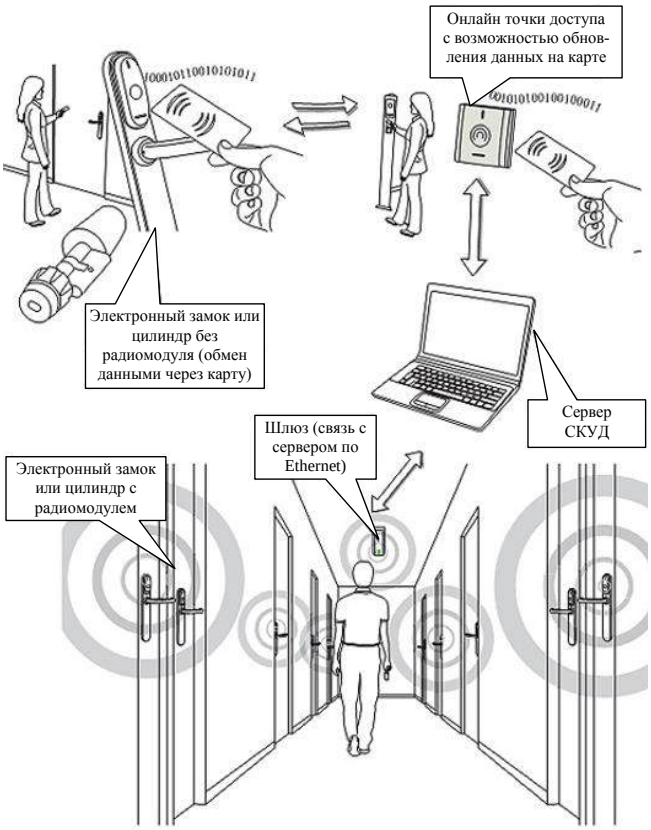


Рис. 4. Схема комбинированной СКУД

Основное отличие онлайн-контроллеров СКУД комбинированной системы от «обычных» состоит в том, что они не просто работают в режиме реального времени, но также выполняют роль промежуточного портала в обмене данными между картой и БД СКУД. В момент прохода через такую точку доступа карта «соединяется» с БД СКУД и происходит описанный двухсторонний обмен данными [5].

Заключение

Таким образом, основной целью данной статьи являлось изучение актуальности и перспективности использования комбинированных систем контроля и управления доступом для защиты информации на предприятии. В результате решены следующие задачи: изучены необходимость развития СКУД, направления защиты информации в СКУД, пути инновационного развития СКУД, основные аспекты, касающиеся использования и разработки комбинированных систем контроля и управления доступом.

В заключение необходимо отметить, что цифровизация ставит перед современным обществом огромное количество задач, связанных с обеспечением информационной безопасности. Именно за счет должного уровня обеспечения информационной безопасности современные предприятия смогут ограничить материальные и экономические потери, а также рационализировать свою деятельность.

Литература

1. *Голубкин Н. Д.* Тенденции развития систем контроля и управления доступом в помещение // Вестник магистратуры. 2021. № 4—3(115). С. 17—19.
2. *Терехов К. Г.* Направления совершенствования систем контроля и управления доступом для радиационно-опасных объектов // Глобальная ядерная безопасность. 2018. № 3(28). С. 23—24.
3. *Девицына С. Н., Елецкая Т. А., Балабанова Т. Н., Гахова Н. Н.* Разработка интеллектуальной системы биометрической идентификации пользователя // Научные ведомости белгородского государственного университета. Сер. «Экономика. Информатика». 2019. Т. 46. № 1. С. 148—160.
4. *Марьенков А. Н., Кузнецова В. Ю., Гелагаев Т. М.* Применение технологий распознавания лиц в системах контроля и управления доступом // Прикаспийский журнал: управление и высокие технологии. 2021. № 1(53). С. 83—90.
5. *Зудинов А. С.* Внедрение биометрии в системы контроля доступа на объектах критической информационной инфраструктуры // StudNet. 2021. Т. 4. № 5. Порядковый номер: 162. DOI: 10.24411/2658-4964-2021-10347.

Ensuring information security by building combined access control and management systems

V. V. Kabakov
Moscow Aviation Institute (National Research University), Moscow, Russia

The presented work is devoted to the study of an innovative approach to information security related to the construction of combined access control and management systems. The author solves a number of problems by means of which the hypothesis is proved that such tools for ensuring information security are sufficiently effective and of high quality. The scientific novelty lies in the methodological study of the innovative method of building access control and management systems.

Keywords: information security, control system, access control, combination, information.

Bibliography — 5 references. *Received December 26, 2021*

УДК 004.056.5
DOI: 10.52190/2073-2600_2022_1_11

Обоснование потребности в разработке методики выбора средств защиты информации для реализации системы защиты информации от несанкционированного доступа

В. А. Пиков; В. А. Кайгородова
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

О. В. Батманова
АНОВО "Российский новый университет", Москва, Россия
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, Москва, Россия

Статья посвящена актуальным вопросам информационной безопасности информационных систем различного предназначения. Детально рассмотрено понятие системы защиты информации от несанкционированного доступа. Выполнен анализ подходов к формированию комплекса мер по защите информации и обеспечению должного уровня информационной безопасности. Сформулирован подход к формированию перечня актуальных угроз безопасности информации информационных систем. На основании результатов анализа сделаны выводы о том, что существует потребность в дальнейшей работе по созданию методики выбора средств защиты информации, реализующих систему защиты информации от несанкционированного доступа.

Ключевые слова: защита информации, информация, информационная безопасность, корпоративная сеть, методы защиты информации, политика безопасности, система защиты безопасности, эффективность защиты информации.

Информация и информационные ресурсы занимают лидирующее место среди главных источников успеха любого предприятия. Как и любое достояние, информацию нужно охранять. Важное значение приобретает конфиденциальная информация. Это особая каста среди всех видов информации, отличающаяся высокой ценой для бизнеса. Информационный ресурс становится одним из главных источников экономической эффективности любого предприятия. Все сферы деятельности организаций зависимы от состояния информационных систем и имеющихся в них информационных ресурсов. Безопасность фирм в основном складывается из безопасности их информации. Основные угрозы — угрозы в сфере информационного обеспечения. Киберпреступники, хакеры — главная угроза для всех сфер человеческой деятельности. Только защитив свои информационные ресурсы, бизнес может спокойно развиваться.

Принятие решений во всех сферах жизнедеятельности предприятия или организации все в большей степени базируется на информационных процессах. Глубокий анализ этих процессов с последующей выработкой управляющих решений осуществляется на основе информационных моделей, построенных на современных информационно-телекоммуникационных технологиях. Поэтому защита информации представляет собой самостоятельную составляющую безопасности предприятия в целом, значение которой с каждым годом растет.

Наблюдается тенденция, в соответствии с которой все сферы жизнедеятельности предприятия становятся зависимыми от информационного развития, в процессе которого они сами порождают информацию и сами же ее потребляют. Информация — основное средство зарабатывания денег.

Негативными последствиями успешного проведения информационных атак могут стать компрометация или искажение конфиденциальной информации, навязывание ложной информации, нарушение политик правил сбора, обработки и

Пиков Виталий Александрович, старший преподаватель кафедры 402 "Радиосистемы и комплексы управления, передачи информации и информационная безопасность".
E-mail: pikov@ya.ru
Кайгородова Вера Андреевна, ассистент кафедры 101 "Проектирование и сертификация авиационной техники".
E-mail: vakajgorodova@mai.education
Батманова Ольга Викторовна, заместитель заведующего кафедрой "Телекоммуникационные системы и информационная безопасность", старший преподаватель факультета финансов и банковского дела.
E-mail: bat-olga@yandex.ru

Статья поступила в редакцию 13 декабря 2021 г.

передачи информации, отказы и сбои в работе технических систем, вызванные преднамеренными и непреднамеренными действиями как со стороны конкурентов, так и со стороны преступных сообществ, организаций и группировок иностранных государств. К одной из наиболее важных задач в области безопасности предприятия следует отнести создание системы защиты информации. Обеспечение комплексности как всеохватывающего средства защиты — одна из самых главных задач.

Эффективный бизнес всегда экономичен. Сфера защиты информации — очень затратное направление деятельности. Иметь на предприятии огромное множество средств защиты информации нерентабельно. Современный бизнес чётко просчитал, что именно за комплексными, универсальными решениями будущее защиты информации. Лучше выбрать одно, но проверенное средство защиты от надёжного поставщика, чем купить много с сомнительной репутацией.

Комплексные решения в области защиты информации позволяют унифицировать рабочие места, создавать ситуационные центры для оперативного реагирования на угрозы безопасности. Не всегда, приобретая комплексное решение, удаётся сэкономить сразу. Первичные траты, такие, как стоимость покупки и внедрения, могут быть весьма ощутимыми. Только со временем эти затраты превратятся в прибыль. Практика установки таких серьёзных решений в организации, показала, что окончательное внедрение оправдывает себя. Как показал опыт внедрения DLP-системы "СёрчИнформ Контур информационной безопасности", 99 % предприятий через считанные месяцы бесплатного, тестового использования комплексных решений в области безопасности информации с огромным желанием переходят на платный режим, однозначно осознав все плюсы защищённости своих бизнес-критичных данных [1].

Материалы и методы

При проектировании информационных систем важное место отводится проработке комплекса организационно-технических мер по защите обрабатываемой информации для обеспечения должного уровня информационной безопасности. Для решения вопросов построения комплексной защиты информации необходимо определить такие, казалось бы, однозначные понятия, как:

- защита информации;
- система защиты информации;
- средство защиты информации;
- объект защиты.

Если воспользоваться поиском по нормативно-технической документации, то можно найти более 30 формулировок термина "защита информации".

Так, например, в соответствии с ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" (англ. Protection of Information. Basic Terms and Definitions):

"2.1.1 **защита информации;** ЗИ: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию", там же далее: "2.3.6 **защита информации от несанкционированного доступа;** ЗИ от НСД: защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации" [2].

Формулировка понятия системы защиты информации и безопасности данных:

"2.4.3 **система защиты информации:** совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

2.4.5 **безопасность информации (данных):** состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность" [2].

В специализированной литературе встречаются достаточно конкретные формулировки терминов: "Система защиты информации от несанкционированного доступа (СЗИ от НСД) — комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах" [3].

"Система защиты информации — комплекс организационных мер и программно-технических средств обеспечения безопасности информации в автоматизированных системах [4].

"…применительно к условиям информационного противоборства термин **"защита информации от НСД"** включает все аспекты обеспечения безопасности информации:

- обеспечение конфиденциальности (защита информации от несанкционированного чтения или копирования);
- обеспечение целостности (защита информации от несанкционированного изменения или разрушения);

- обеспечение доступности (защита информации от блокирования)" [5].

Согласно действующим руководящим документам ФСТЭК России, конкретно по Руководящему документу "Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации". Гостехкомиссия (ФСТЭК) России, 1992 г.:

"2.2. В общем случае комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности" [6].

Защита информации — комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности. Система защиты информации — совокупность ресурсов персонала структурных подразделений по защите информации, используемых способов и средств защиты информации, а также объектов защиты, организованная и функционирующая по правилам и нормам, установленным нормативно-правовыми актами в области защиты информации. Базовым законом в информационной сфере является Федеральный закон 149-ФЗ "Об информации, информационных технологиях и о защите информации", общие понятия и принципы которого распространяются на всю информационную сферу за исключением случаев, когда конкурируют общая и специальная нормы.

В общем случае будем считать, что система защиты информации — это комплекс программно-технических средств и организационных мер обеспечения безопасности информации в информационных системах предприятий (организаций).

Важно также определиться с понятием комплексности. Один из источников гласит, что комплексность (от лат. *complexus* — связь) — это полнота, системность, взаимоувязанность, например анализа, планирования, управления [7].

Комплексная система защиты информации должна отвечать следующим требованиям:

- оперативно реагировать на изменение факторов, определяющих методы и средства защиты информации;
- иметь удобную и достаточно надежную ключевую систему (ключи шифрования), обеспечивающую безопасность при работе с информацией;
- иметь элементы идентификации (аутентификация, авторизация, доступ) пользователей;
- обеспечивать надежность контроля передаваемой и хранимой финансово-экономической информации;
- обеспечивать проведение учёта и расследования случаев нарушения безопасности (инциденты безопасности);
- использовать комплекс программно-технических средств и организационных мер по защите комплексной системы [8].

Следует учитывать, что система защиты информации организации в целом является сложным объектом, выполняющим множество функций. Для каждого структурного элемента системы защиты информации и каждой выполняемой функции возможно применение различных сертифицированных программных и технических средств, во множестве представленных на рынке. Следовательно, в конкретном случае можно построить множество вариантов систем защиты информации, отличающихся структурой, составом, технико-экономическими показателями (быстродействие, надежность, стоимость и т. д.). Поскольку подобные показатели нередко бывают взаимно противоречивыми, то при выборе конкретного комплекса средств защиты информации необходимо решать оптимизационную задачу, требующую наличия показателей эффективности защиты информации и соответствующих критериев построения адекватной защиты.

Руководствуясь ГОСТ Р 56498-2015 "Сети коммуникационные промышленные. Защищённость (кибербезопасность) сети и системы", введём некоторые понятия, необходимые для исследования:

"3.1.2 **источник угрозы** (*adversary*): логический объект, совершающий атаку на систему или представляющий для нее угрозу.

[RFC 2828]

…

3.1.4 **имущественный объект** (*asset*): что-либо, представляющее ценность для организации.

[ИСО/МЭК 13335-1:2004]

…

3.1.6 **атака** (*attack*): попытки уничтожить, подвергнуть опасности, преобразовать или вывести из строя информационную систему и/или содержащуюся в ней информацию или иным образом затронуть политику безопасности.

[ИСО/МЭК 18043]

3.1.7 **поверхность атаки** (*attack surface*): совокупность ресурсов системы, которые напрямую или косвенно подвержены потенциальному риску атаки.

…

3.1.18 **незащищенный, незащищенность** (*exposed, exposure*): состояние уязвимости и отсутствия защиты против атаки.

…

3.1.24 **усилить защиту, усиление защиты** (*harden, hardening*): удаление ненужных функций для уменьшения физических, логических и/или организационных уязвимостей.

…

3.1.26 **инцидент** (*incident*): событие безопасности или комбинация множественных событий безопасности, ставящих под угрозу безопасность.

…

3.1.32 **несанкционированное проникновение** (*intrusion*): инцидент, при котором неуполномоченный логический объект, т. е. злоумышленник, получает или явно пытается получить доступ к служебным ресурсам системы.

[RFC 2828, изменен]

3.1.33 **детектирование несанкционированных проникновений** (*intrusion detection*): сервис безопасности, который позволяет отслеживать и анализировать системные события в целях выявления и уведомления в режиме реального или почти реального времени о попытках получения несанкционированного доступа к ресурсам системы.

[RFC 2828]

…

3.1.37 **контрмера** (*countermeasure*): действие, устройство, процедура или стратегия, ослабляющие угрозу, уязвимость или противодействующие атаке путем ее отражения или предотвращения или минимизации ущерба, который она способна нанести, или путем ее обнаружения и сообщения о ней, чтобы могло быть предпринято корректирующее действие.

[RFC 2828]

…

3.1.52 **риск** (*risk*): сочетание вероятности события и его последствия, где вероятность — это количественная оценка возможности того, что это событие произойдет.

[ИСО/МЭК Руководство 73:2002]

Примечание — последствием называется ущерб для имущественных объектов.

3.1.53 **защищенный, защищенность** (*secure, security*): продукт, система или сервис считаются защищенными в такой степени, что их пользователи могут рассчитывать на то, что они функционируют (или будут функционировать) надлежащим образом. Это понятие обычно рассматривают в контексте оценки фактических или ощущаемых угроз.

[ISO/IEC/TR 15443-1].

3.1.56 **мера безопасности** (*security measure*): мера защиты против возможного нарушения безопасности защищенной системы.

…

3.1.62 **угроза** (*threat*): потенциальная возможность для нарушения безопасности при наличии обстоятельства, средства, действия или события, способных нарушить безопасность и нанести ущерб.

[RFC 2828]" [9].

Исходя из определений следует, что для построения системы защиты информации от несанкционированного доступа необходимо:

- выполнить описание объекта защиты — информационной системы и её защищаемых ресурсов — с обязательным определением максимального уровня конфиденциальности обрабатываемой информации;
- определить множество актуальных угроз безопасности информации для информационной системы и изложить их в виде модели угроз, проведя их анализ.

Выполним описание объекта защиты — информационной системы и её защищаемых ресурсов.

К защищаемым ресурсам в информационной системе, как правило, относят:

- информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию, и информационные ресурсы, представленные на магнитных, оптических и других носителях, а также хранящиеся в оперативной памяти вычислительных средств;
- средства автоматизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (общее и специальное программное обеспечение), системы связи и передачи данных и т. д.

Модель угроз безопасности информации содержит описание изделия, угрозы безопасности информации, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

Согласно ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [2].

Состав угроз зависит от свойств защищаемого объекта и особенностей его функционирования.

Угрозы информационной безопасности могут быть реализованы по техническим каналам утечки данных и путём несанкционированного доступа к защищаемой информации.

Основные свойства безопасности информации, нарушение которых необходимо предотвратить

реализацией комплекса мер по защите информации, — нарушение конфиденциальности, целостности, доступности.

Нарушение доступности представляет собой создание таких условий, при которых доступ к информации будет либо заблокирован, либо возможен за время, недостаточное для выполнения поставленных задач.

Угрозы нарушения целостности связаны с модификацией информации, обрабатываемой в информационной системе.

Угрозы нарушения конфиденциальности информации направлены на создание условий для несанкционированного ознакомления с информацией ограниченного доступа лицами, не имеющими соответствующих полномочий [2].

Результаты

Сформулируем подход к формированию перечня актуальных угроз безопасности информации информационных систем. Для различных сред функционирования формируются перечень актуальных угроз в соответствии с описанным далее алгоритмом.

Рассмотрим алгоритм формирования перечня актуальных угроз.

Во-первых, в качестве исходного перечня используют Банк данных угроз, определённый ФСТЭК России (https://bdu.fstec.ru/).

Во-вторых, из множества перечня угроз удаляют угрозы, не реализуемые в конкретной информационной системе. Например, если не применяются облачные технологии или станки с числовым программным управлением, то эти угрозы не рассматриваются как актуальные.

В-третьих, для каждой актуальной угрозы определяют способы (меры) защиты. Примерами таких мер может служить использование:

- средств антивирусной защиты;
- сертифицированного по требованиям безопасности информации средства защиты;
- средства контроля целостности операционной системы и используемого программного обеспечения.

В целях экономии финансов, а также для минимизации числа одновременно используемых на хостах компьютерной сети программных (программно-аппаратных) средств защиты информации рационально применять комплексные решения. Такие решения позволяют сразу нейтрализовать все (или почти все) актуальные для данной информационной системы угрозы безопасности информации.

Одним из популярных средств защиты информации от несанкционированного доступа, обеспечивающим эффект комплексности, является решение "Secret Net Studio" от российской компании "Код Безопасности". "Secret Net Studio" обеспечивает безопасность рабочих станций и файловых серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования [10—12].

Говоря о конкретных продуктах, "Secret Net Studio" является одним из самых важных средств для защиты информации. Выгода его применения аргументируется возможностью полной настройки политики безопасности информации. Данный продукт однозначно является одним из лидеров в своём сегменте, чего нельзя сказать про продукт "vGate", который на данный момент не совсем доработан и уступает своим иностранным конкурентам [10—12].

Рассмотрим некоторые защитные механизмы "Secret Net Studio" более подробно. Значительную часть работ по защите информации составляют задачи обеспечения безопасности рабочих станций и серверов (защита узлов локальной сети). Для их решения применяют продукты класса "Endpoint Security", которые компенсируют внутренние и внешние угрозы с помощью различных подсистем безопасности (антивирусная защита узла, защита узла от несанкционированного доступа, персональный межсетевой экран и т. д.) [10—12].

"Secret Net Studio" прошёл сертификацию ФСТЭК России, Минобороны России и выполняет требования регуляторов при аттестации (оценке соответствия) информационных систем, в которых обрабатывается конфиденциальная информация, на соответствие различным требованиям российского законодательства (таким, как, защита государственных информационных систем до класса К1, защита персональных данных до УЗ1, автоматизированных систем до класса 1Б включительно (гостайна с грифом "совершенно секретно" и т. д.) [10—12].

Обсуждение

Анализ данных о комплексном средстве защиты информации от несанкционированного доступа "Secret Net Studio" от компании "Код Безопасности", полученный из официальных источников, к сожалению, не позволяет сказать точно, от каких угроз безопасности информации из Банка данных угроз, определённого ФСТЭК России (https://bdu.fstec.ru/), оно защищает, требуется ли устанавливать дополнительные средства защиты информации на рабочих местах (хостах) информационной системы.

Заключение

Конфиденциальная информация, обрабатываемая в информационных системах, должна быть защищена. Это требование не только регуляторов в области обеспечения информационной безопасности, но и здравого смысла.

В результате проведённого исследования обнаружено противоречие, заключающееся в потребности применения в информационных системах комплексных средств защиты информации от несанкционированного доступа и отсутствии полных данных о "закрываемых" ими угрозах. При создании систем защиты информации от несанкционированного доступа в информационных системах количество применяемых средств защиты информации должно быть минимальным в целях экономии финансовых средств и общих вычислительных ресурсов.

Дальнейшая разработка методики выбора средств защиты информации для реализации системы защита информации от несанкционированного доступа является актуальной научной задачей.

Литература

1. DLP-система "СёрчИнформ Контур информационной безопасности" [Электронный ресурс]. Режим доступа: https://searchinform.ru/products/kib/ (дата обращения: 01.11.2021).
2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.
3. *Домарев В. В.* Безопасность информационных технологий. Системный подход. — К.: ООО ТИД "Диасофт", 2004. — 992 с.
4. РД-21-02-2006: "Типовая инструкция о защите информации в автоматизированных средствах центрального аппарата, территориальных органов и организаций Федеральной службы по экологическому, технологическому и атомному надзору".
5. *Макаров О. Ю., Ланкин О. В.* Анализ защищенности информации в автоматизированных системах критического применения от НСД в условиях информационного противоборства // Вестник Воронежского государственного технического университета. 2011. Т. 7. Вып. 4. С. 103—105.
6. Руководящий документ ФСТЭК России "Автоматизированные системы. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации". Гостехкомиссия (ФСТЭК) России, 1992.
7. Комплексность. Энциклопедический словарь экономики и права [Электронный ресурс]. Режим доступа: https://dic.academic.ru/dic.nsf/dic_economic_law/6384/КОМПЛЕКСНОСТЬ (дата обращения: 01.11.2021).
8. *Грибунин В. Г., Чудовский В. В.* Комплексная система защиты информации на предприятии: учеб. пособие для студ. вузов. — М.: Изд. центр "Академия", 2009. — 416 с.
9. ГОСТ Р 56498-2015 Сети коммуникационные промышленные. Защищённость (кибербезопасность) сети и системы.
10. Обзор Secret Net Studio 8.1. Ч. 1. Защитные механизмы [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/Secret_Net_Studio_part1 (дата обращения: 01.11.2021).
11. Обзор Secret Net Studio 8.1. Ч. 2. Механизмы централизованного управления и мониторинга [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/reviews/Secret_Net_Studio_8_1_part2 (дата обращения: 01.11.2021).
12. СЗИ от НСД Secret Net [Электронный ресурс]. Режим доступа: http://www.securitycode.ru/products/secret_net/ (дата обращения: 01.11.2021).

Justification of the need to develop a methodology for choosing information security tools for the implementation of the system of information protection from unauthorized access

V. A. Pikov, V. A. Kaigorodova
Moscow Aviation Institute (National Research University), Moscow, Russia

O. V. Batmanova
Russian New University, Moscow, Russia
Russian Academy of National Economy and Public Administration under the President of the Russian Federation, Moscow, Russia

The article is devoted to topical issues of information security of information systems for various purposes. The concept of a system for protecting information from unauthorized access is considered in detail. The analysis of approaches to the formation of a set of measures to protect information and ensure the proper level of information security is carried out. An approach to the formation of a list of actual threats to the security of information in information systems is formulated. Based on the results of the analysis, it was concluded that there is a need for further work on creating a methodology for choosing information security tools that implement a system for protecting information from unauthorized access.

Keywords: information protection, information, information security, corporate network, information protection methods, security policy, security protection system, information protection efficiency.

Bibliography — 12 references. *Received December 13, 2021*

ДОВЕРЕННАЯ СРЕДА

УДК 004.89
DOI: 10.52190/2073-2600_2022_1_17

Подход к формированию уровней доверия для оценки рисков ошибок аутентификации

[1]*А. Е. Жиляев*; [2]*А. Г. Сабанов*, д-р техн. наук; [2]*П. А. Шелупанова*, канд. эконом. наук; [3]*Д. С. Брагин*; [4]*А. А. Мицель*, д-р техн. наук; [4, 5]*М. Ю. Катаев*, д-р техн. наук

[1] Центр научных исследований и разработок АО «ИнфоТеКС», Москва, Россия
[2] Институт системной интеграции и безопасности (ИСИБ) Томского государственного университета систем управления и радиоэлектроники (ТУСУР), г. Томск, Россия
[3] Центр компетенций национальной технологической инициативы «Технологии доверенного взаимодействия» Томского государственного университета систем управления и радиоэлектроники (ТУСУР), г. Томск, Россия
[4] Томский государственный университет систем управления и радиоэлектроники (ТУСУР), г. Томск, Россия
[5] Центр космического мониторинга Земли из космоса Томского государственного университета систем управления и радиоэлектроники (ТУСУР), г. Томск, Россия

Предложена количественная шкала оценки рисков ошибок аутентификации для наиболее используемых методов аутентификации. Результаты получены на основе анализа рисков для применяемых на определенных уровнях доверия методов аутентификации, выполненных научных исследований, а также рекомендаций международных и национальных стандартов. Предложенная шкала оценки рисков ошибок аутентификации планируется к применению в системах искусственного интеллекта управления идентификацией и аутентификацией.

Ключевые слова: количественные оценки рисков, уровень доверия, идентификация, аутентификация, системы искусственного интеллекта.

В рамках развития цифровизации наблюдается интенсивный рост числа информационных систем (ИС). Как правило, во всех ИС имеется модуль управления доступом, одной из основных задач которого является аутентификация пользователей с минимальными ошибками при каждом запросе на доступ [1]. При этом необходим компромисс между гарантиями того, что злоумышленник не получит доступ к информационным ресурсам ИС, а легальные пользователи будут беспрепятственно получать запрашиваемый доступ, и удобством организации процесса аутентификации для пользователя. Аутентификация — весьма сложный процесс, который уже достаточно изучен для того, чтобы управлять применением того или иного метода аутентификации в автоматизированном режиме. Основой для такого выбора является связь рисков ошибок аутентификации с рисками транзакции, к которой проводится запрос доступа со стороны пользователя ИС, и с рисками ошибок первичной идентификации (ПИ), проводимой во время регистрации нового пользователя в ИС. В основном международном стандарте по аутентификации [2] определено следующее правило: выбор метода аутентификации с определенным уровнем доверия (AAL_i, где i — номер уровня доверия) определяется уровнем рисков транзакции (RL_k, где k — уровень рисков транзакции), к которой запрашивается доступ, и уровнем доверия ПИ (IAL_j, где j — номер уровня доверия ПИ) субъекта

Жиляев Андрей Евгеньевич, исследователь.
E-mail: Andrey.zhilyaev@infotecs.ru
Сабанов Алексей Геннадьевич, доцент, главный научный сотрудник.
E-mail: asabanov@mail.ru
Шелупанова Полина Александровна, доцент кафедры "Безопасность информационных систем", научный сотрудник.
E-mail: uton4ennost@gmail.com
Брагин Дмитрий Сергеевич, руководитель проектного офиса.
E-mail: bds@csp.tusur.ru
Мицель Артур Александрович, профессор кафедры "Автоматизированные системы управления".
E-mail: maa@asu.tusur.ru
Катаев Михаил Юрьевич, профессор кафедры "Автоматизированные системы управления", научный руководитель.
E-mail: kmy@asu.tusur.ru

Статья поступила в редакцию 20 января 2022 г.

доступа. Рекомендации указанного стандарта представлены на качественном (а не количественном) уровне, что является существенным недостатком для целей автоматизации выбора метода аутентификации, соответствующего необходимому уровню доверия $AAL_{i.}$

Данная статья посвящена разработке количественных оценок уровней ошибок аутентификации для наиболее часто применяемых методов аутентификации в целях их дальнейшего использования при проектировании и эксплуатации в ИС различного назначения. Достижение указанной цели позволит автоматизировать процесс выбора метода аутентификации в зависимости от рисков предоставления или отказа в доступе к информационному ресурсу или типовой транзакции, что может создать возможность передачи части функций по управлению доступом пользователей в систему искусственного интеллекта конкретной ИС. В качестве базового метода решения указанной проблемы выбран подход, основанный на анализе рисков аутентификации, рассмотренном в работах [3—14]. Так, в работе [2] сформулированы основные требования к простой, усиленной и строгой аутентификации, конкретизированные в [4, 5]. На основе анализа применимости 31 метода исследования рисков [15], рекомендованных в стандарте [16] к процессу аутентификации, в работе [6] предложены уровни доверия для наиболее часто применяемых методов аутентификации. Результаты указанных работ обобщены в концепции формирования уровней доверия аутентификации на основе анализа рисков, предложенной в работе [7]. Согласно указанной концепции авторами поставлена задача определения количественных значений уровней доверия, которые согласно [7] можно определить с помощью оценок рисков ошибок идентификации и аутентификации.

Оценка рисков аутентификации

Как показано в работе [17], формирование уровней доверия аутентификации основывается на анализе рисков первичной идентификации при регистрации нового пользователя ИС и применяемых методов аутентификации. Согласно [7] риски идентификации и аутентификации могут быть оценены как произведение частоты нежелательных событий на величину последствий:

$$R = \sum_{i=1}^{n} \left[F_{\text{BOC}i}\left(C_i, P_i\right) \right], \qquad (1)$$

где R — величина риска;
P_i — вероятность возникновения i-го вероятного опасного события (ВОС);
C_i — величина потенциального ущерба в результате реализации i-го ВОС;
$F_{\text{BOC}i}$ — функционал, связывающий вероятность P_i и ущерб C_i;
n — количество ВОС.

Приведем уровни рисков транзакций к безразмерному виду: $0 \le \text{LR}_k \le 1$ для всех k при условии, что сумма всех идентифицированных рисков равна 1. Примером такого нормирования является работа [17]. Аналогичные процедуры проведем для рисков ошибок идентификации $0 \le \text{IAL}_i \le 1$ для всех i, как это сделано в работе [18], и для ошибок аутентификации $0 \le \text{AAL}_j \le 1$ для всех уровней доверия j.

Для определения количественных значений границ уровней ошибок аутентификации воспользуемся формулой (1), результатами работы [6] и матрицей последствий и вероятностей (матрицей рисков), приведенной в табл. 2 работы [16]. Заметим, что аналогичная матрица рисков используется при подготовке проектов стандартов по аутентификации во Всемирной организации по стандартизации ISO. Вероятность наступления опасных событий подразделяется на пять уровней: очень низкая, низкая, средняя, высокая и очень высокая. Размер потенциального ущерба также подразделяется на пять уровней: незначительный, низкий, средний, высокий и очень высокий. Как показано в работе [19], количество уровней вероятностей и размера потенциального ущерба может выбираться из соображений достижения наиболее точных значений элементов матрицы рисков. После нормировки приведенная в работе [16] матрица рисков может быть представлена в виде, показанном в табл. 1.

Таблица 1

Матрица рисков

Показатель		Вероятность				
		Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Размер потенциального ущерба	Критический	0,2	0,4	0,6	0,8	1
	Высокий	0,16	0,32	0,48	0,64	0,8
	Средний	0,12	0,24	0,36	0,48	0,6
	Низкий	0,08	0,16	0,24	0,32	0,4
	Незначительный	0,04	0,08	0,12	0,16	0,25

Матрица рисков учитывает как вероятность наступления нежелательного события, так и последствия от реализации рисков. Применим полученную матрицу к оценке рисков аутентификации. Строки и столбцы матрицы рисков представляют шкалы значений оценок последствий и вероятностей, а их пересечение позволяет количественно оценить тот или иной вид риска аутентификации. Согласно национальному стандарту [15] уверенность в результатах аутентификации определяется не только используемым методом аутентификации (определяющим уровень доверия), но и в значительной степени уровнем доверия первичной идентификации, т. е. тем, насколько корректно проводился процесс ПИ субъекта доступа в процессе регистрации, который существенно зависит от качества проверки связи субъекта — физического лица — с его цифровыми идентификационными данными и от тщательности их подтверждения.

В матрице рисков обычно выделяют области высокого, среднего и низкого уровня рисков. Пример количественных оценок уровней рисков идентификации и аутентификации для трех уровней доверия к ПИ, определяемых соответствующими требованиями к процессу регистрации нового пользователя ИС [13, 18], приведена в табл. 2.

Для четырехуровневой системы требований к ПИ количественные оценки уровней рисков приведены в табл. 3.

Преобразуем приведенную в табл. 1 матрицу рисков применительно к иерархии уровней доверия наиболее часто применяемых методов аутентификации [7, 10—14, 21, 22], которые были дополнены в работе [23]. Полученные результаты приводятся в табл. 4.

Предложенные значения рисков ошибок для наиболее часто применяемых методов аутентификации можно применять на практике, сравнивая их в автоматическом режиме с входящими значениями рисков транзакции. При этом риски ошибок ПИ должны соответствовать (не должны превышать) рискам ошибок аутентификации. В корпоративных системах связывание уровней ошибок аутентификации с требованиями к первичной аутентификации проводится на этапе регистрации нового пользователя ИС. Применительно к каждой транзакции комплексный анализ по сравнению RL_k с рисками ошибок AAL_i проводят редко, только для некоторых онлайн-систем. Как правило, для типовых наборов транзакций с ограничением определенного уровня рисков назначается роль, для которой определяют требования к используемому методу аутентификации. Тем не менее с развитием систем искусственного интеллекта рассмотренный в данной работе подход может быть реализован как существенный элемент системы управления доступом пользователей не только корпоративных (закрытых), но и общедоступных ИС.

Таблица 2

Количественные оценки рисков ошибок идентификации и аутентификации для трехуровневой схемы уровней доверия ПИ

№ уровня	Уровень риска аутентификации	Уровень риска идентификации	Уровень доверия ПИ
1	0,04—0,4	0,04—0,24	Низкий
2	0,44—0,76	0,28—0,76	Средний
3	0,8—1	0,8—1	Высокий

Таблица 3

Количественные оценки рисков идентификации и аутентификации для четырехуровневой схемы уровней доверия ПИ

№ уровня	Уровень риска ошибок аутентификации	Уровень риска ошибок идентификации	Уровень доверия ПИ
1	0,04—0,12	0,04—0,12	Низкий
2	0,16—0,24	0,15—0,4	Средний
3	0,28—0,76	0,44—0,76	Высокий
4	0,8—1	0,8—1	Очень высокий

Таблица 4

Количественные оценки рисков ошибок аутентификации

№	Используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Риски ошибок аутентификации	Вид аутентификации
1	Запоминаемый секрет (примеры: пароль, PIN-код)	Пароль	Защита пароля от известных атак	Односторонний	Знание	0,00—0,08	Простая
2	Сгенерированный заранее одноразовый пароль, записанный на носителе (пример: скрэтч-карта)	Одноразовый пароль	Доверенный ДСЧ, защита канала распределения OTP, защита от MitM-атак	Односторонний	Владение	0,08—0,12	
3	"Второй канал" (пример: телефон + SMS)	Одноразовый пароль	Защита операций аутентификации в обоих каналах	Односторонний	Владение	0,12—0,20	
4	Устройство одноразовых паролей, динамически генерирующая OTP	Одноразовый пароль	Защита устройства	Односторонний	Владение	0,20—0,24	
5	Многоразовый пароль + устройство OTP	Одноразовый пароль + многоразовый пароль	Защита многоразового пароля	Односторонний	Владение + знание	0,24—0,32	Усиленная
6	Многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	Одноразовый пароль + многоразовый пароль	Защита устройства и многоразового пароля	Односторонний	Владение + знание или биометрия	0,32—0,48	
7	Криптографический ключ в СВТ или на незащищённым паролем носителе	Криптографические ключи	Защита ключей	Односторонний или взаимный	Владение	0,48—0,60	
8	Устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	Криптографические ключи	Защита устройства	Односторонний или взаимный	Владение + знание	0,60—0,76	
9	СВТ с криптографическим ПО + доступ к ключу по паролю	Криптографические ключи	Защита ключей	Взаимный	Владение + знание	0,76—0,84	Строгая
10	СВТ с криптографическим ПО и отдельное устройство с помещённым и хранящимся в нём криптографическим ключом + доступ к ключу по паролю или биометрии	Криптографические ключи	Защита устройства, содержащего ключ	Взаимный	Владение + знание или биометрия	0,84—0,92	
11	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD), + доступ к ключу по паролю и/или биометрии	Криптографические ключи	Защита устройства, содержащего ключ	Взаимный	Владение + знание или биометрия	0,92—1,00	

Заключение

Согласно концепции формирования уровней доверия идентификации и аутентификации [7] в первом приближении количественные оценки уровней доверия IAL и AAL могут быть ассоциированы с уровнями рисков ошибок ПИ и аутентификации. В такой постановке приведенные авторами оценки могут быть использованы для автоматизации управления идентификацией и аутентификацией в системах управления доступом. Приведенные оценки ошибок аутентификации могут быть уточнены в дальнейшем развитии идей данной работы.

Работа выполнена при финансовой поддержке Министерства науки и высшего образования РФ в рамках базовой части государственного задания ТУСУР на 2020–2022 гг. (проект № FEWM-2020-0037).

Литература

1. *Shelupanov A., Evsyutin O., Konev A., Kostyuchenko E., Kruchinin D., Nikiforov D.* Information Security Methods-Modern Research Directions // Symmerty. 2019. V. 11. № 2. P. 150.

2. ISO/IEC 29115:2013 Information technology — Security techniques — Entity authentication assurance framework [Электронный ресурс]. Режим доступа: https://www.iso.org/standard/45138.html (дата обращения: 15.12.2021).

3. *Сабанов А. Г., Шелупанов А. А., Мещеряков Р. В.* Требования к системам аутентификации по уровням строгости // Ползуновский вестник. 2012. № 2(1). С. 61—67.

4. *Шелупанов А. А., Евсютин О. О., Конев А. А., Костюченко Е. Ю., Кручинин Д. В., Никифоров Д. С.* Актуальные направления развития методов и средств защиты информации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2017. Т. 20. С. 11—24.

5. *Сабанов А. Г.* Об уровнях строгости аутентификации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2012. № 2(26). С. 134—139.

6. *Сабанов А. Г.* Уровни доверия к аутентификаторам // Вопросы защиты информации. 2019. № 2. С. 10—17.

7. *Сабанов А. Г.* Уровни доверия к результатам идентификации и аутентификации субъекта доступа в период цифровой трансформации // Вопросы кибербезопасности. 2019. № 5(33). С. 19—25.

8. *Сабанов А. Г.* Анализ применимости методов оценки рисков к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь. 2014. № 5. С. 44—47.

9. ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска [Электронный ресурс]. Режим доступа: https://docs.cntd.ru/document/1200090083 (дата обращения: 15.12.2021).

10. *Yankovskaya A. E., Shelupanov A. A., Mironova V. G.* Construction of hybrid intelligent system of express-diagnostics of information security attackers based on the synergy of several sciences and scientific directions // Pattern Recognition and Image Analysis (Advances in mathematical theory and applications). 2016. V. 26. № 3. P. 524—532.

11. *Миронова В. Г., Шелупанов А. А., Югов Н. Т.* Реализация модели TAKE-GRANT как представление систем разграничения прав доступа в помещениях // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2(24). Ч. 3. С. 206—210.

12. *Kozachok A. V., Kopylov S. A., Shelupanov A. A. Evsutin O. O.* Text marking approach for data leakage prevention // Journal of computer virology and hacking techniques. 2019. V. 15. № 3. P. 219—232.

13. *Shelupanov A., Konev A., Kosachenko T., Dudkin D.* Threat model for IoT systems on the example of openUNB protocol // International Journal of Emerging Trends in Engineering Research. 2019. V. 7. № 9. P. 283—290.

14. *Novokhrestov A. K., Konev A. A., Shelupanov A. A.* Model of threats to computer network software // Symmetry. 2019. V. 11. № 12. P. 1506.

15. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения. — М.: Стандартинформ, 2020. — 32 с.

16. Руководство по управлению рисками. Утв. Комитетом ПАРТАД по внутреннему контролю, внутреннему аудиту и управлению рисками (протокол № 4/2018 от 21.12.2018) [Электронный ресурс]. Режим доступа: https://new.nfa.ru/upload/iblock/516/Rukovodstvo-po-upravleniyu-riskami.pdf (дата обращения: 15.12.2021).

17. *Сабанов А. Г.* Формирование уровней доверия к идентификации и аутентификации субъектов при удаленном электронном взаимодействии // Электросвязь. 2015. № 10. С. 46—51.

18. *Сабанов А. Г.* Концепция предварительного анализа рисков первичной идентификации субъектов доступа // Инсайд. Защита информации. 2020. № 2. С. 74—79.

19. *Сабанов А. Г., Шубинский И. Б.* Метод анализа технологических рисков первичной идентификации субъектов доступа // Инсайд. Защита информации. 2020. № 3. С. 57—61.

20. *Сабанов А. Г.* О применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь. 2015. № 10. С. 39—42.

21. User authentication guidance for information technology systems. ITSP 30.031.v.3. — Government od Canada. — 2018, April [Электронный ресурс]. Режим доступа: https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng_0.pdf (дата обращения: 15.12.2021).

22. NIST SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-63b/final (дата обращения: 15.12.2021).

23. *Сабанов А. Г.* Методы двухфакторной аутентификации // Инсайд. Защита информации. 2021. № 6. С. 52—56.

An approach to the formation of assurance levels to assess the risks of authentication errors

[1] *A. E. Zhilyaev,* [2] *A. G. Sabanov,* [2] *P. A. Shelupanova,* [3] *D. S. Bragin,*
[4] *A. A. Mitcel,* [4,5] *M. Yu. Kataev*

[1] Research and Development Center JSC "InfoTeCS", Moscow, Russia
[2] Institute for System Assessment and Security of Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia
[3] Competence Center of the National Technology Initiative "Trusted Interaction Technologies" of Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia
[4] Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia
[5] Center for Space Monitoring of the Earth from Space of Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia

A quantitative scale of risk assessments of authentication errors for the most used authentication methods is proposed. The results were obtained on the basis of risk analysis for authentication methods used at certain levels of assurance, scientific research carried out, as well as recommendations of international and national standards. The proposed scale for assessing the risks of authentication errors is planned to be used in artificial intelligence systems for identity and authentication management.

Keywords: quantitative risk assessments, assurance level, identification, authentication, artificial intelligence systems.

Bibliography — 23 references. *Received January 20, 2022*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26
DOI: 10.52190/2073-2600_2022_1_23

Протокол слепой подписи с удвоенным проверочным уравнением

А. А. Костина; А. А. Курышева; А. А. Молдовян, д-р техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН),
Санкт-Петербург, Россия

Предложен вариант построения протокола слепой электронной цифровой подписи (ЭЦП) с использованием удвоенного проверочного уравнения. В качестве алгебраического носителя использована пара четырехмерных конечных коммутативных алгебр с ассоциативной операцией векторного умножения, мультипликативная группа которых обладает четырехмерной или двухмерной цикличностью в зависимости от выбора значения структурного коэффициента, используемого для задания операции векторного умножения. Стойкость протокола основана на специальной форме скрытой задачи дискретного логарифмирования.

Ключевые слова: информационная безопасность, цифровая подпись, слепая подпись, конечная ассоциативная алгебра, коммутативная алгебра, многомерная цикличность.

Ожидаемый в обозримом будущем прорыв в технологии создания квантовых вычислителей делает актуальными вопросы разработки криптографических протоколов и алгоритмов с открытым ключом, обладающих высокой стойкостью к квантовым атакам (атакам с использованием квантовых компьютеров). Постквантовые алгоритмы и протоколы электронной цифровой подписи должны основываться на вычислительно сложных задачах, отличных от задач факторизации (ЗФ) и дискретного логарифмирования (ЗДЛ), поскольку для решения этих задач известны полиномиальные квантовые алгоритмы (алгоритмы для квантового компьютера) [1—6].

В области постквантовой криптогафии значительное внимание криптографического сообщества уделяется разработке криптосхем на алгебрах [4, 5], булевых функциях [6], решетках [7] и линейных кодах [8, 9]. Основным недостатком известных двух ключевых постквантовых криптосхем, включая финалистов всемирного конкурса по разработке кандидатов на постквантовые криптографические стандарты [10], является большой размер открытого ключа, закрытого ключа и подписи. Для устранения этого недостатка в качестве базового криптографического примитива постквантовых алгоритмов ЭЦП предложена скрытая задача дискретного логарифмирования (СЗДЛ) [11—13], а в качестве их носителей — некоммутативные конечные ассоциативные алгебры (КАА). Вопросы задания конечных ассоциативных алгебр рассмотрены в [14—17], а различные формы СЗДЛ — в [18—20]. В некоторых схемах ЭЦП, основанных на СЗДЛ, используется удвоение проверочного уравнения в качестве вспомогательного приема построения [19, 21]. При задании СЗДЛ на коммутативных КАА указанный прием имеет принципиальное значение [22], обеспечивая связывание одним значением подписи двух наборов векторов, принадлежащих двум различным коммутативным КАА, которые использованы для вычисления двух открытых ключей. Это связывание обеспечивает маскирование указанных наборов, поскольку известным является только то, что каждый элемент в первом и каждый элемент во втором открытом ключе вычислен как произведение некоторых степеней векторов, входящих в указанные наборы, причем соответствующие друг другу элементы первого и второго открытых ключей вычислены с использованием одинаковых степеней.

Актуальность задачи разработки постквантовых протоколов слепой подписи обуславливает интерес к использованию алгоритма ЭЦП [22] для разработки на его основе протоколов указанного типа, поскольку использование в нем коммутативных алгебр потенциально позволяет применить метод маскирующих множителей для обеспечения анонимности пользователя, представляющего документ для подписания.

Костина Анна Александровна, научный сотрудник.
E-mail: anya@hotbox.ru
Курышева Алена Андреевна, аспирант.
E-mail: kurysheva.al@yandex.ru
Молдовян Александр Андреевич, главный научный сотрудник.
E-mail: maa1305@yandex.ru

Статья поступила в редакцию 29 января 2022 г.

В данной работе предложен протокол слепой ЭЦП с удвоенным проверочным уравнением.

Понятие слепой подписи

В работах [23, 24] предложен способ решения проблемы обеспечения неотслеживаемости (анонимности) пользователей, возникающей в ряде информационных технологий, на основе использования протоколов слепой подписи.

В протоколе слепой подписи некоторый пользователь (именуемый обычно клиентом) готовит некий электронный документ *M* и, взаимодействуя в ходе протокола с подписантом и используя случайные маскирующие множители, получает от последнего слепую подпись, вычисленную с помощью секретного ключа. Затем клиент, удаляя "влияние" маскирующих множителей, вычисляет подлинную подпись к документу *M*. Если в некотором приложении подписант вычисляет слепые подписи для многих различных клиентов, то получая документы, подписанные вслепую, вместе с соответствующими им подлинными подписями, он не должен иметь возможности идентифицировать клиентов, связанных с конкретными документами. При этом предполагается, что подписант может иметь такое намерение в самом начале выполнения протокола слепой подписи, т. е. предполагается, что подписант хранит все сообщения, получаемые от клиента в ходе протокола. Если это требование выполняется, то считается, что протокол обеспечивает анонимность клиента.

Подлинность подписи проверяется с помощью обычной процедуры верификации ЭЦП, как и в случае, когда подпись формируется подписантом самостоятельно. Это означает, что в основе протокола слепой подписи должна лежать обычная схема подписи, т. е. протокол слепой подписи разрабатывается на основе обычного алгоритма ЭЦП, служащего для протокола базовой схемой подписи. Одни известные схемы ЭЦП (RSA, алгоритм ЭЦП Шнорра, ГОСТ Р 34.10-2012) позволяют разработать на их основе протоколы слепой подписи с использованием маскирующих параметров, а другие (схема ЭЦП Эль-Гамаля, стандарт DSA и ECDSA) нет.

Используемые алгебры

Конечные *m*-мерные алгебры задаются над конечным полем как конечное *m*-мерное векторное пространство с дополнительно определенной операцией векторного умножения векторов (далее просто умножения), которая является замкнутой и дистрибутивной слева и справа относительно операции сложения векторов. В качестве конечного поля будем использовать простое поле $GF(p)$. Элемент алгебры $\mathbf{A}$ можно представить в виде упорядоченного набора его координат $a_i \in GF(p)$, т. е. в виде $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$, или в виде суммы его компонент $a_i\mathbf{e}_i$, т. е. в виде $\mathbf{A} = \sum_{i=0}^{m-1} a_i\mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы.

Операцию умножения векторов $\mathbf{A}$ и $\mathbf{B} = \sum_{j=0}^{m-1} b_j\mathbf{e}_j$ обычно задают по правилу перемножения каждой компоненты вектора $\mathbf{A}$ с каждой компонентой вектора $\mathbf{B}$:

$$\mathbf{AB} = \sum_{i,j=0}^{m-1} a_i b_j \left(\mathbf{e}_i\mathbf{e}_j\right), \qquad (1)$$

где всевозможные произведения пар базисных векторов $\mathbf{e}_i\mathbf{e}_j$ заменяются на соответствующие однокомпонентные векторы вида $\lambda\,\mathbf{e}_k$ (λ — структурная константа), указанные в ячейках на пересечении *i*-й строки и *j*-го столбца в так называемой таблице умножения базисных векторов (ТУБВ). Если заданная операция умножения обладает свойством коммутативности и ассоциативности, то имеем коммутативную КАА.

Свойство ассоциативности обеспечивает возможность использования алгоритма быстрого возведения в степень, основанного на процедуре последовательного возведения в квадрат, и означает выполнимость для всевозможных троек векторов $\mathbf{A}$, $\mathbf{B}$ и $\mathbf{C}$ следующего равенства:

$$\left(\mathbf{AB}\right)\mathbf{C} = \mathbf{A}\left(\mathbf{BC}\right). \qquad (2)$$

Из формул (1) и (2) вытекает, что при составлении ТУБВ достаточно обеспечить выполнимость равенства

$$\left(\mathbf{e}_i\mathbf{e}_j\right)\mathbf{e}_k = \mathbf{e}_i\left(\mathbf{e}_j\mathbf{e}_k\right) \qquad (3)$$

для всевозможных троек базисных векторов $\mathbf{e}_i$, $\mathbf{e}_j$ и $\mathbf{e}_k$. Последнему условию удовлетворяют ТУБВ, представленные в табл. 1 и 2 и задающие четырехмерные коммутативные КАА, мультипликативная группа которых имеет четырехмерное циклическое строение при значении структурной константы λ ($\lambda \neq 0$), равном квадратичному вычету (если λ есть квадратичный невычет, то мультипликативная группа имеет двухмерное циклическое строение). Конечной коммутативной группой с μ-мерной цикличностью называется группа, минимальная система образующих которой включает μ элементов одинакового порядка.

Таблица 1

Задание первой четырехмерной коммутативной КАА над полем $GF(p)$ с единичным вектором вида $\mathbf{E} = (1,0,0,0)$ [22]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_3$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

Таблица 2

Задание второй четырехмерной коммутативной КАА над полем $GF(p)$ с $\mathbf{E} = (0,0,1,0)$ [22]

·	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	$\lambda\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\lambda\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_3$	$\mathbf{e}_2$	$\mathbf{e}_1$	$\mathbf{e}_0$
$\mathbf{e}_2$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\lambda\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$	$\lambda\mathbf{e}_2$

Базовая схема подписи

Первая и вторая КАА, используемые в качестве алгебраического носителя в разрабатываемом протоколе слепой подписи, задаются по табл. 1 и 2 над полем $GF(p)$, порядок которого равен простому числу $p = 2q + 1$ при простом 256-битном целом числе q. В качестве базовой схемы подписи будем использовать алгоритм ЭЦП, предложенный в работе [22], в котором единый открытый ключ состоит из первого открытого ключа, включающего векторы, являющиеся элементами первой КАА, и второго открытого ключа, включающего векторы, являющиеся элементами второй КАА.

Первый (второй) открытый ключ генерируется следующим образом.

- В первой (второй) КАА генерируются два различных случайных вектора $\mathbf{G}$ и $\mathbf{Q}$ ($\mathbf{D}$ и $\mathbf{H}$) порядка q.
- Генерируются два различных случайных равновероятных числа y_1 и y_2 ($y_1 < q$, $y_2 < q$) и случайный примитивный элемент α по модулю p.
- Генерируются два различных случайных равновероятных числа z_1 и z_2 ($z_1 < q$, $z_2 < q$) и случайный примитивный элемент β по модулю p.
- Генерируются случайные число u ($u < q$) и примитивный элемент γ по модулю p.
- Вычисляется первый открытый ключ в виде тройки векторов ($\mathbf{Y}_1, \mathbf{Z}_1, \mathbf{U}_1$) из первой КАА: $\mathbf{Y}_1 = \mathbf{G}^{y_1}\mathbf{Q}^{y_2}\alpha$; $\mathbf{Z}_1 = \mathbf{G}^{z_1}\mathbf{Q}^{z_2}\beta$ и $\mathbf{U}_1 = \mathbf{G}^{u}\gamma$.
- Вычисляется второй открытый ключ в виде тройки векторов ($\mathbf{Y}_2, \mathbf{Z}_2, \mathbf{U}_2$) из первой КАА: $\mathbf{Y}_2 = \mathbf{D}^{y_1}\mathbf{H}^{y_2}\alpha$; $\mathbf{Z}_2 = \mathbf{D}^{z_1}\mathbf{H}^{z_2}\beta$ и $\mathbf{U}_2 = \mathbf{D}^{u}\gamma$.

Секретным ключом является следующий набор из восьми натуральных чисел: (y_1, y_2, α, z_1, z_2, β, u, γ).

Алгоритм генерации ЭЦП к электронному документу M описывается следующими шагами.

- Генерируются случайные равновероятные числа k, t и ρ ($k < q$, $t < q$, $\rho < p$).
- Вычисляются векторы-фиксаторы $\mathbf{R}_1$ и $\mathbf{R}_2$: $\mathbf{R}_1 = \mathbf{G}^{k}\mathbf{Q}^{t}\rho$ и $\mathbf{R}_2 = \mathbf{D}^{k}\mathbf{H}^{t}\rho$.
- С использованием некоторой специфицированной стойкой 256-битной хэш-функции f_H вычисляется первый элемент подписи в виде числа e: $e = f_H(M, \mathbf{R}_1, \mathbf{R}_2)$.
- Вычисляется второй элемент s ЭЦП: $s = z_2^{-1}(t - y_2 e) \bmod q$.
- Вычисляется третий элемент d ЭЦП: $d = u^{-1}(k - y_1 e - z_1 s) \bmod q$.
- Вычисляется четвертый элемент σ ЭЦП: $\sigma = \rho\alpha^{-e}\beta^{-s}\gamma^{-d} \bmod p$.

Алгоритм верификации ЭЦП описывается следующими шагами.

- Вычисляются векторы $\mathbf{R}_1^*$ и $\mathbf{R}_2^*$: $\mathbf{R}_1^* = \mathbf{Y}_1^{e}\mathbf{Z}_1^{s}\mathbf{U}_1^{d}\sigma$ и $\mathbf{R}_2^* = \mathbf{Y}_2^{e}\mathbf{Z}_2^{s}\mathbf{U}_2^{d}\sigma$.
- Вычисляется проверочное значение e^* хэш-функции: $e^* = f_H(M, \mathbf{R}_1^*, \mathbf{R}_2^*)$.
- Если $e^* = e$, то ЭЦП к документу M признается подлинной, в противном случае — ложной.

В основу стойкости представленной схемы ЭЦП положена задача вычисления секретных значений целочисленных степеней y_1, y_2, z_1, z_2, u и множителей α, β и γ. Последние также могут быть представлены как степени некоторых скалярных векторов $\mathbf{L}_1$ и $\mathbf{L}_2$ из первой и второй КАА соответственно. Таким образом, взлом этой схемы ЭЦП связан с решением СЗДЛ, поскольку наборы векторов, возводимые в соответствующие степени, являются неизвестными. На самом деле элементы первого (второго) открытого ключа могут быть выражены как произведения степеней элементов любой минимальной системы образующих (базиса) в мультипликативной группе первой (второй) КНАА. Однако для подделки подписи требуется найти такие базисы в первой и второй КАА, для которых наборы указанных степеней будут совпадать.

Протокол слепой подписи

Свойство коммутативности операции умножения в КАА, используемых в качестве алгебраического носителя базовой схемы ЭЦП, дает основание предположить, что механизм ослепляющих множителей может быть применен для разработки протокола слепой подписи. При этом в качестве аналога протокола слепой подписи может быть использован протокол, разработанный в авторами [25]. В соответствии с этим подходом приходим к выводу, что ослепляющие параметры должны вноситься клиентом в векторы $\mathbf{R}_1$ и $\mathbf{R}_2$ (в обозначениях базовой схемы ЭЦП; в протоколе слепой

ЭЦП эти векторы обозначаются как $\mathbf{R}'_1$ и $\mathbf{R}'_2$ соответственно), генерируемые подписантом и направляемые клиенту. При этом каждый из указанных векторов "ослепляется" с использованием одинаковых наборов ослепляющих параметров. С учетом отмеченного имеем следующий протокол слепой ЭЦП, использующий удвоенное проверочное уравнение.

• Подписант генерирует разовый секретный ключ в виде тройки чисел k, t и ρ ($k < q$, $t < q$, $\rho < p$) и вычисляет векторы-фиксаторы $\mathbf{R}'_1$ и $\mathbf{R}'_2$: $\mathbf{R}'_1 = \mathbf{G}^k\mathbf{Q}^t\rho$ и $\mathbf{R}'_2 = \mathbf{D}^k\mathbf{H}^t\rho$. Затем направляет векторы $\mathbf{R}'_1$ и $\mathbf{R}'_2$ клиенту.

• Клиент генерирует равновероятные ослепляющие значения в виде натуральных чисел ε, τ, δ и μ ($\varepsilon < q$, $\tau < q$, $\delta < q$, $\mu < p$) и вычисляет векторы $\mathbf{R}_1 = \mathbf{R}'_1\mathbf{Y}_1^{\varepsilon}\mathbf{Z}_1^{\tau}\mathbf{U}_1^{\delta}\mu$ и $\mathbf{R}_2 = \mathbf{R}'_2\mathbf{Y}_2^{\varepsilon}\mathbf{Z}_2^{\tau}\mathbf{U}_2^{\delta}\mu$. Затем он вычисляет первый элемент e подлинной ЭЦП: $e = f_H(M, \mathbf{R}_1, \mathbf{R}_2)$, и первый элемент e' слепой ЭЦП: $e' = e - \varepsilon \bmod q$. После этого клиент передает значение e' подписанту.

• Подписант, используя свой секретный ключ и целочисленные значения k, t и ρ, вычисляет следующие элементы слепой подписи:

$s' = z_2^{-1}(t - y_2 e) \bmod q$;

$d' = u^{-1}(k - y_1 e - z_1 s) \bmod q$;

$\sigma' = \rho\alpha^{-e'}\beta^{-s'}\gamma^{-d'} \bmod p$.

Затем подписант передает вычисленные элементы слепой подписи s', d' и σ' клиенту.

• Клиент, используя полученные значения s', d' и σ', вычисляет второй, третий и четвертый элементы подлинной подписи:

$s = s' + \tau \bmod q$;

$d = d' + \delta \bmod q$;

$\sigma = \sigma'\mu \bmod p$.

В результате выполнения описанного протокола слепой подписи клиент получает подлинную подпись подписанта к документу M. При этом обеспечивается требование будущей анонимности клиента после того, как этот электронный документ и подпись к нему станут доступными подписанту. Очевидно, что верификация подлинной ЭЦП, полученной в ходе протокола слепой подписи и сгенерированной самим подписантом, осуществляется с помощью одного и того же алгоритма, а именно алгоритма верификации ЭЦП базовой схемы подписи.

Доказательство корректности работы протокола слепой ЭЦП выполняется как демонстрация того, что сформированная в ходе протокола подлинная подпись действительно проходит процедуру верификации как подлинная ЭЦП. Действительно, учитывая равенства $\mathbf{R}'_1 = \mathbf{Y}_1^{e'}\mathbf{Z}_1^{s'}\mathbf{U}_1^{d'}\sigma'$ и $\mathbf{R}'_2 = \mathbf{Y}_2^{e'}\mathbf{Z}_2^{s'}\mathbf{U}_2^{d'}\sigma'$, имеем:

$$\mathbf{R}_1^* = \mathbf{Y}_1^{e}\mathbf{Z}_1^{s}\mathbf{U}_1^{d}\sigma = \mathbf{Y}_1^{e'+\varepsilon}\mathbf{Z}_1^{s'+\tau}\mathbf{U}_1^{d'+\delta}\sigma =$$
$$= \left(\mathbf{Y}_1^{e'}\mathbf{Z}_1^{s'}\mathbf{U}_1^{d'}\sigma'\right)\mathbf{Y}_1^{\varepsilon}\mathbf{Z}_1^{\tau}\mathbf{U}_1^{\delta}\mu =$$
$$= \mathbf{R}'_1\mathbf{Y}_1^{\varepsilon}\mathbf{Z}_1^{\tau}\mathbf{U}_1^{\delta}\mu = \mathbf{R}_1;$$

$$\mathbf{R}_2^* = \mathbf{Y}_2^{e}\mathbf{Z}_2^{s}\mathbf{U}_2^{d}\sigma = \mathbf{Y}_2^{e'+\varepsilon}\mathbf{Z}_2^{s'+\tau}\mathbf{U}_2^{d'+\delta}\sigma =$$
$$= \left(\mathbf{Y}_2^{e'}\mathbf{Z}_2^{s'}\mathbf{U}_2^{d'}\sigma'\right)\mathbf{Y}_2^{\varepsilon}\mathbf{Z}_2^{\tau}\mathbf{U}_2^{\delta}\mu =$$
$$= \mathbf{R}'_2\mathbf{Y}_2^{\varepsilon}\mathbf{Z}_2^{\tau}\mathbf{U}_2^{\delta}\mu = \mathbf{R}_2 \Rightarrow$$
$$\Rightarrow \left\{\mathbf{R}_2^* = \mathbf{R}_2; \mathbf{R}_2^* = \mathbf{R}_2\right\} \Rightarrow$$
$$\Rightarrow f_H\left(M, \mathbf{R}_1^*, \mathbf{R}_2^*\right) = f_H\left(M, \mathbf{R}_1, \mathbf{R}_2\right) \Rightarrow$$
$$\Rightarrow e^* = e.$$

Обеспечение анонимности клиента можно легко показать путем демонстрации того, что каждая слепая подпись, сформированная в ходе протокола слепой подписи, и любая подлинная подпись подписанта (независимо от того, формировалась ли она непосредственно самим подписантом или в ходе протокола слепой ЭЦП) связаны между собой четверкой случайных целочисленных значений, которые по указанным двум подписям легко могут быть вычислены.

Рассмотрение вопроса реализации протоколов коллективной и слепой коллективной ЭЦП на основе алгоритма ЭЦП [22] с удвоенным проверочным уравнением выявило противоречивость требования секретности скрытой группы в алгоритме [22] и использования фиксированных векторов, применяемых для вычисления открытого ключа различных пользователей в протоколе коллективной подписи [25].

Заключение

Применение приема удвоения проверочного уравнения в алгоритмах ЭЦП со скрытой группой, использующих в качестве алгебраического носителя коммутативные КАА, сохраняет принципиальную возможность разработки на их основе протоколов слепой ЭЦП. Однако реализация протоколов коллективной и слепой коллективной подписи не может быть выполнена, поскольку секретность используемых скрытых групп предполагает, что они различны для различных пользователей, что делает невозможным формирование единого открытого ключа для двух и более пользователей.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а) и бюджетной темы № FFZF-2022-0007.

Литература

1. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.
2. *Smolin J. A., Smith G., Vargo A.* Oversimplifying quantum factoring // Nature. 2013. V. 499. № 7457. P. 163—165.
3. *Jozsa R.* Quantum algorithms and the Fourier transform // Proc. Roy. Soc. London, Ser A. 1988. V. 454. P. 323—337.
4. *Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.* Cryptographic Algorithms on Groups and Algebras // J. Mathematical Sciences. 2017. V. 223. № 5. P. 629—641.
5. *Moldovyan N. A.* Fast Signatures Based on Non-Cyclic Finite Groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.
6. *Agibalov G. P.* El Gamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. С. 57—65. DOI: 10.17223/20710410/42/4.
7. *Hoffstein J., Pipher J., Schanck J. M., Silverman J. H., Whyte W., Zhang Zh.*: Choosing parameters for NTRU Encrypt. Cryptographers' Track at the RSA Conference – CTA-RSA 2017. Springer LNCS. 2017. V. 10159. P. 3—18.
8. *Alamelou Q., Blazy O., Cauchie S., Gaborit Ph.* A code-based group signature scheme // Designs, Codes and Cryptography. 2017. V. 82. № 1−2. P. 469—493.
9. *Kosolapov Y. V., Turchenko O. Y.* On the construction of a semantically secure modification of the McEliece cryptosystem functions // Прикладная дискретная математика. 2019. № 45. P. 33—43. DOI 10.17223/20710410/45/4.
10. Post-Quantum Cryptography. Round 3 Submissions [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (дата обращения: 10.01.2022).
11. *Moldovyan N. A., Moldovyan A. A.* Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Сер. "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81. DOI: 10.14529/mmp190106.
12. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.
13. *Молдовян А. А., Молдовян Д. Н.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.
14. *Молдовян Д. Н., Молдовяну П. А.* Задание умножения в полях векторов большой размерности // Вопросы защиты информации. 2008. № 3(82). С. 12—17.
15. *Молдовян Д. Н., Костина А. А., Куприянов И. А., Захаров Д. В.* Задание некоммутативных конечных групп векторов для синтеза алгоритмов цифровой подписи // Вопросы защиты информации. 2009. № 4(87). С. 12—18.
16. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. V. 17. № 2. P. 271—282.
17. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.
18. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А.* Постквантовая схема цифровой подписи на алгебре матриц // Системы и средства информатики. 2021. Т. 31. № 4. С. 40—49. DOI: 10.14357/08696527210404.
19. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455—461. DOI:10.21638/11701/spbu10.2020.410.
20. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* A new design of the signature schemes based on the hidden discrete logarithm problem // Quasigroups and Related Systems. 2021. V. 29. № 1. P. 97—106.
21. *Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Фахутдинов Р. Ш.* Схемы цифровой подписи с удвоенным проверочным уравнением // Вопросы защиты информации. 2021. № 2. С. 30—36. DOI: 10.52190/2073-2600_2021_2_30.
22. *Moldovyan N. A., Moldovyan D. N.* A novel method for developing post-quantum cryptoschemes and a practical signature algorithm // Applied Computing and Informatics. 2021. DOI: 10.1108/ACI-02-2021-0036.
23. *Chaum D.* Security without identification: Transaction systems to make big brother obsolete // Communications of the AMS. 1985. V. 28. № 10. P. 1030—1044.
24. *Camenisch J. L., Piveteau J.-M., Stadler M. A.* Blind Signatures Based on the Discrete Logarithm Problem // Advances in Crypology — EUROCRYPT '94. Springer LNCS. 1995. V. 950. P. 428—432.
25. *Молдовян Н. А., Костина А. А., Курышева А. А.* Протоколы коллективной и слепой подписи на конечных группах с многомерной цикличностью // Вопросы защиты информации. 2021. № 2. С. 22—29. DOI: 10.52190/2073-2600_2021_2_22.

Blind Signature Protocol with Doubled verification equation

A. A. Kostina, A. A. Kurysheva, A. A. Moldovyan
St. Petersburg Federal Research Center of the RAS (SPC RAS),
St. Petersburg, Russia

A blind digital signature protocol with a doubled verification equation is introduced. A pair of four-dimensional finite commutative algebras with an associative vector multiplication operation are used as an algebraic support. The multiplicative group of the algebras has four-dimensional or two-dimensional cyclicity, depending on the selection of the value of the structural coefficient used to specify the vector multiplication operation. Security of the protocol is based on a special form of a hidden discrete logarithm problem.

Keywords: information security, digital signature, blind signature, finite associative algebra, commutative algebra, multidimensional cyclicity.

Bibliography — 25 references. *Received January 29, 2022*

УДК 004
DOI: 10.52190/2073-2600_2022_1_28

Оценка актуальности и эффективности интеграции цифровой подписи в качестве инструмента обеспечения информационной безопасности информационных систем

А. П. Шовкалюк, канд. техн. наук
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Произведен подробный анализ актуальности и эффективности инструмента цифровой подписи в качестве составляющей информационной безопасности. Он имеет ценность для будущих исследований, касающихся разработки методов защиты от фальсификации электронной подписи. Преимущественная часть посвящена вопросу информационной безопасности информационных систем.

Ключевые слова: цифровая подпись, информация, информационные технологии, информационная система, инструмент.

В современном мире происходит интенсивное цифровое развитие профессиональных и бытовых сфер жизнедеятельности человека. Все большее развитие и повсеместную интеграцию получают различные информационные и цифровые средства. Особую значимость имеют вопросы обеспечения информационной безопасности автоматизированных систем. Данный фактор связан с тем, что современные информационные системы могут хранить различную секретную, корпоративную или конфиденциальную информацию ограниченного доступа, утечка которой может повлечь различные экономические и другие потери [1].

Повсеместная цифровизация предприятий и массовый переход на электронный документооборот ставят множество задач, связанных с обеспечением информационной безопасности. Именно за счет должного уровня обеспечения информационной безопасности предприятия имеют возможность снизить риски незапланированных материальных и экономических потерь.

В данной работе рассмотрены вопросы, связанные с обеспечением должного уровня информационной безопасности информационных систем посредством внедрения технологии цифровой подписи.

Методы

Автором использованы теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных изучены научные работы отечественных и зарубежных авторов. В каждой из работ [1—5] затронуты фундаментальные вопросы, необходимые для воспроизведения общего анализа, касающегося обеспечения информационной безопасности на основе цифровых подписей.

Тематика используемой автором литературы — это проблемы и практика применения электронной цифровой подписи, электронная цифровая подпись и информационная безопасность малых предприятий, использование электронной подписи в условиях образовательной организации, проблемы практического применения цифровых подписей и другие.

Цифровая подпись в аспекте использования системами информационной безопасности

Как уже было сказано, одним из основных трендов является повсеместная цифровизация и роботизация монотонно повторяющихся и выполняемых задач. Информационные системы активно внедряют цифровые подписи в целях получения максимальной эффективности выполняемых процессов.

Особенную актуальность получают вопросы, связанные с конфиденциальностью данных, что проявляется в скептицизме пользователей. Понятие электронной цифровой подписи (ЭЦП) заключается в предоставлении законного цифрового средства для выражения одобрения или согласия на электронных документах, анкетах и иных объектах. Данный инструмент позволяет повысить безопасность процессов продажи, сбора данных и т. д., связанных с работой цифровых технологий.

Шовкалюк Алексей Петрович, профессор учебного военного центра.
E-mail: shovalex@yandex.ru

Статья поступила в редакцию 22 декабря 2021 г.

Инструментарий цифровых подписей поставляют такие компании, как DocuSign, GlobalSign, Skribble и иные [2].

Электронные цифровые подписи создают на основе криптографических преобразований данных с использованием специального ключа, включающего определенную последовательность символов. Данный ключ является аналогом собственноручной подписи на стандартном бумажном носителе, он имеет при этом равную силу с юридической точки зрения. На основе электронных цифровых подписей устанавливают отсутствие какого-либо рода изменений информации в документе, а также определяют и выявляют подделки. Цифровая подпись имеет достаточно высокий уровень защиты, так как для подбора искомой комбинации символов криптографического узла злоумышленнику требуется выполнить колоссальное число сложных математических операций, что может потребовать недели и даже месяцы работы.

Аспекты эффективности использования цифровой подписи для обеспечения информационной безопасности

Рассмотрим основные преимущества использования ЭЦП в качестве факторов эффективности применения данной технологии в системах информационной безопасности. В качестве основного фактора выступают общая эффективность и скорость при работе с данной технологией. Цифровая подпись является одним из основных инструментов, препятствующих получению доступа и изменению информации в документации. Данную технологию активно используют при решении целого класса задач.

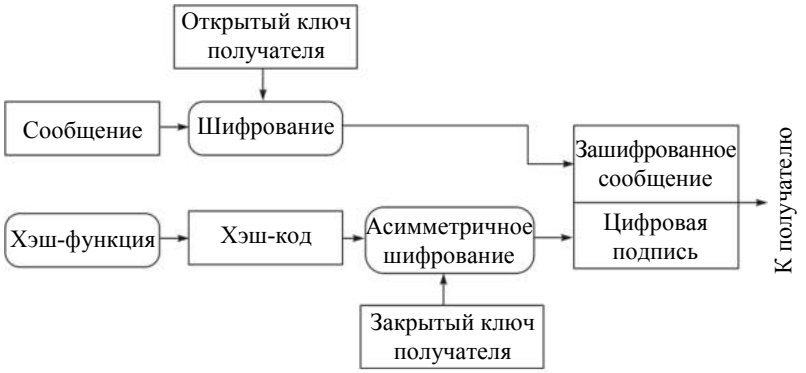
Другим преимуществом использования ЭЦП является соблюдение правовых норм. Данная технология воплощает четкие правила, в частности eIDAS (для Европейского союза). Указанные обязательства устанавливают четкую основу для поставщиков цифровых подписей и обеспечивают целостность в случае возникновения юридических споров по поводу подписи [3].

Основным преимуществом использования ЭЦП является безопасность. Двухфакторная аутентификация и проверка личности способны обеспечить достаточно высокий уровень безопасности в отношении доступа к документам и возможности нарушения их целостности, секретности или фальсификации. При этом в случае получения (перехвата) документа по электронной почте нарушитель не сможет извлечь данные ввиду принципа работы технологии и интегрированных алгоритмов защиты. На рисунке представлен один из примеров принципов работы с цифровой подписью [4].

Помимо этого, двухфакторная аутентификация гарантирует, что ни один из пользователей не сможет скопировать или подделать подпись для дальнейшего использования в других задачах.

Технология облачной электронной цифровой подписи как эффективный инструмент обеспечения информационной безопасности

Одной из наиболее перспективных, но малоизученной разновидностью цифровых подписей является облачная ЭЦП. В таблице представлены основные отличия данных технологий.



Принцип работы электронной цифровой подписи

Отличия обычной и облачной ЭЦП

Классическая ЭП	Облачная ЭП
Персональный носитель закрытого ключа (токен, смарт-карта, реестр)	Носитель закрытого ключа — централизованное защищенное хранилище — двухфакторная аутентификация
Криптопровайдер на рабочем месте пользователя	Центральный криптопровайдер (HSM)
Средство ЭП на рабочем месте пользователя	Централизованное средство ЭП (поддержка основных форматов подписи, возможность интеграции)

Вопросами защищенности облака занимаются "безопасники" и консультирующие их юристы. Сведения должны не просто попасть в облако, но и быть обработаны и сохранены. В случае локального средства ЭП находится в защищенном пространстве пользователя. Для облачной ЭП такое пространство отсутствует [5].

При этом ответственность за обеспечение конфиденциальности данных в каком-то смысле "размывается" между её собственником и поставщиком облачных услуг. Некоторые пользователи не доверяют надежности облака, так как не до конца понимают механизмы его действия. На облако передается ключ ЭП, а это информация, которая конфиденциальна и принадлежит конкретному человеку — собственнику. Защищенность ключа зависит от уровня безопасности средств, которые используют при аутентификации, и от ответственности владельца.

Заключение

Исследованы эффективность и актуальность обеспечения информационной безопасности на основе интеграции ЭЦП. Рассмотрены такие моменты, как цифровая подпись в аспекте использования системами информационной безопасности, аспекты эффективности использования цифровой подписи для обеспечения информационной безопасности, технология облачной электронной цифровой подписи как эффективный инструмент обеспечения информационной безопасности и другие.

ЭПЦ является достаточно уникальным и эффективным инструментом обеспечения информационной безопасности в информационных системах современных организаций. В заключение требуется отметить, что современные специалисты в области информационной безопасности должны уделять большее внимание разработке ЭЦП. Параллельно с этим и руководители организаций должны активно интегрировать технологию ЭЦП на цифровых машинах своих предприятий.

Литература

1. *Асеев А. А., Макаров В. В., Наружный В. Е.* Проблемы и практика использования электронной цифровой подписи // Экономика и бизнес: теория и практика. 2021. № 1—1 (71). С. 20—23.
2. *Попова Е. В.* Электронная цифровая подпись и информационная безопасность малых предприятий // Теория и практика сервиса: экономика, социальная сфера, технологии. 2011. № 2(8). С. 110—118.
3. *Гнедков А. В., Захаров А. Б., Мухаметьева Е. С., Худорожков И. В., Хурматшина А. А.* Использование электронной подписи в условиях образовательной организации // Научно-методическое обеспечение оценки качества образования. 2019. № 3S(8). С. 104—108.
4. *Родионов А. С., Сухарев С. Л.* Использование хеш-функции для защиты информации в локальных вычислительных сетях военного назначения // Изв. ЮФУ. Технические науки. 2012. № 5(130). С. 226—230.
5. *Гнедков А. В., Захаров А. Б., Ильин А. С., Мухаметьева Е. С., Худорожков И. В.* Актуальные аспекты организации защиты персональных данных при их обработке в рамках процедур оценки качества образования // Научно-методическое обеспечение оценки качества образования. 2018. № 2(5). С. 129—133.

Assessment of the relevance and effectiveness of digital signature integration as tool for ensuring information security of information systems

A. P. Shovkaluk
Moscow Aviation Institute (National Research University), Moscow, Russia

Within the framework of the presented article, the most detailed analysis of the relevance and effectiveness of the digital signature tool as a component of information security carried out. This work is of value for future research concerning the development of methods of protection against falsification of electronic signatures. The predominant part of the article is devoted specifically to the issue of information security of information systems.

Keywords: digital signature, information, information technology, information system, tool.

Bibliography — 5 references. *Received December 22, 2021*

УДК 003.26
DOI: 10.52190/2073-2600_2022_1_31

Типовые проверочные уравнения в алгебраических алгоритмах ЭЦП со скрытой группой

Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН (СПб ФИЦ РАН),
Санкт-Петербург, Россия

Предложены типовые варианты задания проверочного уравнения в алгоритмах электронной цифровой подписи (ЭЦП) со скрытой группой, использующих в качестве алгебраического носителя конечные некоммутативные ассоциативные алгебры. Принципиальной особенностью алгоритмов данного типа является то, что подпись включает в качестве одного из элементов некоторый вектор, включаемый многократно в проверочное уравнение. Многократное включение этого элемента в проверочное уравнение определяет стойкость алгоритмов ЭЦП данного типа к подделке подписи и требует использования специального способа вычисления этого элемента по секретному ключу. Конкретный вид проверочного уравнения определяет формулы для вычисления элементов открытого ключа. Показано, что вычисление ЭЦП по секретному ключу может быть выполнено несколькими различными способами, но в обязательном порядке механизм рандомизации подписи включает операции возведения элементов скрытой группы в степени со случайными значениями.

Ключевые слова: информационная безопасность, цифровая подпись, постквантовая криптография, конечная ассоциативная алгебра, некоммутативная алгебра, скрытая группа.

Разработка практичных постквантовых алгоритмов электронной цифровой подписи остается актуальной задачей в области криптографии. Для ее решения представляется наиболее интересным способ, описанный в работах [1, 2], который является новым подходом к построению алгоритмов ЭЦП на конечных некоммутативных ассоциативных алгебрах (КНАА). В отличие от алгебраических алгоритмов, основанных на вычислительной трудности скрытой задачи дискретного логарифмирования (ЗДЛ) [3, 4], способ [1] задает построение алгоритмов ЭЦП, основанных на вычислительной трудности решения систем многих квадратных уравнений с многими неизвестными. Оба типа алгоритмов используют вычисления в скрытой (секретной) коммутативной группе и маскирующие операции в виде левых и правых умножений на векторы, которые являются неперестановочными с векторами, входящими в скрытую группу. Также общим является то, что базовыми операциями в алгоритмах указанных двух типов являются операции экспоненцирования (возведения в большую целочисленную степень).

При этом имеется принципиальное отличие, состоящее в том, что в алгоритмах второго типа ЭЦП в обязательном порядке включает некоторый специальным образом вычисляемый вектор **S** в качестве одного из своих элементов (или в качестве единственного элемента, т. е. в частном случае **S** может являться подписью), тогда как в алгоритмах первого типа использование вектора **S** в качестве элемента подписи является нетипичным. Использование вектора **S** в качестве элемента подписи предполагает, что он будет входить в проверочное уравнение, что создает предпосылки к потенциальной возможности его использования в качестве подгоночного параметра в атаках типа подделки подписи, т. е. вычисления подписи без использования секретного ключа. В алгоритмах ЭЦП, основанных на СЗДЛ, устранение таких атак обеспечивается удвоением проверочного уравнения [5, 6], а в алгоритмах, основанных на вычислительной трудности решения систем многих квадратичных уравнений, — многократным вхождением **S** в проверочное уравнение.

В [1, 2] представлены варианты проверочного уравнения с двумя вхождениями **S**. Поскольку число вхождений не связано с увеличением размера ЭЦП, но потенциально повышает стойкость к подделке подписи, представляет интерес рассмотрение схем ЭЦП, в проверочное уравнение которых вектор **S** входит три и более раз. Автор предлагает два варианта проверочных уравнений с $\beta \geq 3$ вхождениями вектора **S** и рассматривается вопрос о влиянии значения β на размер секретного и открытого ключей.

Используемый алгебраический носитель

В предлагаемых далее к рассмотрению постквантовых алгоритмах ЭЦП со скрытой группой предполагается, что в качестве алгебраическо-

Молдовян Дмитрий Николаевич, научный сотрудник.
E-mail: mdn.spectr@mail.ru

Статья поступила в редакцию 18 февраля 2022 г.

го носителя используется m-мерная КНАА со значением размерности $m \geq 4$, которая содержит глобальную двухстороннюю единицу и большое число коммутативных конечных групп в качестве подмножеств своих элементов. Другие типы КНАА, вероятно, тоже могут быть использованы для построения алгоритмов ЭЦП со скрытой группой, основанных на вычислительной трудности решения систем квадратных уравнений, однако это потребует разработки новых механизмов маскирования скрытой группы, что составляет самостоятельную задачу. Наличие глобальной единицы упрощает построение алгоритмов ЭЦП и предположительно дает возможность обеспечить более высокую производительность алгоритмов и меньшие размеры открытого ключа и подписи.

Известны различные варианты задания КНАА размерности $m = 6$ [7] и $m = 8$ [8]. Кроме того, известны унифицированные способы задания КНАА произвольной четной размерности [9]. Увеличение значения размерности m приводит к квадратичному увеличению числа умножений в конечном поле, над которым задана КНАА, для выполнения одного умножения некоторой пары векторов. Однако при этом имеется возможность уменьшить порядок указанного поля, поэтому вопрос выбора значения m заслуживает отдельного рассмотрения.

Для КНАА, используемых в качестве алгебраического носителя алгоритмов ЭЦП со скрытой группой, важным вопросом является изучение их строения с точки зрения декомпозиции на коммутативные подалгебры. Действительно, мультипликативная группа последних или некоторая ее подгруппа могут использоваться в качестве скрытой группы. В [10, 11] рассмотрены четырехмерные КНАА, заданные по прореженным таблицам умножения базисных векторов (ТУБВ), для которых полностью установлено их строение в упомянутом понимании. В частности, показано, что строение таких КНАА является сходным. Алгебра такого типа разбивается на множество $p^2 + p + 1$ коммутативных подалгебр порядка p^2, попарно пересекающихся строго в множестве скалярных векторов. При этом коммутативные подалгебры относятся к трем типам [10, 12] как содержащие мультипликативные группы:

- Γ_1 порядка

$$\Omega_1 = p^2 - 1, \qquad (1)$$

имеющую циклическое строение. Число таких подалгебр равно $\eta_1 = 2^{-1}p(p - 1)$;

- Γ_2 порядка

$$\Omega_2 = (p - 1)^2, \qquad (2)$$

имеющую двухмерное циклическое строение. Число подалгебр данного типа равно $\eta_2 = 2^{-1}p(p + 1)$;

- Γ_3 порядка

$$\Omega_3 = p(p - 1), \qquad (3)$$

имеющую циклическое строение. Число таких подалгебр равно $\eta_3 = p + 1$.

Таким образом, в данной работе предполагается использование четырехмерных КНАА [10], заданных по прореженным ТУБВ, как основного типа алгебраического носителя разработанных алгоритмов ЭЦП. Кроме того, что для указанных КНАА известно детальное строение, они обеспечивают возможность получения более высокой производительности процедур генерации и верификации ЭЦП, поскольку одна операция умножения векторов требует выполнения всего 8 операций умножения в конечном поле, что в два раза меньше по сравнению с использованием четырехмерных КНАА, заданных по "плотным" ТУБВ, например представленным в [4, 13].

Факторизация порядка скрытой группы не имеет критического влияния на стойкость алгоритмов ЭЦП, основанных на трудности решения систем многих квадратных уравнений. Однако используемый механизм вычисления элемента подписи **S** [1] таков, что при наличии делителей малого размера приводит к появлению существенной вероятности того, что процедуру генерации ЭЦП потребуется выполнять повторно (когда потребуется найти обратное значение из числа, которое не является взаимно простым с порядком скрытой группы). Для устранения таких повторов удобно задавать КНАА над простыми полями $GF(p)$ с простым значением $p = 2q + 1$, где q — тоже простое число. Действительно, это обеспечивает возможность задания скрытой группы порядка q^2 (являющейся подгруппой группы типа Γ_2) или порядка pq (являющейся подгруппой группы типа Γ_3). С учетом того что число подалгебр второго типа примерно в p раз больше, чем число подалгебр третьего типа, будем рассматривать в качестве основного варианта задание скрытой группы порядка q^2, которая обладает двухмерной цикличностью, т. е. порождается минимальной системой образующих (базисом), включающей два вектора, порядок каждого из которых равен q.

В последнем случае скрытая группа задается как вычисление пары векторов **G** и **H**, образующих базис $\langle \mathbf{G}, \mathbf{H} \rangle$ группы с двухмерной цикличностью. Для генерации базиса $\langle \mathbf{G}, \mathbf{H} \rangle$ в общем случае может быть использован следующий алгоритм.

Алгоритм генерации базиса $\langle \mathbf{G}, \mathbf{H} \rangle$.

1. Сгенерировать случайный обратимый вектор **R** и вычислить вектор $\mathbf{L} = \mathbf{R}^2$.

2. Если $\mathbf{L}^q = \mathbf{E}$, где **E** — вектор, являющийся глобальной двухсторонней единицей КНАА, ис-

пользумой в качестве алгебраического носителя, и $\mathbf{L} \neq \lambda\mathbf{E}$ для всех значений $\lambda \in GF(p)$ (т. е. если **L** не является скалярным вектором), то перейти к шагу 3, иначе перейти к шагу 1.

3. Сгенерировать случайное значение $\alpha \in GF(p)$, отличное от нуля и единицы поля $GF(p)$, такое, что β^2 также не равно единице поля $GF(p)$.

4. Сгенерировать случайное целое число k $(0 < k < q)$.

5. Вычислить вектор $\mathbf{H} = \alpha^2\mathbf{L}^k$.

6. Выдать в качестве базиса $\langle \mathbf{G}, \mathbf{H} \rangle$ случайной группы с двухмерной цикличностью два вектора: $\mathbf{G} = \mathbf{L}$ и **H**.

При q = 1443420272407352009010766274913970921515428178119 (160-битное простое число) имеем 161-битное простое число $p = 2q + 1$, предлагаемое для использования в качестве характеристики поля $GF(p)$, над которым задаются КНАА, служащие алгебраическим носителем рассматриваемых далее схем ЭЦП.

Схема ЭЦП со значением β = 3

Секретный ключ генерируется в виде набора четырехмерных векторов **A**, **B**, **D**, **F**, **G**, **H** и натуральных чисел x, w, i и j $(1 < x, w, i, j < q)$. Пара векторов **G** и **H** простого порядка q генерируется как базис $\langle \mathbf{G}, \mathbf{H} \rangle$ скрытой группы. В качестве векторов **A**, **B**, **D** и **F** генерируются случайные обратимые векторы, удовлетворяющие следующим условиям: $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AD} \neq \mathbf{DA}$, $\mathbf{AF} \neq \mathbf{FA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BD} \neq \mathbf{DB}$, $\mathbf{BF} \neq \mathbf{FB}$, $\mathbf{BG} \neq \mathbf{GB}$, $\mathbf{DF} \neq \mathbf{FD}$, $\mathbf{DG} \neq \mathbf{GD}$, $\mathbf{FG} \neq \mathbf{GF}$.

Открытый ключ вычисляется в виде набора четырехмерных векторов $\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{Y}_3$ и $\mathbf{Z}_3$ по следующим формулам:

$$\mathbf{Y}_1 = \mathbf{AGB},\ \mathbf{Z}_1 = \mathbf{DHA}^{-1},\ \mathbf{Y}_2 = \mathbf{FH}^w\mathbf{B},$$
$$\mathbf{Z}_2 = \mathbf{DG}^x\mathbf{F}^{-1},\ \mathbf{Y}_3 = \mathbf{AH}^i\mathbf{D}^{-1} \text{ и } \mathbf{Z}_3 = \mathbf{B}^{-1}\mathbf{G}^j\mathbf{F}^{-1}. \quad (4)$$

Процедура генерации ЭЦП.

1. Сгенерировать случайные целые числа k и t, удовлетворяющие условиям $1 < k < q$ и $1 < t < q$, и вычислить вектор $\mathbf{R} = \mathbf{AG}^k\mathbf{H}^t\mathbf{F}^{-1}$.

2. Используя некоторую коллизионно стойкую 320-битную хэш-функцию f_H, вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$, где M — подписываемый электронный документ, а хэш-значение e представлено как конкатенация двух 160-битных чисел e_1 и e_2.

3. Вычислить целочисленные значения n и d по следующим двум формулам:

$$n = \frac{k - e_1 - xe_2 - j}{e_1 + e_2 - 1} \bmod q; \quad (5)$$

$$d = \frac{t - e_1 - we_2 - i}{e_1 + e_2 - 1} \bmod q. \quad (6)$$

4. Вычислить четырехмерный вектор **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{D}^{-1}. \quad (7)$$

Подписью является пара значений e (320-битное число) и вектор **S** (четыре 161-битных значения) с общим размером ≈121 байт. Основной вклад в вычислительную трудность процедуры генерации ЭЦП вносят четыре операции экспоненцирования четырехмерных векторов, которые можно оценить как 7680 умножений в поле $GF(p)$.

Процедура верификации ЭЦП.

1. Вычислить контрольный четырехмерный вектор $\mathbf{R}_K$ по формуле

$$\mathbf{R}_K = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e_2} \quad (8)$$

с $\beta = 3$ вхождениями вектора **S** и двумя операциями возведения в степень.

2. Вычислить значение хэш-функции $e_K = f_H(M \| \mathbf{R}_K)$.

3. Сравнить значения e_K и e. Если $e_K = e$, то ЭЦП признается подлинной, в противном случае $(e_K \neq e)$ — ложной.

Вычислительная сложность процедуры верификации ЭЦП определяется двумя операциями экспоненцирования четырехмерных векторов, и ее можно оценить как 3840 умножений в поле $GF(p)$.

Доказательство корректности схемы ЭЦП.

Схема ЭЦП работает корректно, если подпись, вычисленная по процедуре генерации ЭЦП, проходит процедуру верификации как подлинная ЭЦП. Действительно, с учетом формул (5)—(8) это демонстрируется следующим образом:

$$\mathbf{R}_K = \left(\mathbf{Y}_1\mathbf{S}\mathbf{Z}_1\right)^{e_1}\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\left(\mathbf{Y}_2\mathbf{S}\mathbf{Z}_2\right)^{e_2} =$$

$$= \begin{pmatrix}\mathbf{AGBB}^{-1}\mathbf{G}^n \times \\ \times\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DHA}^{-1}\end{pmatrix}^{e_1}\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\begin{pmatrix}\mathbf{FH}^w\mathbf{BB}^{-1}\mathbf{G}^n \times \\ \times\mathbf{H}^d\mathbf{D}^{-1}\mathbf{DG}^x\mathbf{F}^{-1}\end{pmatrix}^{e_1} =$$

$$= \left(\mathbf{AG}^{n+1}\mathbf{H}^{d+1}\mathbf{A}^{-1}\right)^{e_1}\left(\mathbf{Y}_3\mathbf{S}^{-1}\mathbf{Z}_3\right)\left(\mathbf{FH}^{w+d}\mathbf{G}^{n+x}\mathbf{F}^{-1}\right)^{e_2} =$$

$$= \mathbf{AG}^{ne_1+e_1}\mathbf{H}^{de_1+e_1}\mathbf{A}^{-1}\begin{pmatrix}\mathbf{AH}^i\mathbf{D}^{-1}\mathbf{DG}^{-n} \times \\ \times\mathbf{H}^{-d}\mathbf{BB}^{-1}\mathbf{G}^j\mathbf{F}^{-1}\end{pmatrix} \times$$

$$\times\mathbf{FH}^{we_2+de_2}\mathbf{G}^{ne_2+xe_2}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{ne_1+e_1-n+j+ne_2+xe_2}\mathbf{H}^{de_1+e_1+i-d+we_2+de_2}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{n(e_1+e_2-1)+e_1+xe_2+j}\mathbf{H}^{d(e_1+e_2-1)+e_1+we_2+i}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^{\frac{k-e_1-xe_2-j}{e_1+e_2-1}(e_1+e_2-1)+e_1+xe_2+j} \times$$

$$\times\mathbf{H}^{\frac{t-e_1-we_2-i}{e_1+e_2-1}(e_1+e_2-1)+e_1+we_2+i}\mathbf{F}^{-1} =$$

$$= \mathbf{AG}^k\mathbf{H}^t\mathbf{F}^{-1} = \mathbf{R} \Rightarrow f\left(M \| \mathbf{R}_K\right) = f\left(M \| \mathbf{R}\right) \Rightarrow e_K = e.$$

Постквантовая стойкость описанной схемы ЭЦП обеспечивается тем, что вычисление секретного ключа по открытому ключу связано с решением системы из 11 квадратных векторных уравнений (определяемых шестью формулами (4) и условием попарной перестановочности векторов **G**, **H**, $\mathbf{H}^w$, $\mathbf{G}^x$, $\mathbf{G}^j$ и $\mathbf{H}^i$) с 10 неизвестными (которыми являются четырехмерные векторы **A**, **B**, **D**, **F**, **G**, **H**, $\mathbf{H}^w$, $\mathbf{G}^x$, $\mathbf{G}^j$ и $\mathbf{H}^i$), заданной над использованной в качестве алгебраического носителя четырехмерной КНАА. Указанная система векторных уравнений сводится к системе из 44 квадратных уравнений с 40 неизвестными, заданной над полем $GF(p)$ со 161-битным значением порядка.

Заметим, что в данной схеме ЭЦП секретный ключ можно сформировать в виде набора **A**, **B**, **D**, **F**, **G**, **H**, $\mathbf{H}_w$, $\mathbf{G}_x$, $\mathbf{G}_j$ и $\mathbf{H}_i$, в котором векторы $\mathbf{H}_w$, $\mathbf{G}_x$, $\mathbf{G}_j$ и $\mathbf{H}_i$ выбираются случайным образом из скрытой группы, задаваемой базисом ⟨**G**, **H**⟩. При этом процедура верификации остается неизменной, однако процедура генерации ЭЦП приобретает вид следующего алгоритма.

1. Сгенерировать случайные целые числа k_1, k_2, k_3, k_4, k_5 и k_6 и вычислить вектор

$$\mathbf{R} = \mathbf{A}\mathbf{G}^{k_1}\mathbf{H}^{k_2}\mathbf{H}_w^{k_3}\mathbf{G}_x^{k_4}\mathbf{G}_j^{k_5}\mathbf{H}_i^{k_6}\mathbf{F}^{-1}. \qquad (9)$$

2. Вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$.

3. Вычислить целочисленные значения n_i для $i = 1, 2, \ldots, 6$ по следующим формулам:

$$n_1 = \frac{k_1 - e_1}{e_1 + e_2 - 1} \bmod q; \quad n_2 = \frac{k_2 - e_1}{e_1 + e_2 - 1} \bmod q;$$

$$n_3 = \frac{k_3 - e_2}{e_1 + e_2 - 1} \bmod q; \quad n_4 = \frac{k_4 - e_2}{e_1 + e_2 - 1} \bmod q;$$

$$n_5 = \frac{k_5 - 1}{e_1 + e_2 - 1} \bmod q; \quad n_6 = \frac{k_6 - 1}{e_1 + e_2 - 1} \bmod q.$$

4. Вычислить четырехмерный вектор **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{n_1}\mathbf{H}^{n_2}\mathbf{H}_w^{n_3}\mathbf{G}_x^{n_4}\mathbf{G}_j^{n_5}\mathbf{H}_i^{n_6}\mathbf{D}^{-1}. \qquad (10)$$

В модифицированной процедуре генерации ЭЦП выполняется 12 операций экспоненцирования, т. е. ее производительность в три раза меньше по сравнению с исходным вариантом этой процедуры. Видно, что предпочтительным является вычисление значений $\mathbf{H}_w$, $\mathbf{G}_x$, $\mathbf{G}_j$ и $\mathbf{H}_i$ по формулам $\mathbf{H}_w = \mathbf{H}^w$, $\mathbf{G}_x = \mathbf{G}^x$, $\mathbf{G}_j = \mathbf{G}^j$ и $\mathbf{H}_i = \mathbf{H}^i$. Из модифицированной версии процедуры генерации ЭЦП явно видно, что операции возведения векторов **G** и **H** в секретные степени при вычислении элементов открытого ключа используются как технический прием задания случайного выбора векторов из скрытой группы, который обеспечивает повышение производительности схемы ЭЦП.

Схема ЭЦП со значением β = 4

Секретный ключ генерируется в виде набора четырехмерных векторов **A**, **B**, **G** и натурального числа x ($1 < x < q$), где векторы **G** и **H** порядка q составляют базис ⟨**G**, **H**⟩ скрытой группы. В качестве векторов **A** и **B** генерируются случайные обратимые векторы, удовлетворяющие условиям $\mathbf{AB} \neq \mathbf{BA}$, $\mathbf{AG} \neq \mathbf{GA}$, $\mathbf{BG} \neq \mathbf{GB}$.

Открытый ключ вычисляется в виде набора векторов **Y**, **Z** и **U** по следующим формулам:

$$\mathbf{Y} = \mathbf{AGB}, \ \mathbf{Z} = \mathbf{AG}^x\mathbf{B} \text{ и } \mathbf{U} = \mathbf{AHB}. \qquad (11)$$

Процедура генерации ЭЦП.

1. Сгенерировать случайные целые числа k и t ($1 < k < q$; $1 < t < q$) и вычислить четырехмерный вектор

$$\mathbf{R} = \mathbf{B}^{-1}\mathbf{G}^k\mathbf{H}^t\mathbf{B}. \qquad (12)$$

2. Используя 320-битную хэш-функцию f_H, вычислить значение $e = e_1 \| e_2 = f_H(M \| \mathbf{R})$, где M — подписываемый электронный документа, а хэш-значение e представлено как конкатенация двух 160-битных чисел e_1 и e_2.

3. Вычислить целочисленные значения n и d по следующим двум формулам:

$$n = \frac{k - e_1 - e_1^2 - xe_1}{e_1(e_1 + e_2 + 1)} \bmod q; \qquad (13)$$

$$d = \frac{t - e_1 e_2}{e_1(e_1 + e_2 + 1)} \bmod q. \qquad (14)$$

4. Вычислить подгоночный элемент ЭЦП в виде четырехмерного вектора **S** по формуле

$$\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^n\mathbf{H}^d\mathbf{A}^{-1}. \qquad (15)$$

Подписью является пара (e, **S**) с общим размером ≈121 байт. Основной вклад в вычислительную трудность процедуры генерации ЭЦП вносят четыре операции экспоненцирования четырехмерных векторов, из которых две выполняются при генерации вектора **R** и две — при вычислении вектора **S**.

Процедура верификации ЭЦП.

1. Вычислить контрольный четырехмерный вектор $\mathbf{R}_K$ по формуле

$$\mathbf{R}_K = \left((\mathbf{SY})^{e_1}\,\mathbf{S}(\mathbf{US})^{e_2}\,\mathbf{ZSY}\right)^{e_1} \qquad (16)$$

с β = 4 вхождениями вектора **S** и тремя операциями возведения в степень.

2. Вычислить значение хэш-функции $e_K = f_H(M \| \mathbf{R}_K)$.

3. Сравнить значения e_K и e. Если $e_K = e$, то ЭЦП признается подлинной, иначе ($e_K \neq e$) — ложной.

Доказательство корректности схемы ЭЦП.

Корректность работы последней схемы ЭЦП показывается с учетом формул (11)–(16) следующим образом:

$$\mathbf{R}_K = \left((\mathbf{SY})^{e_1}\,\mathbf{S}(\mathbf{US})^{e_2}\,\mathbf{ZSY}\right)^{e_1} =$$

$$= \left(\left(\mathbf{B}^{-1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{GB}\right)^{e_1}\mathbf{S}\left(\mathbf{AHG}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}\right)^{e_2}\mathbf{AG}^{x}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{A}^{-1}\mathbf{Y}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{ne_1+e_1}\mathbf{H}^{de_1}\mathbf{BSAG}^{ne_2}\mathbf{H}^{de_2+e_2}\mathbf{A}^{-1}\mathbf{AG}^{x+n}\mathbf{H}^{d}\mathbf{A}^{-1}\mathbf{Y}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{ne_1+e_1}\mathbf{H}^{de_1}\mathbf{G}^{n}\mathbf{H}^{d}\mathbf{G}^{ne_2}\mathbf{H}^{de_2+e_2}\mathbf{G}^{x+n}\mathbf{H}^{d}\mathrm{GB}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{ne_1+n+ne_2+e_1+x+n+1}\mathbf{H}^{de_1+d+de_2+e_2+d}\mathbf{B}\right)^{e_1} =$$

$$= \left(\mathbf{B}^{-1}\mathbf{G}^{n(e_1+e_2+1)+e_1+x+1}\mathbf{H}^{d(e_1+e_2+1)+e_2}\mathbf{B}\right)^{e_1} =$$

$$= \mathbf{B}^{-1}\mathbf{G}^{ne_1(e_1+e_2+1)+e_1^2+xe_1+e_1}\mathbf{H}^{de_1(e_1+e_2+1)+e_1e_2}\mathbf{B} =$$

$$= \mathbf{B}^{-1}\mathbf{G}^{k}\mathbf{H}^{t}\mathbf{B} = \mathbf{R} \Rightarrow f\left(M \,\|\, \mathbf{R}_K\right) = f\left(M \,\|\, \mathbf{R}\right) \Rightarrow e_K = e.$$

Постквантовая стойкость представленной схемы ЭЦП обеспечивается тем, что вычисление секретного ключа по открытому ключу требует нахождения решения системы из следующих 5 квадратных векторных уравнений с 5 неизвестными, **A**, $\mathbf{B}^{-1}$, **G**, $\mathbf{G}_x = \mathbf{G}^x$ и **H**:

$$\mathbf{YB}^{-1} = \mathbf{AG},\ \mathbf{ZB}^{-1} = \mathbf{AG}_x,\ \mathbf{UB}^{-1} = \mathbf{AH},$$
$$\mathbf{GG}_x = \mathbf{G}_x\mathbf{G},\ \mathbf{GH} = \mathbf{HG}.$$

Указанная система векторных уравнений сводится к системе из 20 квадратных уравнений с 20 неизвестными, заданной над полем $GF(p)$, порядок которого равен 161-битному простому числу.

Обсуждение

Известные алгоритмы ЭЦП и алгоритмы открытого распределения ключей и открытого шифрования, основанные на вычислительной сложности нахождения решений систем многих квадратных уравнений с многими неизвестными, относятся к так называемой многомерной криптографии [14, 15]. Предложенные в данной работе алгоритмы ЭЦП имеют общность с криптосхемами многомерной криптографии по используемой базовой вычислительно трудной задаче, которая определяет их постквантовую стойкость. По построению алгоритмы ЭЦП со скрытой группой существенно отличаются от двухключевых алгоритмов многомерной криптографии.

Существенно, что в предложенных схемах ЭЦП системы квадратных уравнений заданы над полем значительно большего порядка, чем в случае алгоритмов многомерной криптографии. Однако в последних число квадратных уравнений и число неизвестных составляет от 30 до 200, тогда как в первых число неизвестных равно 40 (в алгоритме со значением $\beta = 3$) и 20 (в алгоритме со значением $\beta = 4$). Меньшее число неизвестных компенсируется тем, что квадратные уравнения задаются над полем, размер порядка которого значительно больше (в 10 и более раз).

В [1] предложен неформальный показатель ψ уровня стойкости алгоритмов ЭЦП, основанных на вычислительной сложности решения систем многих квадратных уравнений, трактуемый как произведение двоичного логарифма от порядка поля, над которым задана система, и числа неизвестных. В соответствии с этим критерием предложенные два алгебраических алгоритма ЭЦП со скрытой группой обладают более высоким ожидаемым уровнем стойкости по сравнению с многими известными постквантовыми алгоритмами ЭЦП, относящимися к многомерной криптографии. Однако вопрос детального рассмотрения их стойкости к атакам различных типов является открытым.

Предложенные два алгоритма используют проверочные уравнения с различным числом β вхождений вектора **S**. Из построения алгоритмов видно, что с ростом значения β размер ЭЦП не изменяется, а размер открытого ключа больше зависит от формул, по которым вычисляются элементы открытого ключа в зависимости от элементов секретного ключа, чем от значения β.

Механизм многократного вхождения вектора **S** как подгоночного элемента подписи (элемента, вычисляемого в зависимости от рандомизирующего элемента e, определяемого значением вектора рандомизации **R**, таким способом, что для сгенерированной подписи выполняется проверочное уравнение) предназначен для предотвращения возможности использования **S** в качестве подгоночного значения также и при подделке подписи (атаки на алгоритм ЭЦП, связанные с попыткой вычисления правильной подписи без вычисления секретного ключа). Использование значения $\beta = 2$ представляется достаточным (при соответствующем построении алгоритма ЭЦП со скрытой группой) для достижения указанной цели. Однако разработка алгоритмов ЭЦП со значениями $\beta = 3$ и $\beta = 4$ также представляют интерес, поскольку при этом сохраняются достаточно высокая производительность и малые размеры подписи и открытого ключа и обеспечивается потенциально более высокий уровень защищенности от атак с использованием **S** в качестве подгоночного параметра алгоритма подделки ЭЦП.

Сравнение известных и предложенных постквантовых алгоритмов ЭЦП, использующих однотипную вычислительно трудную задачу, представлено в таблице, которая показывает, что вторые обладают преимуществами по некоторым параметрам.

Сравнение предложенных алгоритмов ЭЦП с известными алгоритмами, основанными на вычислительной сложности решения систем многих квадратичных уравнений

Алгоритм ЭЦП	Размер ЭЦП, байт	Размер открытого ключа, байт	Число квадратных уравнений (неизвестных)	Порядок поля, над которым заданы уравнения	Показатель ψ
[14]	—	—	27 (27)	2^{16}	432
Rainbow [16]	33	16065	27 (33)	2^8	264
QUARTZ [15]	16	72704	100 (107)	2^4	428
Rainbow [17] (3 разных версии)	66—204	>150000—>1900000	64 (96)—128 (204)	2^4, 31, 2^8	384—1632
[1] (β = 2)	160	512	28 (28)	$>2^{256}$	≈7168
Предложенный (β = 3)	121	483	36 (32)	$>2^{160}$	≈5120
Предложенный (β = 4)	121	242	20 (20)	$>2^{160}$	≈3200

Заключение

Увеличение числа вхождений элемента подписи **S** в проверочное уравнение расширяет вариативность разработки постквантовых алгебраических алгоритмов ЭЦП со скрытой группой при сохранении их преимуществ по производительности и размерам открытого ключа и подписи по сравнению с известными постквантовыми схемами ЭЦП. Представляет интерес использование проверочных уравнений в предложенных двух алгоритмах для разработки постквантовых алгебраических алгоритмов на КНАА, заданных над конечными полями характеристики два, что обеспечит снижение схемотехнической сложности реализации и повышение производительности. Однако это является вопросом отдельного рассмотрения. Также для будущих исследований представляется интересным и важным рассмотрение выбора параметров алгоритмов ЭЦП со скрытой группой при использовании в качестве их алгебраического носителя шестимерных и восьмимерных КНАА, заданных над простыми конечными полями $GF(p)$ и полями $GF(2^z)$.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а) и бюджетной темы № FFZF-2022-0007.

Литература

1. *Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Костина А. А.* Новый подход к разработке алгоритмов цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2021. № 4. С. 45—49. DOI: 0.52190/2073-2600_2021_4_45.

2. *Молдовян Д. Н., Молдовян А. А., Молдовян Н. А*. Новая концепция разработки постквантовых алгоритмов цифровой подписи на некоммутативных алгебрах // Вопросы кибербезопасности. 2022. № 1(47). С. 18—25. DOI: 10.21681/2311-3456-2022-1-18-25.

3. *Moldovyan N. A., Moldovyan A. A.* Finite Non-commutative Associative Algebras as Carriers of Hidden Discrete Logarithm Problem // Вестник ЮУрГУ. Сер. "Математическое моделирование и программирование". 2019. Т. 12. № 1. С. 66—81. DOI: 10.14529/mmp190106.

4. *Moldovyan A. A., Moldovyan N. A.* Post-quantum signature algorithms based on the hidden discrete logarithm problem // Computer Science J. Moldova. 2018. V. 26. № 3(78). P. 301—313.

5. *Молдовян А. А., Молдовян Н. А., Молдовян Д. Н., Фахутдинов Р. Ш.* Схемы цифровой подписи с удвоенным проверочным уравнением // Вопросы защиты информации. 2021. № 2. С. 30—36. DOI: 10.52190/2073-2600_2021_2_30.

6. *Moldovyan N. A., Moldovyan A. A.* Candidate for practical post-quantum signature scheme // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2020. Т. 16. Вып. 4. С. 455—461. DOI: 10.21638/11701/spbu10.2020.410.

7. *Moldovyan D. N.* A unified method for setting finite non-commutative associative algebras and their properties // Quasigroups and Related Systems. 2019. V. 27. № 2. P. 293—308.

8. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* Digital signature scheme with doubled verification equation // Computer Science J. Moldova. 2020. V. 28. № 1(82). P. 80—103.

9. *Moldovyan N. A.* Unified Method for Defining Finite Associative Algebras of Arbitrary Even Dimensions // Quasigroups and Related Systems. 2018. V. 26. № 2. P. 263—270.

10. *Молдовян Д. Н.* Задание шестимерных алгебр как носителей криптосхем, основанных на скрытой задаче дискретного логарифмирования // Вопросы защиты информации. 2021. № 1. С. 26—32. DOI: 10.52190/2073-2600_2021_1_26.

11. *Moldovyan N. A., Moldovyan A. A.* Digital signature scheme on the 2x2 matrix algebra // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 254—261. DOI: 10.21638/11701/spbu10.2021.303.

12. *Moldovyan D. N.* A practical digital signature scheme based on the hidden logarithm problem // Computer Science J. Moldova. 2021. V. 29. № 2(86). P. 206—226.

13. *Moldovyan N. A.* Signature Schemes on Algebras, Satisfying Enhanced Criterion of Post-quantum Security // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2(93). P. 62—67.

14. *Shuaiting Q., Wenbao H., Yifa Li, Luyao J.* Construction of Extended Multivariate Public Key Cryptosystems // International J. Network Security. 2016. Vol. 18. № 1. P. 60—67.

15. *Jintai D., Dieter S.* Multivariable Public Key Cryptosystems [Электронный ресурс]. Режим доступа: https://eprint.iacr.org/2004/350.pdf (дата обращения: 15.02.2022).

16. *Ding J., Schmidt D.* Rainbow, a new multivariable polynomial signature scheme : Conference on Applied Cryptography and Network Security — ACNS 2005. Springer Lecture Notes in Computer Science. 2005. V. 3531. P. 164—175.

17. Rainbow Signature. One of three NIST Post-quantum Signature Finalists [Электронный ресурс]. Режим доступа: https://www.pqcrainbow.org/ (дата обращения: 15.02.2022)

Typical verification equations in algebraic digital signature algorithms with a hidden group

D. N. Moldovyan
St. Petersburg Federal Research Center of the RAS (SPC RAS),
St. Petersburg, Russia

Typical forms of the verification equation of the digital signature algorithms with a hidden group, which use finite non-commutative associative algebras as an algebraic support are proposed. The principal feature of the algorithms of this type is that the signature includes a certain vector ***S*** *as one of its elements, which enters several times in the verification equation. The multiple entry of the vector* ***S*** *in the verification equation determines the security of the algorithms to the forging signature attacks that use the vector* ***S*** *as a fitting parameter. However the multiple entry requires the use of a special method for calculating the vector* ***S****, when using the secret key. The specific form of the verification equation determines the formulas for calculation of the public-key elements. It is shown that the calculation of the signature can be performed in several different ways, but in all cases the signature randomization mechanism includes exponentiations of the elements of the hidden group to the degrees with random values.*

Keywords: information security, digital signature, post-quantum cryptography, finite associative algebra, non-commutative algebra, hidden group.

Bibliography — 17 references. *Received February 18, 2022*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.932.2
DOI: 10.52190/2073-2600_2022_1_38

Метод обнаружения стеганографических вставок, встроенных методом Коха—Жао, в изображениях с низким заполнением стегоконтейнера

Д. Э. Вильховский
Омский государственный университет им. Ф. М. Достоевского, Омск, Россия

Представлен метод обнаружения стеганографических вставок, выполненных методом Коха—Жао, и области их расположения в черно-белых и цветных изображениях с низким уровнем стеганографической нагрузки (10—25 % от общего объема стегоконтейнера). Метод основан на использовании двух сигнатур и кластеризации имеющейся последовательности коэффициентов дискретного косинусного преобразования с выделением кластера, содержащего элементы последовательности, одновременно удовлетворяющие условиям, заданным по каждой из сигнатур.

Ключевые слова: стегоанализ, стеганографический анализ, анализ стегоконтейнера, метод Коха—Жао, обнаружение стеганографических вставок.

Проблема информационной безопасности затрагивает в том числе проблематику обнаружения секретных сообщений (стеганографических вставок), встраиваемых в различные медиафайлы, которые могут быть переданы третьим лицам, доступ для которых к подобного рода информации изначально не предоставлен или даже запрещен. Следовательно, разработка метода стеганографического анализа имеет важное значение с точки зрения повышения общей информационной безопасности организации, а также в масштабах национальной информационной безопасности.

В данной работе автор в качестве медиафайлов исследует цветные и черно-белые фотографические цифровые изображения. В качестве метода стеганографии, в противодействие которому предлагается изложенный в работе метод стегоанализа, исследуется алгоритм встраивания Коха—Жао [1]. Выбор данного алгоритма обусловлен его достаточно широким распространением для изображений формата .JPEG, а также для встраивания в изображения, которые впоследствии планируют подвергнуть сжатию (архивированию), в связи с устойчивостью данного алгоритма к сжатию, т. е. отсутствию существенных искажений при обработке такого контейнера в целях последующего извлечения секретного сообщения.

Вильховский Данил Эдуардович, ассистент кафедры "Информационная безопасность".
E-mail: vilkhovskiy@gmail.com

Статья поступила в редакцию 31 января 2022 г.

Общая постановка задачи

Известно, что алгоритм встраивания Коха—Жао основывается на использовании коэффициентов дискретного косинусного преобразования (ДКП) с предварительной разбивкой используемого изображения-контейнера на блоки размерностью 8×8 [2]. Также известно, что для снижения риска обнаружения при работе с ДКП встраивание следует осуществлять в среднечастотные компоненты.

Таким образом, для общей постановки задачи об обнаружении стеганографических вставок, выполненных методом Коха—Жао, в изображениях с низкой стегонагрузкой, а также области их расположения исходят из следующих допущений:

- встраивание производится в 3-ю и 4-ю компоненты;
- уровень стеганографической нагрузки не превышает 25 % от общего объема стегоконтейнера;
- встраивание производится дискретным образом, что позволяет дополнительно использовать преимущество малых локаций встраивания.

На рис. 1 приведен пример областей встраивания, выполненных методом Коха—Жао с учетом изложенных допущений. Границами прямоугольников отмечены области, содержащие встроенные сообщения.

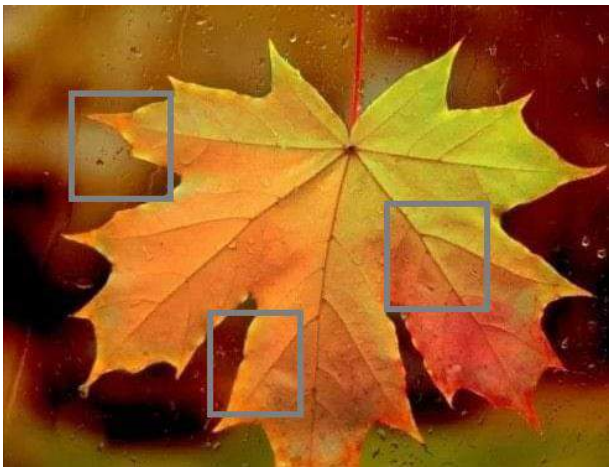


Рис. 1. Изображение, содержащее дискретные встраивания, выполненные методом Коха—Жао

Видно, что в изображение выполнено три встраивания, каждое из которых не превышает 3,35 % представленного фотографического изображения. В сумме все три вставки занимают не более 10 % общего объема стегоконтейнера.

Необходимо разработать метод стегоанализа контейнеров с низким уровнем стеганографической нагрузки, который позволит установить не только факт наличия встраивания, но и место расположения (осуществить локализацию) всех областей встраивания с высокой степенью точности и сравнительно небольшой ресурсоемкостью.

Использование двух сигнатур как необходимое и достаточное условие установления наличия и локализации стеганографических вставок

Анализ изменений в гистограмме последовательности коэффициентов ДКП в результате встраивания какого-либо сообщения позволил выявить следующие две основополагающие особенности:

- значения элементов последовательности, в которые было выполнено встраивание, существенно отличаются от значений тех элементов последовательности, которые не содержат стеганографических вставок;
- модульные значения элементов последовательности, в которые было выполнено встраивание, имеют незначительные отличия между собой.

Для фотографического изображения со встраиванием, приведенного на рис. 1, гистограмма последовательности блоков коэффициентов ДКП имеет вид, приведенный на рис. 2.

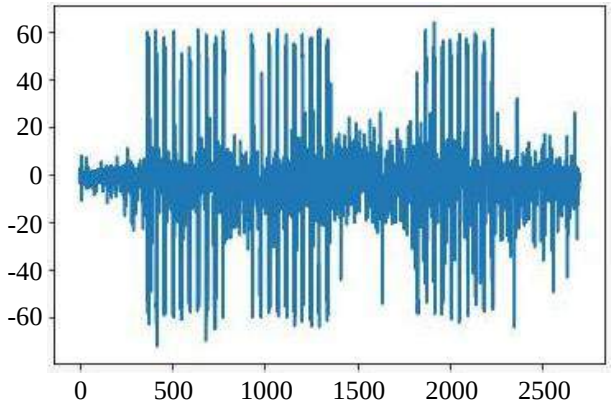


Рис. 2. Гистограмма последовательности блоков коэффициентов ДКП фотографического изображения, содержащего три дискретных встраивания

Таким образом, определены следующие две сигнатуры, необходимые и достаточные для проведения стеганографического анализа:

- Отклонение P_i текущего значения элемента последовательности от максимума среди всей последовательности, взятого по модулю:

$$P_i = M_j - |C_i|,$$

где M_j — максимальное значение среди всех элементов последовательности, взятое по модулю;

$|C_i|$ — значение анализируемого элемента последовательности, взятое по модулю.

- Отклонение R_i текущего значения элемента последовательности от его последующего значения:

$$R_i = C_i - C_{i+1},$$

где C_i — значение анализируемого элемента последовательности;

C_{i+1} — значение элемента последовательности, следующего за анализируемым.

Сигнатура P_i позволяет установить наличие встраивания. Сигнатура R_i, являясь вспомогательной в целях установления факта встраивания, помогает определить границы встраивания. В общем виде можно сделать следующие выводы:

- если значение сигнатуры P_i анализируемого элемента стремится к максимальному значению среди всех значений элементов последовательности, взятых по модулю, то такой элемент следует признать как чистый, т. е. не содержащий встраивания;

- если значение сигнатуры P_i анализируемого элемента стремится к значению, близкому к нулю, анализируемый элемент следует признать как блок, в который было осуществлено встраивание;
- если модульное значение сигнатуры R_i анализируемого элемента стремится к максимальному значению среди всех элементов последовательности, взятых по модулю, то такой элемент следует признать границей встраивания;
- если значение сигнатуры R_i анализируемого элемента стремится к значению, близкому к нулю, то анализируемый элемент следует признать элементом, не являющимся границей встраивания.

Таким образом, блок содержит встраивание, если одновременно удовлетворяются условия:

- значение сигнатуры P_i анализируемого элемента стремится к значению, близкому к нулю;
- значение сигнатуры R_i анализируемого элемента стремится к значению, близкому к нулю.

В математическом виде такое условие можно записать как условие оператора строгого логического И:

$$P_i = n \pm \alpha;\ R_i = m \pm \beta, \qquad (1)$$

где n — значение сигнатуры P_i, при котором $(n-\alpha) \to 0$;

α — допустимый разброс значений по сигнатуре P_i;

m — значение сигнатуры R_i, при котором $(m-\beta) \to 0$ или $(m+\beta) \to 0$;

β — допустимый разброс значений по сигнатуре R_i.

Кластеризация на основе двух сигнатур в целях выявления областей встраивания

Основываясь на представленных результатах, для выявления факта встраивания и локализации области встраивания необходимо произвести кластеризацию всех элементов исходной последовательности в двухмерном пространстве, где:

- P_i определяет местоположение каждого из элементов исследуемой последовательности относительно оси OX;
- R_i определяет местоположение каждого из элементов исследуемой последовательности относительно оси OY.

Например, разнесение всех элементов последовательности, представленной на рис. 2, на плоскости с использованием двух выявленных сигнатур имеет вид, показанный на рис. 3.

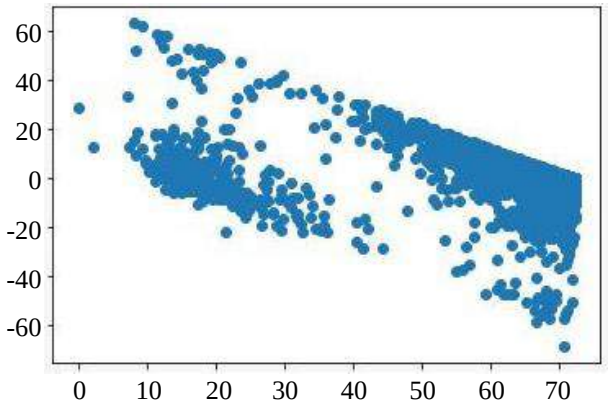


Рис. 3. Разнесение элементов последовательности на плоскости на основе значений их сигнатур

Можно заметить, что для анализируемого изображения в результате разнесения элементов последовательности на основе значений их сигнатур образуется три основных кластера. Помимо этого, можно предположить, что в некоторой части элементов последовательности может присутствовать некоторое искажение, т. е. нельзя с большой точностью утверждать, к какому кластеру они относятся и относятся ли вообще к одному из кластеров. Такие элементы последовательности можно назвать цифровым шумом.

Так, условию, заданному выражением (1), удовлетворяют только точки, принадлежащие кластеру 1. Таким образом, следует полагать, что блоки, которым эти точки соответствуют, содержат встраивание.

Применение алгоритма машинного обучения DBSCAN для целей стеганографического анализа

Для успешной автоматизации задач выявления и локализации блоков, содержащих встраивание, необходимо решить проблему кластеризации, т. е. определения центройдов кластеров, в особенности центройда первого кластера, принадлежность к которому позволяет сделать вывод о наличии и локации встраивания.

С учетом данной постановки задачи для условия отнесения элемента последовательности к категории стего, т. е. содержащего встраивание, представленного выражением (1), можно определить, что:

- n — значение сигнатуры P_i, являющейся координатой *x* центройда кластера 1;
- m — значение сигнатуры R_i, являющейся координатой *y* центройда кластера 1.

В целях выявления устойчивых кластеров и установления значений координат центройдов

кластеров (инициализации) предлагается использовать алгоритм машинного обучения DBSCAN [1].

Данный алгоритм позволяет кластеризовать имеющуюся последовательность в двухмерном пространстве, одновременно работая с шумом и отсекая его. В основе алгоритма DBSCAN лежат всего 2 параметра:

- eps — плотность соседних элементов, допустимая для того, чтобы считать анализируемый элемент элементом кластера;
- min samples — минимально допустимое количество элементов, формирующих один кластер.

Таким образом, важнейшей задачей, которую следует решить для успешного использования алгоритма DBSCAN, является проблема выбора необходимой и достаточной плотности соседних элементов, а также минимального количества элементов кластера, т. е. параметров алгоритма, при которых достигается высокий функционал при адекватной его точности.

Для обнаружения стеганографических вставок, встроенных методом Коха—Жао, эвристически определены следующие параметры, которые можно считать оптимальными:

- eps = 0,3;
- min samples = 5.

Так, для случая, представленного на рис. 2, характеризующего последовательность блоков коэффициентов дискретного косинусного преобразования исследуемого образца фотографического изображения-стегоконтейнера, результаты кластеризации посредством алгоритма машинного обучения DBSCAN имеют вид, приведенный на рис. 4.

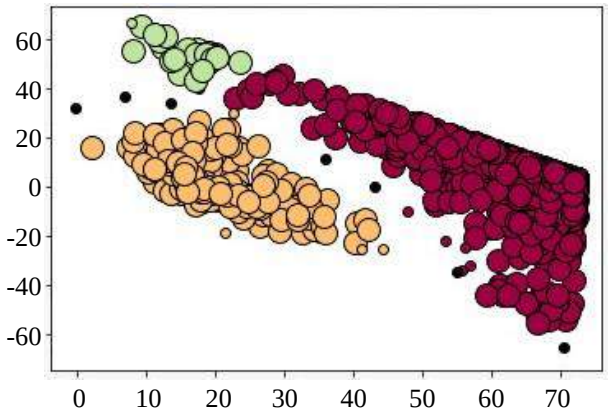


Рис. 4. Кластеризация пикселей анализируемого изображения с использованием алгоритма DBSCAN

Видно, что множество элементов исследуемой последовательности разделено на три кластера. При этом часть элементов определена как шумы, что графически отображается в виде плотных черных точек меньшего диаметра.

Также определены координаты центройда кластера, содержащего элементы последовательности со встроенным сообщением, — (22,72768; -0,93326), с центром масс в точке (12,72768; 1,233265).

Так, для исследуемого образца фотографического изображения условие отнесения элемента к категории элементов, содержащих встраивание, имеет следующий вид:

$$P_i = 22,72768 \pm 22,04568;\ R_i = -0,93326 \pm 21,83658.$$

Заключение

Таким образом, предложенный метод стегоанализа позволил определить исследуемое фотографическое изображение, представленное на рис. 1, как стего, а также локализовать области встраивания. Результаты локализации областей встраивания представлены на рис. 5. Прямоугольные области с серой заливкой являются областями встраивания, обнаруженными при помощи предлагаемого метода обнаружения и локализации стеганографических вставок, выполненных методом Коха—Жао.

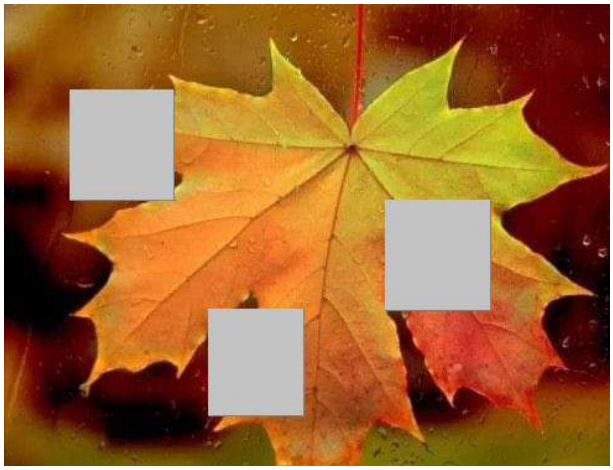


Рис. 5. Результаты локализации области встраивания

В целях тестирования точности обнаружения стеганографических вставок, выполненных методом Коха—Жао, а также точности их локализации предложенным в работе методом стеганографического анализа проанализировано 500 цветных и 500 черно-белых фотографических изображений.

Тестирование показало, что:

- предложенный метод стегоанализа способен обнаруживать встраивание в 99,9 % случаев;
- средняя точность обнаружения области составляет 96,3 %, т. е. границы обнаруженной области встраивания отклоняются от фактической области встраивания в среднем не более чем на 3,7 %;

- точность обнаружения и локализации не зависит от фактического уровня заполнения стегоконтейнера и стабильна при работе с 10—25 %-м уровнем стегонагрузки;
- точность метода не зависит от цветовой гаммы и палитры анализируемого изображения, т. е. метод показывает приблизительно одинаковую точность при работе с цветными и черно-белыми изображениями.

Таким образом, можно сделать вывод, что предлагаемый в данной работе метод обнаружения стеганографических вставок, встроенных методом Коха—Жао, в фотографических изображениях с низким уровнем заполнения стегоконтейнера обладает высокой эффективностью обнаружения и локализации.

Литература

1. *Koch E., Zhao J.* Towards robust and hidden image copyright labeling // IEEE Workshop on Nonlinear Signal and Image Processing. 1995. P. 452—455.

2. *Жерон О.* Прикладное машинное обучение с помощью Scikit-Learn, Keras и TensorFlow: концепции, инструменты и техники для создания интеллектуальных систем. Изд. 2 / Пер. с англ. — СПб.: ООО "Диалектика", 2020.

Method of detecting inserts embedded using the Koch—Zhao steganographic method in low stego-payload images

D. E. Vilkhovsky
Dostoevsky Omsk State University, Omsk, Russia

The article presents a method for detecting steganographic inserts made by the Koh—Zhao method and their locating in gray-scale and color images with low stego-payload (10—25 % of the total carrier). The method is based on two signatures and the subsequent clustering of the existing discrete cosine transform coefficient array and the further selection of the cluster containing the array elements that meet both signature conditions.

Keywords: steganalysis, steganographic analysis, stegocarrier analysis, Koh—Zhao method, steganographic-insert detection.

Bibliography — 2 references. *Received January 31, 2022*

УДК 004
DOI: 10.52190/2073-2600_2022_1_43

Методика определения срока временного ограничения прав граждан на выезд из Российской Федерации на основе нечеткого моделирования

И. Д. Королев, д-р техн. наук; *В. В. Губарев; М. Ф. Ковнацкий*
Краснодарское высшее военное училище им. генерала армии С. М. Штеменко,
г. Краснодар, Россия

Рассмотрена разработанная авторами методика определения срока временного ограничения прав граждан на выезд из Российской Федерации на основе математического аппарата теории нечетких множеств, нечеткой логики и экспертных оценок.

Ключевые слова: граждане, решения об ограничении, показатели, лингвистические переменные, нечеткие множества, функции принадлежности, экспертный опрос.

В соответствии с требованиями законодательства Российской Федерации, граждане, допущенные или ранее допускавшиеся к государственной тайне с грифом секретности "особой важности" или "совершенно секретно", могут быть временно ограничены в праве выезда за границу Российской Федерации [1], что документально отображено в "решении о временном ограничении права гражданина Российской Федерации, осведомленного в сведениях особой важности и (или) совершенно секретных сведениях, на выезд из Российской Федерации или возможности выдачи паспорта и выезда из Российской Федерации, а также по определению срока временного ограничения этого права" (далее — решениях), принимаемых уполномоченными должностными лицами.

Конституционный Суд Российской Федерации определил, что накладываемые ограничения должны быть необходимы и пропорциональны конституционно признанным целям, а государство должно использовать не чрезмерные, а лишь необходимые и строго обусловленные этими целями меры [2, 3]. Иными словами, решения о накладываемых ограничениях должны приниматься с учетом соразмерности (пропорциональности) ограничения конституционных прав граждан, что предполагает оценку всех влияющих факторов, т. е. учитываться должны не только наличие у гражданина формального допуска к "особой важности" или "совершенно секретным" сведениям и фактического доступа к ним, но и другие показатели, определенные требованиями руководящих документов.

Анализ показывает, что в подавляющем большинстве случаев в принимаемых решениях устанавливается максимально возможный срок ограничения до 5 лет, что говорит о необъективности и нарушении тем самым конституционных прав граждан. Причинами такого состояния дел являются:

- отсутствие порядка оценивания установленных показателей;
- сложность оценивания большого количества показателей, обусловленная психологическими особенностями человеческого мозга, не способного одновременно удерживать в своей оперативной памяти объем информации более 7—9 единиц [4];
- ограниченный лимит времени, отводимый на принятие решений и, соответственно, на определение срока ограничения, установленный требованиями нормативно-правовых актов, не позволяющий в отдельных случаях проводить полноценную оценку всей необходимой информации о гражданине;
- субъективизм самого процесса принятия решения, когда лицо, принимающее решение, определяет срок ограничения, руководствуясь своими знаниями, опытом, пониманием требований руководящих документов, а также интуитивной оценкой значения того или иного показателя.

Из сказанного вытекает актуальность задачи разработки методики, позволяющей повысить обоснованность принимаемых решений (в части, касающейся определения срока ограничения) и уменьшить время, затрачиваемое на их принятие.

Одним из путей решения данной задачи является автоматизация процесса принятия решений, представляющего собой систему, на вход которой

Королев Игорь Дмитриевич, профессор, профессор кафедры "Защита информации специальными методами и средствами".
E-mail: pi_korolev@mail.ru
Губарев Владислав Владимирович, адъюнкт.
E-mail: vladuha79@mail.ru
Ковнацкий Михаил Федорович, начальник службы — помощник начальника училища по защите государственной тайны.
E-mail: vladuha79@mail.ru

Статья поступила в редакцию 6 декабря 2021 г.

поступают показатели, характеризующие гражданина, а выходом является решение с конкретным сроком ограничения.

Формализация указанных показателей затруднена тем, что их значениями являются не числа, а слова (предложения) на естественном языке (особенность ознакомления со сведениями, составляющими государственную тайну; личностные качества гражданина; объем и важность сведений, известных гражданину, и т. д.), что обуславливает их лингвистическую неопределенность [5]. Математическим аппаратом, обеспечивающим адекватное описание и формализацию такого рода показателей, является теория нечетких множеств, позволяющая задавать данные показатели с помощью лингвистических переменных [6].

Для формализованного описания процесса принятия решения об ограничении прав граждан на выезд за границу РФ на основании теории нечетких множеств рассмотрим показатели, влияющие на определение срока ограничения, как множество входных лингвистических переменных x_i, принимающих значения a_{i,p_i}, а срок ограничения y — как выходную лингвистическую переменную, принимающую значения d_j [7]:

$X = \{x_1, x_2, ..., x_{17}\}$ — множество входных лингвистических переменных x_i, количество которых определено требованиями руководящих документов ($i = \overline{1,17}$);

$A_i = \{a_{i,1}, a_{i,2}, ..., a_{i,l_i}\}$ — множество лингвистических значений (термов) входной переменной x_i; l_i — количество значений i-й переменной;

a_{i,p_i} — лингвистический терм входной переменной x_i ($p = \overline{1,l_i}$);

y — выходная лингвистическая переменная, значения которой определяют конкретный срок ограничения;

$D = \{d_1, d_2, ..., d_m\}$ — множество лингвистических значений (термов) выходной переменной y;

d_j — лингвистический терм выходной переменной y ($j = \overline{1,m}$).

Задача принятия решения состоит в том, чтобы на основе информации о значениях оцениваемых показателей, характеризующих конкретного гражданина, определить срок ограничения его прав на выезд из Российской Федерации, т. е. установить зависимости между ними (рис. 1) [8].

Определить данные зависимости можно, используя знания и опыт экспертов, понимание которыми причинно-следственных связей процесса определения срока ограничения позволяет сформировать совокупность правил на основе условий ЕСЛИ, ТО.

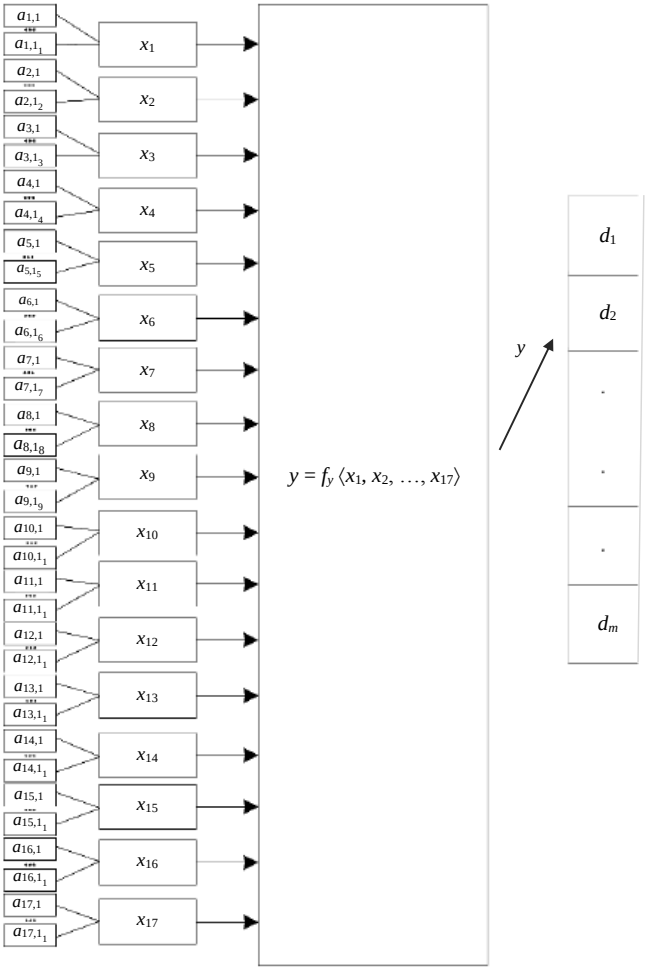


Рис. 1. Модель принятия решения по определению срока временного ограничения на выезд граждан за пределы Российской Федерации

Множество систематизированных правил в совокупности представляет модель предметной области и составляет основу базы знаний, на которой строится система нечеткого логического вывода. Для описания процесса принятия решения о временном ограничении целесообразно применять нечетко-продукционные правила, которые позволят использовать разнотипные входные и выходные параметры правил, обрабатывать четкие и нечеткие входные данные [9].

Большое число показателей x_i делает затруднительным практическое построение нечеткой базы знаний о зависимостях. Для устранения избыточности используется метод построения иерархической базы знаний, подразумевающий классификацию входных переменных и построение дерева логического вывода, определяющего систему вложенных друг в друга высказываний-знаний меньшей размерности [10] (рис. 2).

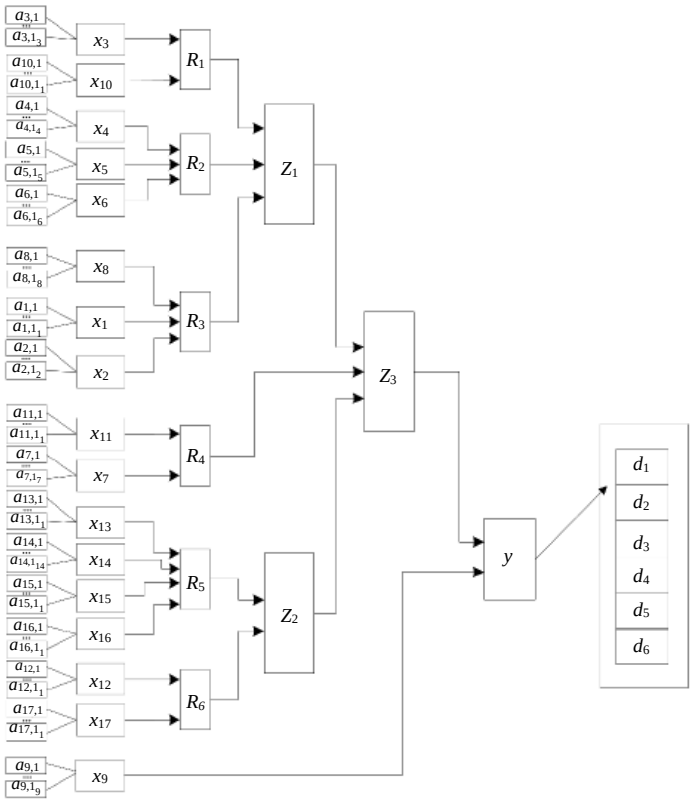


Рис. 2. Дерево логического вывода

Знания вида $y = y(x_1, x_2, \ldots, x_{17})$, связывающие входы x_1—x_{17} с выходом y, заменяются последовательностью постановок:

$$y = f_y(Z_3, x_9); \quad (1)$$

$$Z_3 = f_{Z_3}(Z_1, Z_2, R_4); \quad (2)$$

$$Z_1 = f_{Z_1}(R_1, R_2, R_3); \quad (3)$$

$$Z_2 = f_{Z_2}(R_5, R_6); \quad (4)$$

$$R_1 = f_{R_1}(x_1, x_{10}); \quad (5)$$

$$R_2 = f_{R_2}(x_4, x_5, x_6); \quad (6)$$

$$R_3 = f_{R_3}(x_1, x_2, x_8); \quad (7)$$

$$R_4 = f_{R_4}(x_7, x_{11}); \quad (8)$$

$$R_5 = f_{R_5}(x_{13}, x_{14}, x_{15}, x_{16}); \quad (9)$$

$$R_6 = f_{R_6}(x_{12}, x_{17}), \quad (10)$$

где x_1—x_{17} — входные переменные;
Z_1—Z_3 — классы входных переменных;
R_1—R_6 — подклассы входных переменных;
y — выходная переменная (интегральный показатель).

Методом экспертного опроса установлено, что оптимальным количеством возможных сроков ограничений являются 1, 2, 3, 4 и 5 лет, т. е. $m = 6$. При необходимости точность определения срока ограничения можно повысить (до полугода, месяца).

Все переменные, стоящие в вершинах дерева (рис. 2), являются лингвистическими переменными со следующими термами: $\{a_{i,1}, a_{i,2}, ..., a_{i,l_i}\}$ — множество термов для оценки переменной x_i; $\{d_1, d_2, ..., d_6\}$ — множество термов для оценки переменной y; $\{Z_{1,1}, Z_{1,2}, ..., Z_{1,b_1}\}$ — множество термов для оценки переменной Z_1; $\{Z_{2,1}, Z_{2,2}, ..., Z_{2,b_2}\}$ — множество термов для оценки переменной Z_2; $\{Z_{3,1}, Z_{3,2}, ..., Z_{3,b_3}\}$ — множество термов для оценки переменной Z_3; $\{R_{1,1}, R_{1,2}, ..., R_{1,c_1}\}$ — множество термов для оценки переменной R_1; $\{R_{2,1}, R_{2,2}, ..., R_{2,c_2}\}$ — множество термов для оценки переменной R_2; $\{R_{3,1}, R_{3,2}, ..., R_{3,c_3}\}$ — множество термов для оценки переменной R_3; $\{R_{4,1}, R_{4,2}, ..., R_{4,c_4}\}$ — множество термов для оценки переменной R_4; $\{R_{5,1}, R_{5,2}, ..., R_{5,c_5}\}$ — множество термов для оценки переменной R_5; $\{R_{6,1}, R_{6,2}, ..., R_{6,c_6}\}$ — множество термов для оценки переменной R_6.

Введенные множества термов обозначены на соответствующих ветвях дерева. Для оценки значений лингвистических переменных Z_1—Z_3, R_1—R_6 используется единая шкала качественных термов: О — срок ограничения отсутствует, Н — низкий, НС — ниже среднего, С — средний, ВС — выше среднего, В — высокий.

На основе введенных термов и экспертных знаний соотношения (1)—(10) представляются в виде таблиц. В приведенной таблице представлен фрагмент знаний о соотношении $y = f_y(Z_3, x_9)$.

Фрагмент знаний о соотношении y $f_y(Z_3, x_9)$

№	Z_3	x_9	y
1	О	О	d_1
2	Н	О	
3	НС	О	
4	С	О	
5	ВС	О	
6	В	О	
7	О	Н	d_2
8	Н	Н	
9	Н	НС	
10	Н	С	
11	Н	ВС	
12	НС	Н	
…	…	…	…
32	О	В	d_6
33	ВС	В	
34	В	С	
35	В	ВС	
36	В	В	

Общая база знаний для дерева логического вывода (рис. 2) содержит 408 экспертных высказываний.

На основе полученных знаний, заданных таблично, а также операций (И) и (ИЛИ) составляется система нечетких логических уравнений [11].

В качестве примера приведен фрагмент системы нечетких логических уравнений для знаний о зависимости $y = f_y(Z_3, x_9)$:

$$
\begin{aligned}
\mu^{d_1}(y) \;=\; & \left[\mu^{\text{О}}(Z_3)\mu^{\text{О}}(x_9)\right] \vee \left[\mu^{\text{Н}}(Z_3)\mu^{\text{О}}(x_9)\right] \vee \\
& \vee \left[\mu^{\text{НС}}(Z_3)\mu^{\text{О}}(x_9)\right] \vee \left[\mu^{\text{С}}(Z_3)\mu^{\text{О}}(x_9)\right] \vee \\
& \vee \left[\mu^{\text{ВС}}(Z_3)\mu^{\text{О}}(x_9)\right] \vee \left[\mu^{\text{В}}(Z_3)\mu^{\text{О}}(x_9)\right]; \\
\mu^{d_2}(y) \;=\; & \left[\mu^{\text{О}}(Z_3)\mu^{\text{Н}}(x_9)\right] \vee \left[\mu^{\text{Н}}(Z_3)\mu^{\text{Н}}(x_9)\right] \vee \\
& \vee \left[\mu^{\text{Н}}(Z_3)\mu^{\text{НС}}(x_9)\right] \vee \left[\mu^{\text{Н}}(Z_3)\mu^{\text{С}}(x_9)\right] \vee \\
& \vee \left[\mu^{\text{Н}}(Z_3)\mu^{\text{ВС}}(x_9)\right] \vee \left[\mu^{\text{НС}}(Z_3)\mu^{\text{Н}}(x_9)\right]; \\
\ldots \quad & \ldots \qquad\qquad \ldots \\
\mu^{d_6}(y) \;=\; & \left[\mu^{\text{О}}(Z_3)\mu^{\text{В}}(x_9)\right] \vee \left[\mu^{\text{ВС}}(Z_3)\mu^{\text{В}}(x_9)\right] \vee \\
& \vee \left[\mu^{\text{В}}(Z_3)\mu^{\text{ВС}}(x_9)\right] \vee \left[\mu^{\text{В}}(Z_3)\mu^{\text{ВС}}(x_9)\right] \vee \\
& \left[\mu^{\text{В}}(Z_3)\mu^{\text{В}}(x_9)\right].
\end{aligned}
\qquad (11)
$$

Данная система уравнений, представляющая собой нечеткую базу знаний, определяет связь между функциями принадлежности $\mu^{a_{i,p_i}}(x_i)$ входных переменных x_i и функцией принадлежности $\mu^{d_j}(y)$, $(j = \overline{1,6})$ выходной переменной y [12].

Определение конкретных лингвистических термов входных и выходных переменных, а также соответствующих им значений функций принадлежности, описывающих показатели, учитываемые при принятии решений об ограничении прав граждан на выезд из Российской Федерации, осуществляется методом экспертных оценок.

В этих целях формируют экспертную группу из специалистов по защите государственной тайны, рекомендованной численностью $10 \le K \le 30$ человек [13], что соответствует рекомендованному количественному составу экспертной группы [14], где K — количество экспертов в рабочей группе. Компетентность экспертной группы и ее способность корректно решить поставленную задачу должны подтверждаться попаданием уровня компетентности в установленный диапазон $0{,}67 \le M \le 1{,}0$, где M — уровень компетентности экспертной группы. При этом оценивание компетентности рабочей группы экспертов вычисляется по формуле [15]:

$$M = \frac{1}{m_{\text{эк}}} \sum_{j=1}^{m} K_j, \qquad (12)$$

где K_j — уровень компетентности j-го эксперта;

$m_{\text{эк}}$ — количество экспертов в группе.

Оценка уровня компетентности K_j каждого j-го эксперта ($j = \overline{1, m_{\text{эк}}}$) складывается из уровня его профессиональной подготовленности, знаний требований нормативно-правовых актов по порядку подготовки решения о возможности выезда граждан за пределы Российской Федерации, практического опыта по подготовке решений, а также учета органа военного управления, в котором эксперт проходил службу, и осуществляется по формуле

$$K_j = \frac{1}{2} \sum_{i=1}^{2} K_{ij}, \qquad (13)$$

где K_{ij} — комплексный показатель эксперта, учитываемый при оценке уровня компетентности j-го эксперта ($0 \le K_{ij} \le 1$);

K_{1j} — коэффициент, учитывающий практический опыт работы эксперта в данной области;

K_{2j} — коэффициент, учитывающий уровень органа военного управления, в котором работает эксперт.

Если уровень компетентности рабочей группы экспертов соответствует поставленному условию, она признается работоспособной и приступает к выполнению своих обязанностей.

В методике использован метод построения модифицированных нечетких термов на основе тра-

пециевидных функций принадлежности, выбор которых обусловлен тем, что верхнее основание трапеции позволяет выразить уверенность эксперта в правильности своей классификации, а нижнее — уверенность в том, что никакие другие значения интервала не попадают в выбранное нечеткое множество. Нечеткие подмножества рассматриваются как трапециевидные нечеткие числа, для чего семантические правила заданы графически с использованием функций принадлежности термов множеству значений [16]:

$$f_{\mathrm{T}}(x;a,b,c,d)=\begin{cases}0, & x\le a;\\ \dfrac{x-a}{b-a}, & a\le x\le b;\\ 1, & b\le x\le c;\\ \dfrac{d-x}{d-c}, & c\le x\le d;\\ 0, & d\le x.\end{cases} \qquad (14)$$

Экспертный опрос проводится методом независимых характеристик с соблюдением принципов проведения экспертных опросов, что позволяет получить обобщенную оценку значений функций принадлежности лингвистических переменных. Для этого каждый эксперт заполняет таблицу, в которой указывает свое мнение о параметрах (a,b,c,d) трапециевидных функций принадлежности заданных лингвистических термов. Результаты экспертного опроса обрабатываются методами математической статистики.

Для определения адекватности полученных данных вычисляется согласованность экспертной информации с использованием коэффициента вариации мнений по каждому *i*-у параметру [17]:

$$V_i=\frac{\sigma_i}{\overline{x_{\text{эк}}}}\cdot 100\ \%, \qquad (15)$$

где $\sigma_i=\sqrt{\dfrac{\sum\limits_{j=1}^{m_{\text{эк}}}(x_{j\text{эк}}-\overline{x_{\text{эк}}})}{m_{\text{эк}}-1}}$ — среднеквадратическое отклонение по каждому *i*-у параметру;

$\overline{x_{\text{эк}}}=\dfrac{\sum\limits_{j=1}^{m_{\text{эк}}}x_j}{m_{\text{эк}}}$ — среднее арифметическое;

x_j — оценка *j*-го эксперта $(j=\overline{1,m_{\text{эк}}})$;

$m_{\text{эк}}$ — количество экспертов в рабочей группе.

Степень согласованности всей экспертной информации определяется путем вычисления усредненного коэффициента вариации по всем значениям экспертных данных:

$$V_{\text{сред}}=\frac{\sum\limits_{i=1}^{n}V_i}{n}, \qquad (16)$$

где n — количество оцениваемых параметров.

Результаты экспертного опроса признаются корректными при значениях $V_{\text{сред}}<25\,\%$, что говорит о высокой степени согласованности мнений экспертов.

Сформированная полная база знаний, а также рассчитанное множество функций принадлежности позволяют реализовать нечёткий логический вывод по алгоритму Мамдами [18].

Описанная методика определения срока ограничения прав граждан на выезд за пределы Российской Федерации реализована с использованием графических средств редактирования и визуализации специального пакета расширения Fuzzy Logic Toolbox в среде MATLAB. Адекватность разработанной методики проверена на основе результатов моделирования и анализа характеристик поверхностей откликов соответствующих баз правил, имеющих форму, представленную на рис. 3.

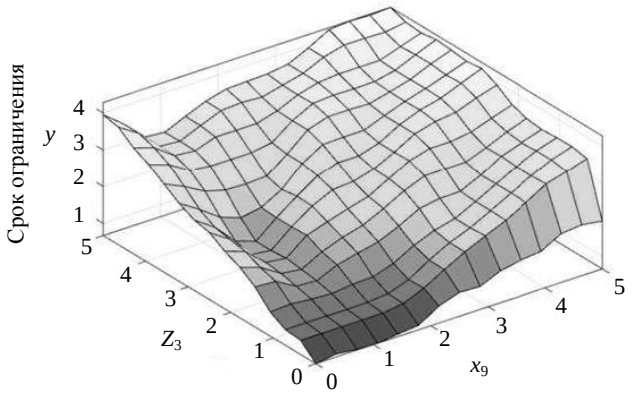


Рис. 3. Зависимость срока ограничения y от интегрального показателя Z_3 и показателя, обратного времени, прошедшего со дня последнего ознакомления x_9

Заключение

Приведена методика определения срока временного ограничения прав граждан на выезд из Российской Федерации на основе математического аппарата теории нечетких множеств, нечеткой логики и экспертных оценок. Проведено формализованное описание предметной области, введены лингвистические переменные, определены базовые терм-множества, методом экспертного опроса

построены соответствующие функции принадлежности. На основе разработанной базы знаний создана система нечеткого логического вывода, способная определять обоснованный срок ограничения прав граждан на выезд за пределы Российской Федерации. Процесс дефаззификации реализован с использованием графических средств редактирования и визуализации специального пакета расширения Fuzzy Logic Toolbox в среде MATLAB.

Предложенная методика позволяет повысить обоснованность и оперативность принимаемых решений по ограничению прав граждан на выезд за пределы Российской Федерации и тем самым исключить нарушения конституционных прав граждан, а также нарушения сроков их представления в установленных случаях.

Методика может быть использована должностными лицами, на которых возложена обязанность по подготовке (принятию) соответствующих решений, а также для подготовки специалистов в данной области в ходе учебного процесса.

Литература

1. О государственной тайне: закон Российской Федерации от 21.07.1993 № 5485-1 // Российская газета. 1993. 21 сент. С. 1, 2.
2. Конституция Российской Федерации [Электронный ресурс]. Режим доступа: https://rg.ru/2020/07/04/ konstituciya-site-dok.html
3. Постановление Конституционного Суда РФ от 07.06.2012 № 14-П по делу о проверке конституционности положений подпункта 1 статьи 15 Федерального закона "О порядке выезда из Российской Федерации и въезда в Российскую Федерацию" и статьи 24 Закона Российской Федерации "О государственной тайне".
4. *Miller G. A.* The Magic Number Seven Plus or Minus Two: Some Limits on Our Capacity for Processing Information // Psychological Review. 1956. № 63. P. 81—97.
5. *Лотов А. В., Поспелова И. И.* Многокритериальные задачи принятия решений: учеб. пособие. — М.: МАКС Пресс, 2008. — 197 с.
6. *Ларичев О. И.* Теория и методы принятия решений, а также Хроника событий в Волшебных Странах: учебник. — М.: Логос, 2000. — 296 с.
7. *Конышева Л. К., Назаров Д. М.* К65 Основы теории нечетких множеств: учеб. пособие. — СПб.: Питер, 2011. — 192 с.
8. *Алтунин А. Е., Семухин М. В.* Модели и алгоритмы принятия решений в нечетких условиях. — Тюмень: Изд-во Тюменского государственного университета, 2000. — 352 с.
9. *Леонков А. В.* Нечеткое моделирование в среде MATLAB и fuzzyTECH. — СПб.: БХВ-Петербург, 2003. — 736 с.
10. *Ротштейн А. П.* Интеллектуальные технологии идентификации: нечеткая логика, генетические алгоритмы, нейронные сети. — Винница: УНИВЕРСУМ-Винница, 1999. — 320 с.
11. *Ротштейн А. П.* Медицинская диагностика на нечеткой логике. — Винница: Континент-Прим., 1996. — 132 с.
12. *Катасёв А. С.* Математическое и программное обеспечение формирований баз знаний мягких экспертных систем диагностики состояния сложных объектов. — Казань: ГБУ "Республиканский центр мониторинга качества образования", 2013. — 200 с.
13. *Крымский С. Б., Жилин Б. Б., Паниотто В. И. и др.* Экспертные оценки в социологических исследованиях. — Киев: Наукова думка, 1990. — 320 с.
14. *Афоничкин А. И., Михаленко Д. Г.* Управленческие решения в экономических системах. — СПб.: Питер, 2009. 480 с.
15. *Лукичева Л. И., Егорычев Д. Н.* Управленческие решения. — М.: Омега-Л, 2009. — 383 с.
16. *Чернышев Ю. О., Требухин А. В., Панасенко П. А., Белоножко Д. Г.* Существующие способы формализации нечеткостей в транспортных процессах // Инженерный вестник Дона. 2021. № 7.
17. *Подольская М. Н.* Квалиметрия и управление качеством: лабораторный практикум. Ч. 1. Экспертные методы. — Тамбов: Изд-во ФГБОУ ВПО "ТГТУ", 2011. — 80 с.
18. *Пегат А.* Нечеткое моделирование и управление. Изд. 3. Пер. с англ. — Электрон. текстовые дан. (1 файл pdf : 801 с.).

Methodology for determining the term of temporary restriction of citizens ' rights to leave the Russian Federation based on fuzzy modeling

I. D. Korolev, V. V. Gubarev, M. F. Kovnatsky

Krasnodar Higher Military School named after Army General S. M. Shtemenko, Krasnodar, Russia

The article discusses the methodology developed by the authors for determining the time limit of citizens' rights to leave the Russian Federation based on the mathematical apparatus of the theory of fuzzy sets, fuzzy logic and expert assessments.

Keywords: citizens, restriction decisions, indicators, linguistic variables, fuzzy sets, membership functions, expert survey.

Bibliography — 18 references. *Received December 6, 2021*

УДК 004.056:316.613
DOI: 10.52190/2073-2600_2022_1_49

Смарт-контракты и их реализация в условиях угроз социальной инженерии

А. А. Кривоногов; *К. В. Пителинский*, канд. техн. наук; *Н. В. Федоров*, канд. техн. наук; *Т. В. Щипунов*
ФГАОУ ВО «Московский политехнический университет», Москва, Россия

Рассмотрены ключевые особенности технологии блокчейн и смарт-контрактов. Проведен сравнительный анализ преимуществ и недостатков смарт-контрактов. Обсуждены принципы и методы социальной инженерии, оказывающие деструктивное воздействие на смарт-контракты.

Ключевые слова: блокчейн, уязвимость, человеческий фактор, информационная безопасность, экономическая безопасность, утечка данных, кибератака, злоумышленник.

Глубокое проникновение информационных и инновационных технологий в ткань социально-экономических отношений дало импульс развитию множества инновационных технологий, которые стремительно интегрируются между собой. Одним из приоритетных векторов развития любого государства является процесс цифровизации всех его экономических институтов. Финансово-технологический сектор экономики Российской Федерации затронули существенные изменения, обусловленные упомянутым процессом. Изменения, идущие в рамках деятельности предприятий и организаций, относятся к массовому выходу социума на принципиально иную ступень автоматизации его логистических и производственных систем.

Современные предприятия и организации должны быть нацелены на развитие при наличии турбулентных факторов внешней среды (например, разрывов логистических цепей из-за эпидемии COVID-19), а также быть адаптивными и гибкими к действию всех неблагоприятных изменений и потенциальных внутренних и внешних рисков. Поэтому для уверенного и уместного использования новых методов и средств цифровизации (например, смарт-контрактов) требуется подробное и всестороннее изучение специфики формализации и интеграции онтологических понятий цифровых технологий в финансово-технологический сектор РФ (например, такой категории, как цифровизация промышленных предприятий).

К сожалению, униформное и строгое определение сути данной категории пока невозможно из-за отсутствия сонаправленного вектора взглядов на него среди современных ученых, анализирующих процессы формирования цифровой экономики, и многообразия теоретико-методологических подходов к этому явлению. Некоторые подходы к определению онтологии понятия цифровизации промышленных предприятий представлены в табл. 1.

В последние годы смарт-контракты приобрели большую популярность за счет их внедрения в блокчейн-проекты для осуществления успешной цифровизации промышленных предприятий и организаций финансового сектора экономики.

Смарт-контракт — компьютерный алгоритм, который позволяет отслеживать и гарантировать соблюдение договорных обязательств между сторонами информационного обмена. В рамках того или иного бизнес-процесса стороны обсуждают и устанавливают условия выполнения смарт-контракта, подкрепляя свое согласие электронной подписью.

По технологии блокчейна, обеспечивающей подконтрольность изменений и неизменность информации, выполняются транзакции по смарт-контракту. В рамках реализации смарт-контракта проверяется соответствие заданным требованиям. Лишь если все условия транзакции соблюдены, сделка считается завершенной. При возникновении какой-либо ошибки или несоблюдения одним из участников условий сделки смарт-контракт аннулируется.

Кривоногов Антон Алексеевич, аспирант кафедры "Информационная безопасность".
E-mail: aakrivonogov97@yandex.ru
Пителинский Кирилл Владимирович, доцент, MBA, доцент кафедры "Информационная безопасность".
E-mail: yekadath@gmail.com
Федоров Николай Владимирович, доцент, заведующий кафедрой "Информационная безопасность".
E-mail: fedorovnv31@mail.ru
Щипунов Тимофей Викторович, студент кафедры "Информационная безопасность".
E-mail: timothey.shchipunov@mail.ru

Статья поступила в редакцию 26 января 2022 г.

Таблица 1

Вариативность категории "цифровизация промышленных предприятий" [1]

Авторы трактовки	Сущность категории
Бушмелева Г., Солодянкина О., Батов А.	Цифровизация промышленных предприятий — адаптируемый инструментарий трансформации системы управления промышленным предприятием, основанный на цифровых технологиях (оцифровка данных), реализованных в инновационной инфраструктуре [2]
Карина Ж. П.	Цифровизация промышленных предприятий может быть охарактеризована как внедрение и широкое использование цифровых систем передачи информации, управления, моделирования и прогнозирования, а также автоматизации производственного процесса путем использования высокотехнологичного оборудования [3]
Ламентова А. Ю.	Цифровизация промышленности (четвертая индустриальная революция) — процесс, который будет способствовать росту показателей производительности, высокой скорости выпуска новой продукции, улучшению качества проектирования и изготовления, снижению себестоимости продукции [4]
Ярошевич Н. Ю.	Цифровизация промышленных предприятий — процесс, который находит свое проявление в таких сферах, как использование базовых программных средств (программные продукты для решения организационно-управленческих задач, справочные системы, средства обеспечения информационной безопасности), специальных программ для научных разработок, сложных комплексных систем управления процессами экономической деятельности (CRM-, ERP-, SCM-системы) [5]

В смарт-контракте может быть столько условий, сколько необходимо, чтобы участники сделки были уверены в том, что она будет однозначно выполнена. Чтобы установить условия, участники сначала должны определить, как транзакции и относящиеся к ним данные представлены в блокчейне, затем согласовать правила выполнения обязательств, которые управляют этими транзакциями, а потом исследовать любые возможные исключения и задать механизм разрешения спора [6].

Пример смарт-контракта, осуществляющего перевод денежных средств, показан на рис. 1.

Для осуществления схожих бизнес-процессов при использовании смарт-контракта в целях обеспечения эффективной деятельности предприятия/организации необходимо кратко определить порядок его работы, а именно:

- инициирование транзакции, в рамках которой осуществляется передача информации (в том числе цифровых активов) в одноранговую компьютерную сеть;
- подтверждение статуса пользователя и транзакции в одноранговой компьютерной сети;
- объединение текущей транзакции с другими транзакциями для образования нового блока и его включения в блокчейн-сеть.

Схематичное описание работы смарт-контракта приведено на рис. 2.

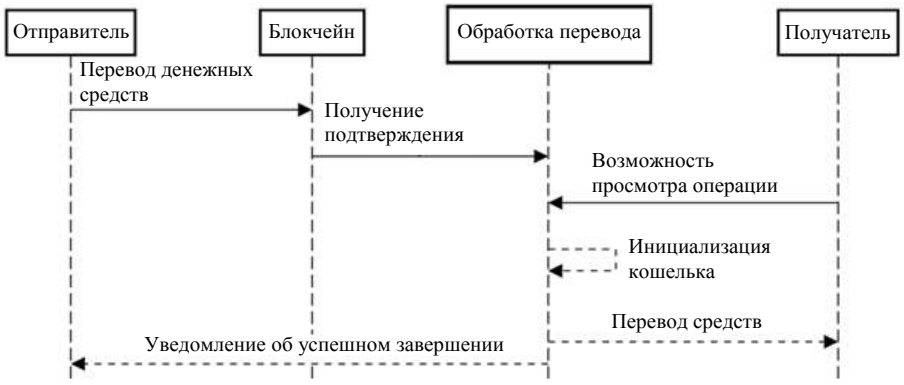


Рис. 1. Пример смарт-контракта, осуществляющего перевод денежных средств

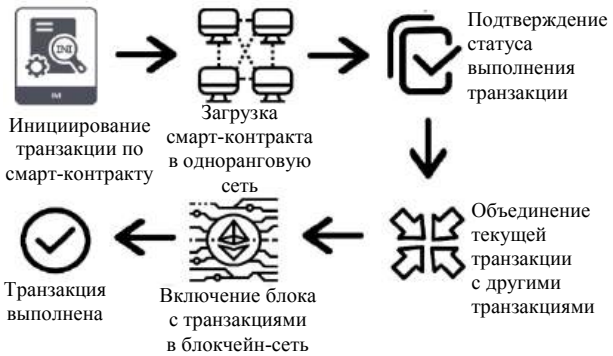


Рис. 2. Принципы работы смарт-контракта

Технология блокчейн устраняет дополнительных посредников, что значительно упрощает реализацию бизнес-процессов. Например, в централизованной сети средства управления используются только одним субъектом и все ее компоненты располагаются в одном конкретном месте. В распределенной информационно-вычислительной сети нет единого регулирующего органа и элементы управления распределены между несколькими независимыми подразделениями, которые сосредоточены в разных местах, что обеспечивает отказоустойчивость в работе. Это становится особенно актуальным в условиях массовых ограничений на социально-экономическую деятельность, обусловленных влиянием короновирусной эпидемии.

Смарт-контракты должны учитывать требования рукописного договора, позволяя понизить роль негативного человеческого фактора (упущений и ошибок). Это снимает и проблему привлечения посредников (нотариусов и иных доверенных третьих лиц) при исполнении соглашений. Кроме того, с использованием смарт-контракта сократится значительная доля мошеннических операций [6].

Смарт-контракт доступен для просмотра всем участникам в блокчейне, однако это приводит к ситуации, когда уязвимости и ошибки безопасности также становятся видны всем, но при этом они не могут быть оперативно исправлены [7]. Например, одной из громких кибератак является атака на кошелек с мультиподписями Parity [8], в ходе которой было похищено порядка 30 млн долл. Основные причины возникновения ошибок в смарт-контрактах представлены в табл. 2.

Однако смарт-контракты могут обеспечить приемлемую политику безопасности компании/организации, постоянное совершенствование методов и технологий обеспечения экономической и информационной безопасности (ЭИБ).

Перед развертыванием системы безопасности необходимо понять суть безопасности субъектов экономики. Здесь для каждой компании/организации и каждого отдельного случая риск безопасности в ЭИБ задается характеристиками осуществляющей бизнес-деятельность организационной структуры [9]. Оценивая риск, важно качественно и количественно выявить факторы, действующие на эффективную деятельность предприятия/организации (рис. 3).

Таблица 2

Основные причины возникновения ошибок в смарт-контрактах

Причина возникновения ошибки	Описание
Ошибка в конструкциях	Использование простых и логичных конструкций, не закрепленных в официальных спецификациях
Ошибка компилятора	Ошибки, возникающие как при компиляции фрагмента исходного кода смарт-контракта, так и при работе самого компилятора
Ошибка виртуальной машины Ethereum	Возникновение ошибок и ложноположительных исключений в виртуальной машине Ethereum в процессе выполнения байт-кода смарт-контракта
Уязвимость и атака на смарт-контракт	Деструктивные воздействия злоумышленников на слабые конструкции смарт-контракта в целях вызова методов злонамеренного смарт-контракта или вывода цифровых активов
Слабая документация	Недостаточное количество документации по разработке смарт-контракта из официальных источников
Атака на участников блокчейн-сети	Атаки, направленные на участников блокчейн-сети, закрепленных в смарт-контракте, или закрытие криптовалютных проектов (OneCoin, Bitconnect, PlusToken и т. д.)

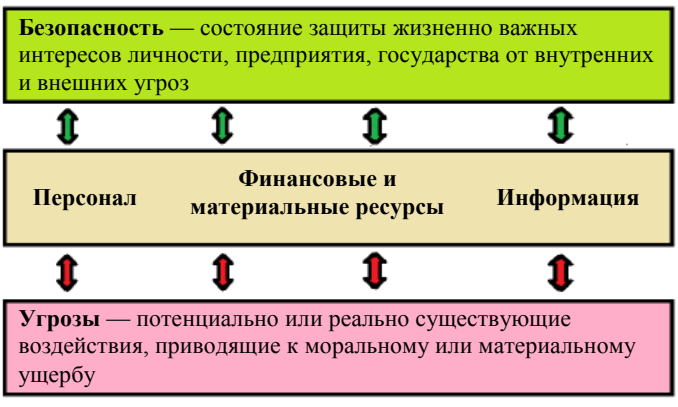


Рис. 3. Факторы, влияющие на эффективную деятельность предприятия [9]

Существующий закон РФ "О цифровых финансовых активах" (ЦФА) позволяет банкам выпускать свои ЦФА, обменивать их на другие подобные активы. При этом граждане страны смогут покупать цифровые активы, выпущенные за пределами юрисдикции РФ, на зарубежных площадках.

Блокчейн-технология может позволить любому разработчику активировать ЦФА в своих программных решениях с помощью смарт-контрактов. Такая открытая экосистема информационно-финансовых технологий дает новые импульсы к развитию рынка, а законодательные нормы упрощают процедуру выпуска финансовых инструментов. Поэтому перспективным представляется использование смарт-контрактов для ведения сделок как между физическими лицами, так и между компаниями. Все это в комплексе может привести к появлению новых категорий активов и к переносу части существующих проблем в инфраструктуру ЦФА.

На рис. 4 приведено количество блокчейн-проектов и смарт-контрактов, размещенных на Github в период с января 2013 г. по апрель 2018 г. Согласно Dune Analytics [10], число новых смарт-контрактов в сети Ethereum в марте 2020 г. составило почти 2 млн по всему миру. Это на 75 % больше, чем в феврале того же года. Благодаря масштабу технологии и выпуску Ethereum 2.0 (сеть Ethereum 2.0 Topaz) в апреле 2020 г. возросла доступность этой технологии. По исследованию компании Gartner [11] к 2020 г. порядка 14 % корпоративных блокчейн-проектов уже достигло стадии промышленного внедрения смарт-контрактов.

На российском рынке уже давно присутствуют крупные компании, которые активно тестируют (или уже внедрили) смарт-контракты для выполнения типовых промышленных операций. Ими являются Альфа-Банк, Газпром нефть, Россети, Сбер, S7 Airlines, РЖД, Дикси, Первоуральскбанк. При этом такими компаниями, как Яндекс и Сбербанк, были созданы собственные модульные технологические решения для создания и размещения смарт-контрактов в блокчейн-сети.

Для большего понимания особенностей смарт-контракта необходимо провести сравнение с обычным договором (или бумажным контрактом) (табл. 3).

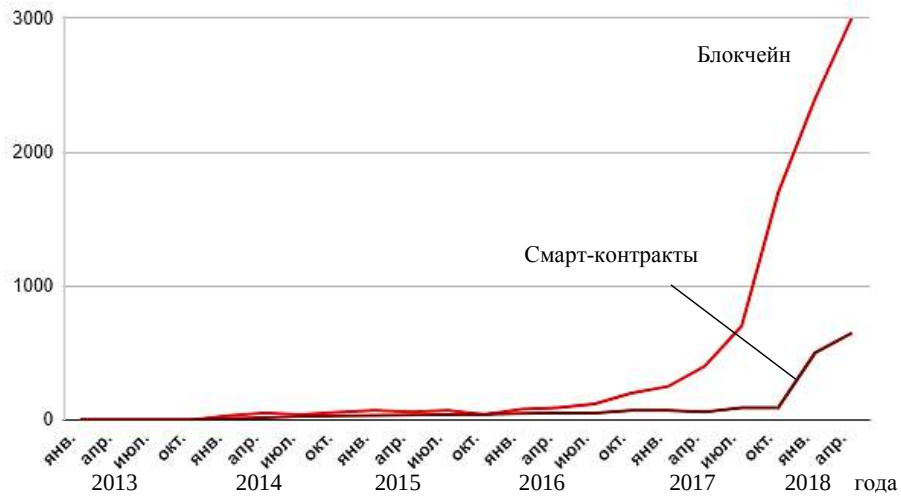


Рис. 4. Количество блокчейн-проектов и смарт-контрактов

Таблица 3

Сопоставление критериев контрактов

Критерии	Смарт-контракт	Обычный контракт
Тип визуализации данных	Машинный носитель	Бумажный носитель
Постоянство условий договорных отношений	Хранение в блокчейне	На основании правил
Язык заключения договорных отношений	Машинный язык	Юридический язык
Риски применения	Безопасно и без посредников	Риск обмана, посредники
Валюта исполнения обязательств по договору	Цифровая валюта	Безналичные и наличные деньги

Смарт-контракт (как и любая технология) имеет свои преимущества и недостатки (табл. 4).

Стоит также указать недостатки данной технологии, из-за которых смарт-контракт не может быть идеальным инструментом взаимодействия между субъектами экономики. Некоторые из них приведены в табл. 5.

Главное преимущество смарт-контрактов заключается в использовании технологии блокчейн, благодаря чему отсутствует возможность обмана (поскольку для его выявления достаточно изучить код программы). Однако пользователь, не владеющий технологиями программирования, не сможет проверить надежность кода. Единственный способ сделать это — обратиться к специалистам. На этом и смогут сыграть злоумышленники, поскольку они могут убедить жертву в полной безопасности предлагаемого смарт-контакта и сделать код его программы неверно исполняемым.

Далее укажем проблемы, тормозящие распространение смарт-контрактов. К оплате на основе смарт-контрактов принимают только криптовалюты на ограниченном числе блокчейн-платформ. Есть платформы для обмена криптовалют на наличные, но сделать это на практике сложно. Кроме того, в РФ криптовалюты не признаны официально, отчего они считаются высокорисковыми. Злоумышленники могут воспользоваться этим, понимая, что рядовой гражданин не всегда имеет криптокошелек, и обманом заключить с ним как с участником смарт-контракта сделку на оказание недобросовестной услуги. Также не стоит забывать о том, что программист может и просто совершить ошибку в коде. Исходя из разных источников от 2 до 3 % от общего числа смарт-контрактов на блокчейн-платформе содержат уязвимости и ошибки в коде. Все перечисленные уязвимости можно связать с влиянием человеческого фактора и с социальной инженерией (СИ).

Человек по-прежнему остается самым слабым звеном в любой системе безопасности, в том числе и в смарт-контрактах. Заставить человека действовать в нужном манипулятору ключе проще, чем взломать цифровые системы и сети. Большинство людей склонно доверять другим людям, чем и пользуются злоумышленники. Социальные инженеры используют различные методы для отправки вредоносного программного обеспечения (ПО), принудительного получения личной информации, получения доступа к защищенным системам и множество иных злонамеренных приемов.

Таблица 4

Преимущества смарт-контрактов

Преимущество	Описание
Резервное копирование	Смарт-контракты хранятся в блокчейне, где они многократно дублируются; следовательно, их оригиналы могут быть в случае потери данных восстановлены
Безопасность	Смарт-контракты защищены от модификации злоумышленником. После согласия на выполнение смарт-контракта ни одна из сторон не может изменить его код
Скорость	Смарт-контракты с помощью компьютерных протоколов автоматизируют операции, сокращая время, необходимое для выполнения бизнес-процессов
Автономия и экономия	Для подтверждения соглашения смарт-контракты не нуждаются в брокерах или иных посредниках, что исключает риск манипуляций со стороны третьих лиц. Отсутствие посредника в смарт-контрактах ведет к экономии затрат
Эргономичность	Использование смарт-контрактов позволяет снизить число ошибок, возникающих при заполнении вручную многочисленных форм, и повысить удобство работы пользователя

Таблица 5

Недостатки смарт-контрактов

Недостаток	Описание
Невозможность изменения	Нельзя изменить процессы смарт-контрактов. Чтобы исправить ошибки в коде, надо потратить много времени и денег. В случае, если в смарт-контракте допущена ошибка и его необходимо изменить, текущий смарт-контракт аннулируется, создается новый смарт-контракт, который заново загружается в блокчейн для исполнения
Третья сторона	Смарт-контракты обычно исключают третьих лиц, но полностью их нельзя исключить. Такой стороной является оракул, который берет на себя другие роли, отличные от традиционных контрактов. Он (чтобы инициировать выполнение кода) завязывает на смарт-контракт те или иные события, но при этом также есть возможность отправки с его стороны ошибочных данных
Нечеткость формулировок	Смарт-контракт — это сложный механизм, в функционировании которого его пользователю сложно быстро разобраться, отчего он может быть выполнен неоднозначно

СИ позволяет получить необходимый доступ к информации, основанный на специфике человеческой психологии. Основная функция СИ — незаметно получить доступ к секретной информации, паролям, банковской информации и другим защищенным системам. Обычно преступники скрываются от ничего не подозревающих пользователей, чтобы раскрыть данные, распространить вредоносное ПО или получить доступ к системам с ограниченным доступом. Именно поэтому была создана такая технология, как смарт-контракт, позволяющая минимизировать влияние человеческого фактора при выполнении критичных операций или транзакций.

Атаки при использовании методов СИ могут происходить как при личном контакте людей, так и в интернет-среде. Согласно статистике Positive Technologies [12] за 2020 г. злоумышленники активно использовали СИ в своих атаках, причем данный метод являлся наиболее популярным среди злоумышленников в отношении частных лиц (рис. 5).

Для защиты сети и серверов предприятия/организации часто развертывают интегрированные системы информационной безопасности для защиты от вредоносного ПО и хакерских атак. Однако в любом случае эти решения не учитывают самое слабое звено — пользователей информационной системы. Поэтому киберпреступники часто используют приемы СИ, чтобы обманным путем обойти существующие системы и протоколы безопасности для достижения своих целей.

Как сообщили в Райффайзенбанке, в 2019 г. более 70 % мошеннических операций в отношении физических лиц было вызвано методами СИ [13]. По статистике в 98 % кибератак используют СИ как основной или побочный способ получения нужной информации [14] (рис. 6).

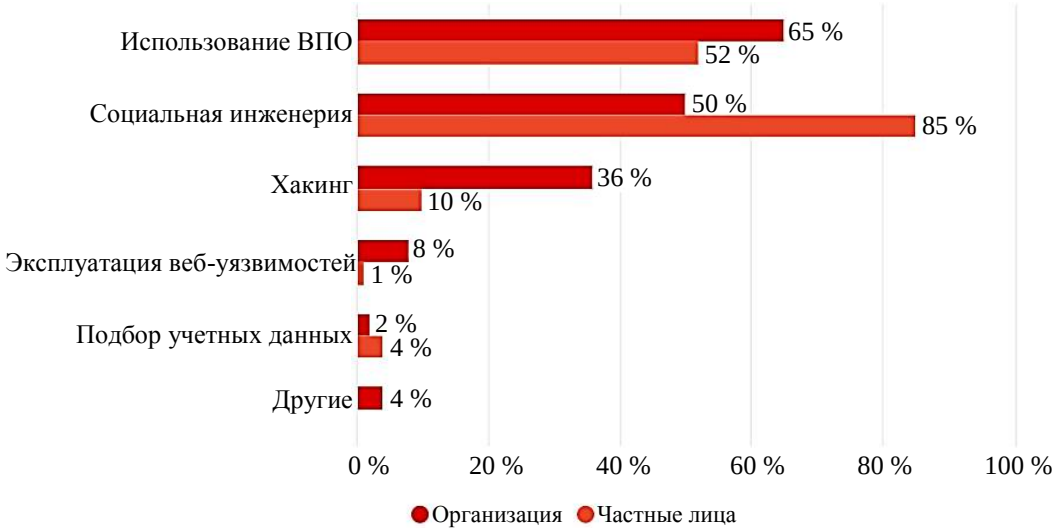


Рис. 5. Статистика киберугроз для организаций и частных лиц

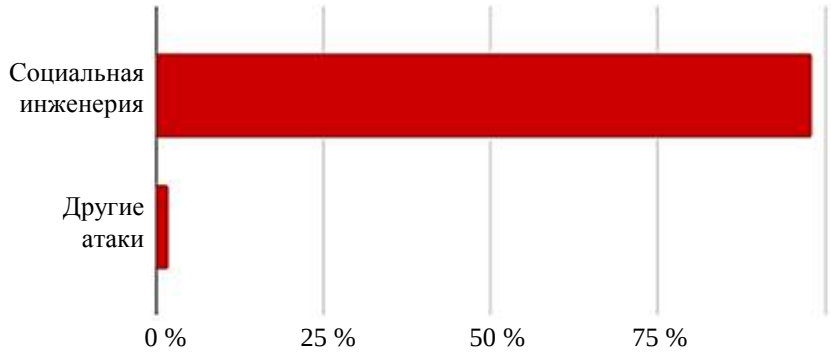


Рис. 6. Соотношение кибератак с помощью СИ

Эксперты в области человеческого поведения указывают на качества и эмоции, которые испытывают многие люди (страх, доверие, жадность). В рассматриваемом случае самой главной причиной СИ является желание идти в ногу со временем без желания понимать все тонкости применения новых сложных технологий. Для обмана социальные инженеры часто используют принципы из табл. 6 [15, 16].

Часто нерациональные или рискованные действия совершаются, когда человек находится в усиленном эмоциональном (аффективном или экзальтированном) состоянии. Чтобы убедить пользователя, манипуляторы используют следующие естественные эмоции: доверие, нетерпеливость, гнев, любопытство и т. д. Обычно киберпреступники совершают типы нарушений при помощи методов СИ, приведенных на рис. 7.

По данным InfoWatch [17], в 2019 г. более 172 млн записей персональных данных и платежной информации в РФ было похищено несмотря на то, что в РФ предусмотрены наказания за разглашение или хищение конфиденциальной информации (ст. 183 УК РФ. "Приготовление к хищению (компьютерной) информации и перехват данных"). Есть и иные статьи и федеральные законы РФ, определяющие уголовную или административную ответственность за нарушение сохранности данных.

Таблица 6

Базовые принципы социальной инженерии

Принципы	Описание
Взаимность	Предпочтение платить добром за добро. Пользователю, который не разбирается в информационных технологиях, могут предложить воспользоваться смарт-контрактом, поскольку это надежно и (в отличие от стандартного договора) является лучшим способом провести сделку. На самом деле этот смарт-контракт будет написан с умышленными ошибками и лазейками для мошенников
Власть и авторитет	Аналогичен принципу симпатии. Люди склонны прислушиваться к авторитетным фигурам, даже если их просят совершить необдуманные или потенциально неблагоприятные для них действия
Дефицит ресурсов	Воспринимаемая нехватка порождает спрос. Например, предложения "С помощью смарт-контрактов мы доставим Вам недорогой и качественный товар с использованием новых информационных технологий" или "Только у нас эксклюзивный товар, спешите, время ограничено" стимулируют масштабность продаж
Симпатия	Человека легко переубедить людям, которые ему импонируют. Например, если какой-нибудь блогер или знаменитость начнет рекламировать технологию смарт-контрактов как простой и надежный способ проведения сделок, то его последователи могут поспешно воспользоваться данной услугой
Социальное доказательство	Многие люди не могут определить свой способ поведения в сложных ситуациях. Полагая, что окружающие лучше владеют ситуацией, эти люди будут делать то, что, по их мнению, делают другие. Это часто успешно используется в технологиях СИ (например, так называемое сарафанное радио)

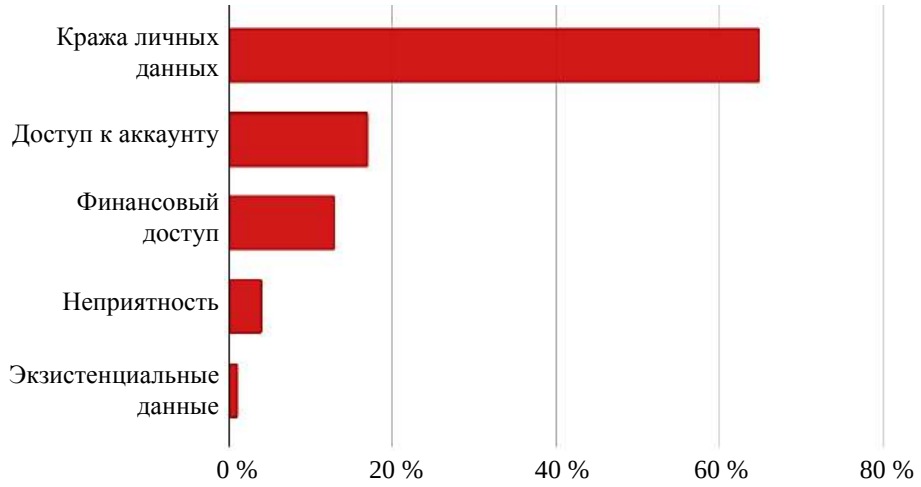


Рис. 7. Типы нарушений при помощи социальной инженерии

Отдельно следует рассмотреть нормативно-правовую базу РФ, касающуюся киберпреступности при использовании методов СИ [18, 19].

- Федеральный закон РФ № 98-ФЗ "О коммерческой тайне", определяющий отношения по созданию, изменению и прекращению коммерческой тайны, связанные с раскрытием фактической или вероятной коммерческой ценности неким другим сторонам.
- Федеральный закон РФ № 152-ФЗ "О персональных данных", который регулирует отношения, связанные с обработкой персональных данных при использовании, в том числе средств автоматизации.
- Глава 28 Уголовного кодекса РФ "Преступления в сфере компьютерной информации", содержащая в том числе следующие статьи:

– Статья 272 "Неправомерный доступ к компьютерной информации";

– Статья 273 "Создание, использование и распространение вредоносных компьютерных программ";

– Статья 274 "Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей";

– Статья 283 "Разглашение государственной тайны", где рассмотрено разглашение информации, составляющей государственную тайну, лицом, которому она доверена или стала известна по работе, учебе или в других случаях, предусмотренных законодательством, если эта информация стала собственностью других лиц".

- Федеральный закон от 12.11.2019 № 375-ФЗ "О внесении изменений в Федеральный закон "Об исполнительном производстве".
- Федеральный закон от 23.11.2020 № 374-ФЗ "О внесении изменений в части первую и вторую Налогового кодекса Российской Федерации и отдельные законодательные акты Российской Федерации".

Последние два из перечисленных законов обязывают хранить телефонные звонки и сообщения всех российских пользователей, а также предоставлять эту информацию спецслужбам.

Предполагается, что онлайн-сервисы должны будут хранить у себя конфиденциальную информацию людей, такую, как адрес почты, данные паспорта, тексты переписок, фамилию, имя, отчество. Исходя из этого нужно понимать, что персональная информация пользователей может попасть в руки злоумышленников, после чего быть использована в атаках против них самих.

Дополнительно необходимо рассмотреть пример возможной реализации атаки на смарт-контракт с двумя участниками и неким посредником (так называемая атака "человек посередине"), причем злоумышленник может украсть данные пользователей еще до совершения смарт-контракта (рис. 8).

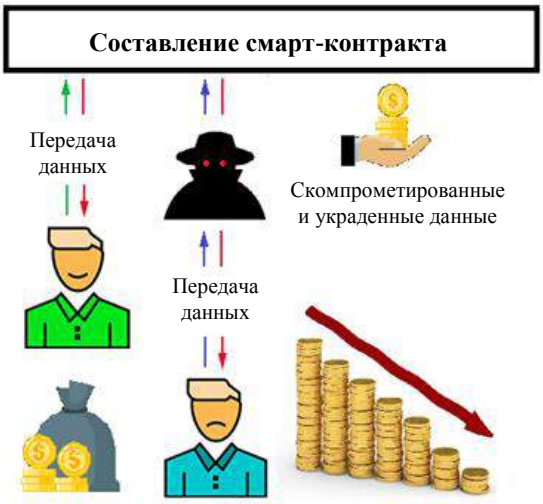


Рис. 8. Хищение данных пользователя злоумышленником

При составлении смарт-контракта одна из сторон может использовать и специальное упущение важных слов или (при обработке персональных данных) указать некие общие слова, которые прямо не соответствуют пониманию реальной цели предоставления данных. Такая расплывчатость — верный признак типичной политики, когда юристы не вникают в суть того, зачем эта политика создавалась. Это означает, что никто не собирается защищать личные данные участника сделки.

Резюмируя, отметим, что влияние злоумышленника на бизнес-процессы и ресурсы атакуемого предприятия/организации (или физического лица) через методы СИ или кибератак может усиливаться (табл. 7).

Поскольку методы СИ предполагают использование многочисленных ошибок и слабостей людей, сложно создать стереотипные и универсальные планы для противодействия и купирования последствий применения СИ [20, 21].

Одним из вариантов решения упомянутых проблем является повышение киберграмотности участников взаимоотношений в рамках смарт-контракта (в том числе путем прохождения курсов повышения квалификации по ЭИБ и по новым информационно-коммуникационным технологиям). Для лиц, не являющихся сотрудниками предприятий/организаций, но желающих использовать для своих целей технологию смарт-контрактов, повышение их осведомленности зависит только от их личной заинтересованности и от помощи окружающих.

Таблица 7

Причины возможных негативных последствий

Возможные причины
Ошибки персонала/потребителя товаров или услуг
Отказ и/или неисправность штатного оборудования или ПО
Неприемлемые и/или неопределенные внешние воздействия
Отсутствие и/или неисправность оборудования для ЭИБ объекта защиты
(Не)намеренные воздействия на материальные, информационные и иные ресурсы
Использование специальных технических средств
Психотропные вещества, оказывающие влияние на возможности и психическое состояние персонала
Воздействие на психофизическое состояние человека (в целях изменения его функционального и биологического потенциала) психотропным и другим оружием
Вредные природные, стихийные или климатические воздействия
Другие факторы

В заключение отметим, что комплексная, эффективная и адекватная ЭИБ предприятия/организации основана на умелом и своевременном применении трех видов обеспечения ЭИБ: программно-математического, организационно-правового и инженерно-технического (причем все эти составляющие синергетически усиливают и дополняют друг друга). Компрометация любой из этих составляющих нарушает ЭИБ смарт-контрактов, поскольку злоумышленники могут использовать их для своих целей.

Блокчейн изначально спроектирован так, чтобы быть безопасным, отчего эта инновационная технология имеет значительные потенциальные преимущества. Однако под действием человеческого фактора в практику применения блокчейна в сфере финансовых технологий могут быть привнесены риски безопасности [22], которые должны надлежащим образом купироваться с использованием службы безопасности предприятия/организации или за счет приращения личных знаний и компетенций лица, совершающего операции со смарт-контрактами.

Литература

1. *Тимохина О. А., Близкий Р. С.* Оценка уровня цифровизации промышленных предприятий как одна из приоритетных задач в системе стратегического менеджмента современной организации // Менеджмент в России и за рубежом. 2020. № 5. С. 48—55.
2. *Бушмелева Г., Солодянкина О., Батов А.* Цифровизация промышленного предприятия: цифровая инфраструктура // Polish J. Science. 2019. № 20–2(20). С. 16—18.
3. *Карина Ж. П.* Цифровизация процессов производства: сб. ст. III Междунар. науч.-исслед. конкурса "Основные принципы, перспективы развития и проблемы внедрения в РФ". — Пенза, 2013. С. 62—64.
4. *Ламентова А. Ю.* Цифровизация промышленности как новая стратегия экономического развития // Синергия наук. 2018. № 25. С. 243—249.
5. *Ярошевич Н. Ю.* Цифровизация промышленности в неоиндустриальном развитии региона: мат. III Междунар. науч.-практ. конф. "Урал — XXI век: макрорегион неоиндустриального и инновационного развития". — Екатеринбург, 2018 С. 196—201.
6. *Кривоногов А. А., Пителинский К. В., Федоров Н. В.* Перспективные платформы смарт-контрактов как новый виток развития глобального рынка цифровых технологий // Информационные технологии в проектировании и производстве. 2021. № 4(184). С. 46—52.
7. *Кривоногов А. А., Репин М. М., Федоров Н. В.* Методика анализа уязвимостей и определения уровня безопасности смарт-контрактов при размещении в системах распределенных реестров // Вопросы кибербезопасности. 2020. № 4(38). С. 56—65.
8. Атака на кошелек с мультиподписью Parity [Электронный ресурс]. Режим доступа: https://www.parity.io/blog/a-postmortem-on-the-parity-multi-sig-library-self-destruct/ (дата обращения: 29.11.2021).
9. *Пителинский К. В., Александрова А. В.* Смарт-контракты: принципы работы, преимущества и перспективы // Оборонный комплекс — научно-техническому прогрессу России. 2020. № 1(145). С. 9—14.
10. Статистика смарт-контрактов Dune Analytics [Электронный ресурс]. URL: https://dune.xyz/queries/329#515 (дата обращения: 13.10.2021).
11. Статистика смарт-контрактов Gartner [Электронный ресурс]. URL: https://blogs.gartner.com/avivah-litan/2021/01/13/3-blockbuster-blockchain-trends-in-2021/ (дата обращения: 13.10.2021).
12. Статистика Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения: 04.12.2021).
13. Тренды мошенничеств с банковскими картами 2019 года [Электронный ресурс]. URL: https://www.kaspersky.ru/about/press-releases/2019_rayffayzenbank-i-laboratoriya-kasperskogo-proanalizirovali-trendy-kartochnogo-froda (дата обращения: 29.11.2021).
14. Статистика социальной инженерии [Электронный ресурс]. URL: https://www.idagent.com/blog/10-important-facts-about-social-engineering/ (дата обращения: 29.11.2021).
15. *Гончаренко Г. Ю., Ермаков И. К., Ермолатий Д. А., Пителинский К. В.* Компьютерная психология или универсальный подход к уязвимостям конфиденциальной информации // Вопросы защиты информации. 2018. № 4. С. 62—67.
16. *Саймон Вильям Л., Митник Кевин.* Искусство обмана. — М.: Компания АйТи, 2004. — 121 с.
17. Статистика InfoWatch [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2019-godu (дата обращения: 29.11.2021).

18. *Родичев Ю.* Нормативная база и стандарты в области информационной безопасности. — СПб.: Питер, 2017. — 254 с.
19. Гражданский кодекс Российской Федерации [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 01.11.2021).
20. Блокчейн (мировой рынок) [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Блокчейн_(мировой_рынок) (дата обращения: 04.10.2021).
21. Блокчейн и смарт-контракты [Электронный ресурс]. URL: https://www.nber.org/system/files/working_papers/w24399/w24399.pdf (дата обращения: 30.09.2021).
22. Компании стремятся к умным договорам [Электронный ресурс]. URL: https://rspectr.com/articles/661/kompanii-stremyatsya-k-umnym-dogovoram (дата обращения: 04.10.2021).

Smart contracts and their execution in the context of social engineering threats

A. A. Krivonogov, K. V. Pitelinskiy, N. V. Fedorov, T. V. Shchipunov
Moscow Polytechnic University, Moscow, Russia

The key features of blockchain technology and smart contracts are revealed. A comparative analysis of the advantages and disadvantages of smart contracts has been carried out. The principles and methods of social engineering that have a destructive effect on smart contracts are discussed.

Keywords: blockchain, vulnerability, human factor, information security, economic security, data leakage, cyberattack, attacker.

Bibliography — 22 references. *Received January 26, 2022*

Правила для авторов по оформлению рукописей статей, предлагаемых к публикации в журналах

Направляя рукопись статьи в редакцию журнала, авторы передают редколлегии и издателю журнала безвозмездное неисключительное право опубликовать ее на русском языке в качестве статьи в печатной и электронной версиях журнала в сети Интернет. При этом за авторами сохраняются их интеллектуальные права на рукопись статьи (в том числе "авторское право"). В связи с этим и с учетом Четвертой части (Раздел VII) Гражданского кодекса РФ авторами должно быть представлено в редакцию письмо в следующей форме:

Лицензионный договор о передаче права на публикацию
(издательский лицензионный договор)

Мы, нижеподписавшиеся, авторы рукописи ……..……., предоставляем редколлегии журнала и журнала и издателю ФГУП «НТЦ оборонного комплекса «Компас» ……..……
(название журнала)
безвозмездную простую (неисключительную) лицензию на публикацию рукописи статьи как в печатной, так и в электронной версиях журнала.

Мы подтверждаем, что данная публикация не нарушает интеллектуальных прав других лиц или организаций.

Подписи авторов: …… (ф.и.о., ученая степень, дата)
……..…….
……...…….

Статья должна быть подписана всеми авторами. В случае нескольких авторов указывается фамилия автора, ответственного за переписку с редакцией. Рукопись статьи направляется на адрес редакции журнала: 125424, Москва, Волоколамское ш., д. 77, ФГУП «НТЦ оборонного комплекса «Компас», Редакция журнала. Дополнительная информация может быть получена в редакции при обращении по телефону: 8 (495) 491-43-17 или по E-mail: izdanie@ntckompas.ru.

Каждая статья рецензируется в соответствии с решением редколлегии журнала. Рецензенты выбираются из числа ученых и специалистов, компетентных в вопросах, рассматриваемых в статье, и имеющих собственные публикации в данном направлении. Решение о порядке публикации статьи принимается редколлегией с учетом мнения рецензентов. В случае разногласий среди членов редколлегии окончательное решение принимает главный редактор. При полном отклонении рукописи статьи от публикации редакция журнала направляет авторам мотивированный отказ. По этому факту редакция не вступает в полемику с авторами.

Комплектование статьи (обзора)

Статья должна быть представлена в редакцию в следующем комплекте:

- сопроводительное письмо, подписанное руководством организации;
- экспертное заключение о возможности опубликования в открытой печати и распространения в Российской Федерации и других государствах. При отсутствии в организации экспертной комиссии вместо экспертного заключения может быть представлено соответствующее заявление на имя главного редактора журнала от имени руководства организации, где работают авторы. В экспертном заключении или заявлении в обязательном порядке должна быть отражена возможность открытой публикации и передачи публикуемых материалов за границу.
- лицензионный договор по приведенному образцу;
- рукопись статьи — объем статьи (без рисунков) не должен превышать 10 страниц формата А4 при 1,5 межстрочных интервалах, а объем статьи обзорного характера — 20 страниц. Рекомендуемая гарнитура — New Times Roman. Размер шрифта — 12;
- Материал статьи представляется в редакцию в печатном виде (на бумажном носителе) и в электронном варианте с текстом в формате Word на электронную почту.

Оформление статьи:

- статья начинается с указания УДК;
- название статьи набирается строчными буквами (кроме начальной прописной) полужирным шрифтом, размер шрифта 14, для остального текста используется простой шрифт размером 12, причем рекомендуемая гарнитура шрифта — Times New Roman;
- после названия — список авторов, инициалы авторов предшествуют их фамилиям;

- далее представляется аннотация статьи (10—15 строк с раскрытием цели работы и её основных результатов);
- далее приводится список ключевых слов для данной статьи (не более десяти);
- страницы текста нумеруются без пропусков и добавлений литерных обозначений (типа 1*а*, 2*б* и т. п.), причем в сквозную нумерацию должны быть включены все элементы статьи;
- внизу первой страницы текста помещается отдельный абзац (с полужирным шрифтом), содержащий контактную информацию об авторе (или авторах) в следующем виде: фамилия, имя, отчество, должность, ученая степень, почтовый адрес предприятия, телефон, E-mail;
- основной текст статьи должен начинаться с четкой постановкой цели и задач работы, сопровождаемой аргументами в пользу ее выполнения на фоне существующего состояния затронутой в статье проблемы. Дальнейший текст статьи также должен иметь смысловые рубрикаторы (разделы и подразделы) без их нумерации. Заканчиваться статья должна отдельным разделом «Заключение» с перечислением основных результатов, следующих из них выводов и, по возможности, предложений по развитию исследований и использованию их результатов.
- после основного текста — список использованных источников "Литература" (не менее 5 источников); Список использованной литературы должен соответствовать всем ссылкам на внешние источники в тексте статьи. Ссылки оформляются в квадратных скобках, например, [1—6], [7, 8]. Внутренние ссылки, т. е. ссылки на формулы, рисунки и таблицы статьи оформляются с использованием круглых скобок, например, формула (1), уравнение (4), (рис. 3), (табл. 2). Любые ссылки в подписях к рисункам и в самих рисунках не рекомендуются;
- далее размещается подробная англоязычная информация о статье: название статьи, фамилия и инициалы авторов (английская транслитерация), предприятие, аннотация, ключевые слова (Keywords).

Оформление рисунков:

- рисунки и графики вставляются непосредственно в нужном месте в статье и в желаемом масштабе.
- рядом с осями графиков указываются отображаемые физические величины только в символьной (буквенной) форме, а через запятую — размерность величины по-русски (прямым шрифтом). Различные кривые на графиках рекомендуется нумеровать, даже если они характеризуются отдельным цветом или типом линии. Графики представляются только на белом фоне. Вспомогательные сетки на площади графика не допускаются;
- подписи под соответствующими рисунками (полужирный курсивный) представляются в нужных местах текста. Каждая подпись должна быть по возможности лаконичной, но емкой по содержанию.

Оформление формул:

- простые формулы вводить в текст в формате используемого текстового редактора, более сложные формулы — с использованием редактора формул MathType;
- стандартные математические обозначения (например, max, log, sin, exp и т. д.) должны быть набраны прямо. То же относится к цифрам и числам;
- для символьного обозначения невекторных физических (технических) величин использовать только латинский и греческий алфавиты, при этом в тексте для греческих букв использовать прямой шрифт, для латинских букв — наклонный шрифт (курсив);
- векторы и матрицы обозначать полужирным прямым шрифтом;
- для нижних и верхних индексов применять арабские цифры, латинские или греческие буквы. Если индекс представляет собой сокращенную форму русского слова — характеристики, то допустимо использовать в его обозначении русские буквы (прямой шрифт), например $U_{вх}$, $I_{вых}$, $\nu_{гр}$ и т. п.
- размерность физических величин обозначается всегда только по-русски прямым шрифтом.

Оформление таблицы:

- содержание таблицы не должно дублировать данные, приводимые на графиках или в тексте;
- графы должны иметь название без сокращения отдельных слов.

Рисунки, формулы и таблицы должны иметь свою отдельную сквозную нумерацию. Если на конкретную формулу нет дополнительных (возвратных) ссылок в тексте или она в единственном числе, то нумерация ее не нужна. Единственные таблица и/или рисунок также не нумеруются.

При публикации в журнале каждая статья (в контактной информации) сопровождается сноской со знаком охраны авторского права ©, поставленным перед фамилией автора (фамилиями авторов) и годом издания.

Авторы (или автор) каждой статьи после выхода журнала в свет имеют право на получение от редакции электронной версии статьи в PDF-формате (редактор Adobe Acrobat).