Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

4

(135)

Подписывайтесь,

читайте,

пишите в наш журнал

Москва 2021

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**

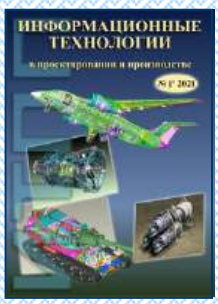
Издается с 1984 года

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

4 (135)

Москва 2021
Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2021.
Вып. 4 (135). С. 1—64.

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

Подписано в печать 10.12.2021. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 7,4 . Уч.-изд. л. 7,6.
Тираж 400 экз. Заказ 1985. Свободная цена.
Адрес редакции: 125424, Москва,
Волоколамское ш., 77. ФГУП «НТЦ оборонного комплекса «Компас».
http://ntckompas.ru
Отпечатано в ООО "РАПИТОГРАФ".
117342, Москва, ул. Бутлерова, д. 17Б.
Индекс 79187.

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.00
DOI: 10.52190/2073-2600_2021_4_3

Обеспечение информационной безопасности и управление доступом в информационных системах современных компаний на основе технологии блокчейн

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

Проработан вопрос обеспечения информационной безопасности и управления доступом в информационных системах на основе технологии блокчейн. Предприняты попытки проанализировать аспекты использования технологии блокчейн в задачах обеспечения информационной безопасности. Новизна представленной работы заключается в систематизации знаний, касающихся обеспечения информационной безопасности и интеграции технологии блокчейн в современных информационных системах.

Ключевые слова: информационная безопасность, блокчейн, управление доступом, информация, информационная система.

В XXI в. произошли качественные изменения, связанные с развитием и интеграцией на современных предприятиях различных информационных технологий, значительно повышающих эффективность и качество работы.

Повсеместная цифровизация общества ставит перед ИТ-сектором множество актуальных и сложных задач, связанных с обеспечением информационной безопасности. Ведутся активные разработки и интеграции инновационных технологий, значительно повышающих уровень обеспечения информационной безопасности компаний, использующих в своей деятельности различные цифровые средства. Несмотря на это, сегмент информационной безопасности (ИБ) нуждается в повышении качества и эффективности работы алгоритмов, препятствующих несанкционированному доступу к информации. Одной из наиболее актуальных и требующих особого внимания задач из области ИБ является управление доступом [1].

Используемые информационные системы имеют недостаточный уровень информационной безопасности, являясь уязвимыми перед потенциальными атаками и несанкционированным проникновением в информационные ресурсы предприятия. В целях снижения подобного рода рисков ведутся активные разработки механизма безопасности, посредством которого происходит управление процессами взаимодействия пользователей с информационными системами и ресурсами (управление доступом).

Основная проблематика представленной работы — изучение путей повышения качества и эффективности работы систем, обеспечивающих информационную безопасность на предприятиях и в организациях. Автор подробно исследует вопрос, касающийся управления доступом в информационных системах компаний на основе технологии блокчейн.

Методы

Использованы теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных рассмотрены научные работы отечественного и зарубежного авторства. В результате автором использованы научные материалы таких авторов, как Пряников М. М., Чугунов А. В., Харченко О. И., Голикова О. М., Федотова А. И. и другие. В каждой из этих работ затрагиваются фундаментальные вопросы, касающиеся общего анализа обеспечения информационной безопасности посредством разработки и интеграции доверенной среды.

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

Статья поступила в редакцию 26 октября 2021 г.

В используемой литературе раскрываты такие вопросы: блокчейн как коммуникационная основа формирования цифровой экономики, блокчейн в информационном обществе, системы контроля и управления доступом, защита информации в информационных системах персональных данных, аспекты обеспечения информационной безопасности в информационных системах.

Актуальные аспекты обеспечения информационной безопасности на основе контроля и управления доступом

Появление крупномасштабных информационных систем обуславливается рядом факторов, связанных с развитием, расширением и цифровизацией бизнеса. Одной из основных проблем эффективного функционирования информационных систем на предприятиях является уязвимость перед вредоносными атаками, направленными на реализацию угроз информационной безопасности. Проблемы, связанные с недостаточным уровнем обеспечения ИБ, способны привести к нарушению конфиденциальности, потере, уничтожению или изменению информации, а также сбою и колоссальным экономическим потерям. Исходя из этого актуальность обеспечения информационной безопасности на основе контроля и управления доступом находится на высоком уровне среди задач ИТ-сегмента.

Комплекс программно-технических средств по защите информации от несанкционированного доступа должен включать в себя подсистему управления доступом для всех классов информационных систем, используемых на предприятии. Таким образом, задача адекватного построения политики разграничения доступа является одним из наиболее важных аспектов в задачах обеспечения информационной безопасности. Реализация программно-технических инструментов по разграничению и управлению доступом способна обеспечить эффективное решение задачи защиты информационных ресурсов информационной системы от несанкционированного доступа (рис. 1) [2].

Основным требованием, предъявляемым к новым технологиям, используемым в системах контроля и управления доступом, является автоматизация процессов построения и разграничения доступа. Исходя из этого наиболее целесообразно использовать подходы, основанные на процессах поддержки принятия решений. Таким образом, в качестве инструмента повышения эффективности функционирования систем управления доступом могут быть задействованы различные интеллектуальные средства, методы иерархий, технология блокчейна и т. д. Новые подходы, интегрируемые в системах управления доступом, должны обеспечивать работоспособность системы ИБ по мере увеличения числа находящихся в информационной системе пользователей.

Таким образом, информационные системы являются объектом повышенной потенциальной и реальной опасности со стороны злоумышленников в лице хакеров, желающих завладеть личными данными, архивами или иной секретной информацией. Существующие средства и методы защиты информации становятся подверженными удачным взломам и несанкционированному доступу, в результате чего актуализируется роль разработки и интеграции инновационных средств обеспечения защищенности информации. Наиболее актуальными становятся задачи, решения которых позволяют повысить эффективность и рациональность работы систем информационной безопасности на основе разработки и интеграции инновационных методов контроля и управления доступом.

Рис. 1. Модель разграничения доступа в системе комплексного обеспечения ИБ

Использование технологии блокчейн в качестве инструмента обеспечения информационной безопасности

Технология блокчейн представляет собой наиболее широкий класс технологий хранения и синхронизации данных. Основной особенностью управления в данном случае является отсутствие централизации. Каждый из узлов распределительной системы делает записи независимо. Записи в технологии блокчейн соединяются в инкрементальную цепочку блоков с помощью криптографических алгоритмов (рис. 2).

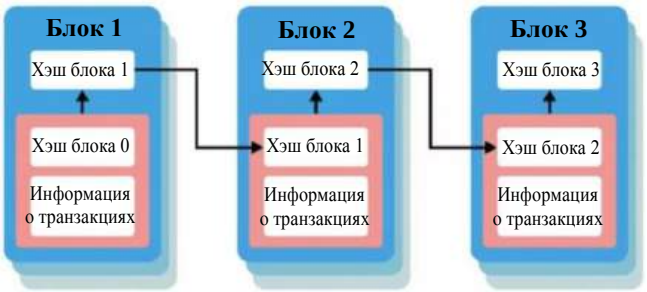


Рис. 2. Принципиальная схема работы технологии блокчейн

Таким образом, блокчейн является децентрализованной базой данных, записи в которой собираются в блоки и связываются на основе криптографических методов. Помимо этого в блоки включаются хеш-суммы текущего и предыдущего блока. Именно они и являются результатом вычисления криптографических функций [3].

Блокчейн, включающий в себя свойства распределенного реестра и блочную структуру данных, реализует такие ключевые аспекты информационной безопасности, как целостность и доступность информации. В результате использования децентрализованной типологии наряду с криптографическими методами манипуляции злоумышленников становятся дорогостоящими и достаточно сложными.

В сетях технологии блокчейн используют специальные криптографические механизмы (SHA-256 и ECDSA и другие), считающиеся достаточно стойкими относительно взлома существующими максимальными мощностями вычислительных систем. Таким образом, блокчейн может быть реализован в качестве инструмента контроля и управления доступом, решая задачи информационной безопасности на предприятии. В течение последних лет на рынке ИТ появляется все большее количество проектов кибербезопасности, использующих в своей основе данную технологию. Так, к примеру, разрабатываются системы контроля и управления доступом, системы проверки целостности прошивок устройств Интернета вещей, алгоритмы защиты от DDoS-атак, децентрализованная идентификация и аутентификация и т. д. [4].

Управление доступом в информационных системах на основе технологии блокчейн

Системы контроля и управления доступом являются ключевым инструментом в обеспечении информационной безопасности, обеспечивая регулирование доступа к важным или засекреченным информационным ресурсам предприятия.

Технология блокчейн может быть использована для разработки стандартного протокола безопасности, поскольку она является более надежной альтернативой сквозному шифрованию. При хранении данных в децентрализованной форме с использованием блокчейна злоумышленникам практически невозможно получить доступ к системам хранения данных. Технология блокчейна может быть использована для проверки таких действий, как исправления, установки и обновления встроенного ПО, а также для защиты данных от несанкционированного доступа во время их передачи с помощью шифрования.

На рис. 3 представлена архитектура структуры для обеспечения контроля и управления доступом на основе технологии блокчейн.

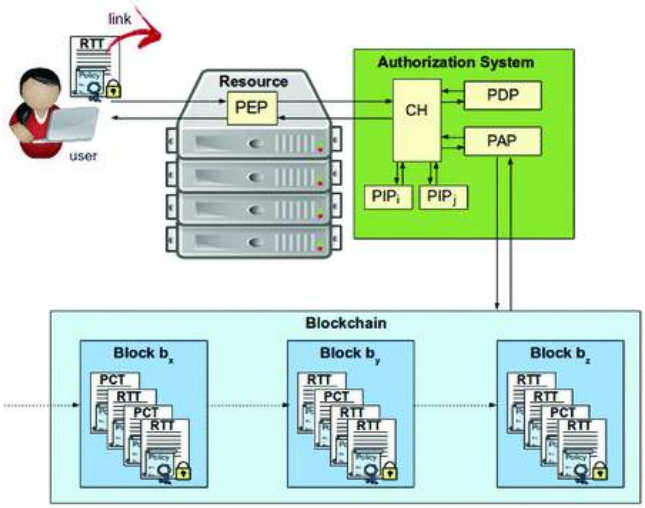


Рис. 3. Архитектура системы управления доступом на основе блокчейна

Данная структура основана на архитектуре XACML, интегрированной с блокчейн. Для обеспечения работоспособности контроля доступа на базе блокчейн необходима настройка точки применения политики (PEP), а также точки администрирования (PAP) [5].

При запросе на выполнение действия над ресурсом помимо идентификаторов субъекта, ресурса и действия PEP также должна получить допол-

нительную информацию, чтобы однозначно связать субъект с информационной базой в блокчейне. В качестве примера, субъекту может потребоваться подписать вызов с закрытым ключом, соответствующим идентификатору, который он использовал для получения прав доступа в систему. Это ничем не отличается от классической схемы аутентификации в сценарии контроля доступа. Вся эта информация необходимым образом включена в запрос, который передается обработчику контекста (CH). CH отвечает за управление рабочим процессом процесса принятия решений, взаимодействуя со всеми другими компонентами системы авторизации.

Кратко можно описать данный процесс следующим образом. Пользователь подает запрос на авторизацию в информационной системе. Далее на основе стандарта XACML по запросу выполняется проверка соответствия в блокчейн. Модуль CH запрашивает информацию и передает запрос в точку принятия решений (PDP), которая сверяет данные и возвращает итоговое решение CH: разрешить или запретить доступ пользователю к информационной системе. Затем CH передает решение PEP, которая применяет его к ресурсу, и выполняется запрос.

Заключение

В результате изучения основных вопросов, касающихся актуальности и возможности использования технологии блокчейн в задачах обеспечения информационной безопасности, в частности контроля и управления доступом, были проработаны такие аспекты, как обеспечение ИБ на основе контроля и управления доступом, модель разграничения доступа в системе комплексного обеспечения ИБ, использование технологии блокчейн в качестве инструмента обеспечения ИБ, управление доступом на основе технологии блокчейн.

Необходимо отметить, что технология блокчейн имеет колоссальный потенциал в реализации мер по защите информации. Хотя данный инструмент и является малоизученным как средство повышения уровня информационной безопасности предприятий, его значение имеет достаточно высокий теоретический уровень. Исходя из сказанного изучению использования блокчейна в качестве инструмента контроля и управления доступом должно быть уделено намного большее внимание со стороны современных ученых и исследователей в области информационной безопасности.

Литература

1. *Пряников М. М., Чугунов А. В.* Блокчейн как коммуникационная основа формирования цифровой экономики: преимущества и проблемы // International J. Open Information Technologies. 2017. V. 5. № 6. P. 49—55.
2. *Харченко О. И.* Блокчейн в информационном обществе // Вестник Саратовского государственного социально-экономического университета. 2018. № 2(71). С. 28—30.
3. *Волошин И. П.* Защита информации в информационных системах персональных данных // Информационная безопасность регионов. 2016. № 1(22). С. 12—15.
4. *Комлев Д. В.* Обеспечение защиты персональных данных как элемент информационной безопасности: актуальность проблемы и способы ее решения: V Междунар. научно-практ. конф. "Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего". 2021. С. 19—27.
5. *Голикова О. М., Федотова А. И.* Способна ли криптовалюта, основанная на технологии "Блокчейн", решить проблемы информационной безопасности финансового сектора? // ИТпортал. 2017. № 3(15). С. 3.

Information security and access control in information systems of modern companies based on blockchain technology

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

The main purpose of this article is to study an important issue concerning information security and access control based on blockchain technology. The author attempts to analyze aspects of the use of blockchain technology in the tasks of ensuring information security. The novelty of the presented work lies in the systematization of knowledge related to information security and the integration of blockchain technology in modern information systems.

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

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

УДК 004.00
DOI: 10.52190/2073-2600_2021_4_7

Разработка проекта автоматизированной контрольно-пропускной системы на предприятии с интегрированной биометрической системой контроля и управления доступом

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

Приведено техническое описание проекта, связанного с разработкой автоматизированной системы контроля управления доступом (СКУД) на предприятии. Новизна представленной работы заключается в разработке системы, не имеющей аналогов, включающей широкий круг возможностей в аспекте контроля и управления доступом. Применены теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных использованы отечественные и зарубежные научные работы.

Ключевые слова: управление доступом, информация, биометрическая система, информационная безопасность, контрольно-пропускная система.

Представлен авторский проект по разработке автоматизированной контрольно-пропускной системы на предприятии с интегрированием биометрической системы контроля и управления доступом. Создаваемая информационная система (ИС) с кодовым названием MonibioAcces основана на применении дактилоскопического метода. Этот метод биометрической идентификации имеет наибольшее распространение. В его основе лежит уникальность рисунков папиллярных линий пальцев человека. Проектируемая ИС является системой класса ИС, обрабатывающей комплекс персональных данных (ИСПД), включающей комплекс информационных технологий и технических средств, автоматизирующих обработку персональных данных (ПД). Хранение ПД в таких системах осуществляется в базах данных (БД). В комплекс ИСПД MonibioAcces будут входить как собственно ПД, так и средства, предназначенные для их обработки и защиты.

Требования к обеспечению безопасности ПД в процессе их обработки в ИСПД устанавливаются Правительством Российской Федерации на законодательном уровне. Согласно требованиям Правительства РФ по достижению целей обработки ПД они должны быть уничтожены либо обезличены. Такие мероприятия проводятся для того, чтобы было невозможно определить, какому конкретному субъекту персональных данных принадлежат эти ПД. Основываясь на требованиях к ПД, необходимо обеспечить в разрабатываемой ИСПД MonibioAcces наличие методов, направленных на обезличивание, которые перечислены в Приказе Роскомнадзора № 996. Один из таких методов заключается в замене ПД или их семантики результатами статистических обработок, обобщений или удаления части данных.

В процессе разработки автоматизированной системы использованы научные достижения отечественных и зарубежных авторов, Так, в работе производится обращение к таким авторам, как Ворона В. А., Костенко В. О., Максимов Р. Л., Рафиков А. Г., Маслова М. А., Полякова Е. Н., Дорофеева А. С. и Spevakov A. G. В работах этих такие фундаментальные темы, как изучение биометрических технологий идентификации в системах контроля и управления доступом, разработка автоматической СКУД повышенной безопасности, обзор современных систем разграничения доступа к ресурсам вычислительной системы и т. д.

Описание концепции автоматизированной системы контроля и управления доступом на базе биометрических методов

Использование биометрической технологии в создаваемой системе заключается не в оперировании непосредственно биометрическими идентификаторами, которые представляют собой изображения отпечатков пальцев, а в обработке их цифровых моделей. При этом восстановление реального биометрического идентификатора по его цифровой модели нельзя осуществить ввиду при-

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

Статья поступила в редакцию 20 сентября 2021 г.

менения шифрования. В процессе шифрования используется датчик, осуществляющий кодирование и подпись идентификатора, а хранение информации обеспечивает частная флэш-память. Хранение данных о папиллярном узоре не требуется, поскольку в памяти сохранится только короткий идентификационный код, созданный на основе характерных особенностей отпечатков пальцев. Такой код не дает возможности восстановить узор отпечатка. Соответственно невозможно сравнить его с отпечатками пальцев. Таким способом гарантируется защита персональных биометрических данных пользователей [1].

Контроль ситуации, обеспечение безопасности персонала, сохранность материальных ценностей и информации, контроль порядка на объекте обеспечиваются автоматической фильтрацией посетителей. Обрабатываемые в ИСПН биометрические характеристики обеспечивают безопасность систем, поскольку их сложнее переместить, потерять или украсть, чем ПИН-коды, пароли и токены. Разрабатываемый модуль (ИС MonibioAcces) интегрируется со СКУД предприятия в качестве исполнительного устройства в информационной системе предприятия.

Состав и функции разрабатываемой системы MonibioAcces

СКУД представляет собой комплекс, состоящий из технических средств и организационных мероприятий, предназначенных для контроля доступа к объектам СКУД и отслеживания перемещения людей по охраняемой территории для того, чтобы обеспечить безопасность, а также регулировать посещения каждого объекта на территории организации. Применение СКУД считают одним из самых эффективных методов обеспечения комплексной безопасности организации. При внедрении СКУД повышается уровень общей безопасности охраняемого объекта, в то время как объем затрат на обеспечение безопасности снижается, поскольку для функционирования СКУД не требуется большой штат персонала для обслуживания. Кроме того, СКУД позволяет экономить на потреблении электроэнергии.

Контроллер исполнительного устройства СКУД, кроме обмена данными с концентраторами СКУД с помощью линий связи, осуществляет следующие функции: анализ входной информации от устройств, считывающих биометрические идентификаторы (результаты анализа используются для последующей выдачи управляющих сигналов на отпирание/запирание исполнительного устройства); контроль состояния исполнительного устройства; хранение данных журнала перемещений в оперативной энергонезависимой памяти устройства; фиксирование каждой попытки несанкционированного доступа.

Контроллер может работать даже в случае аварии электросети, имея резервный источник питания.

Считыватель — устройство, определяющее код идентификатора и передающее его на контроллер.

Наиболее распространены считыватели штрихкода, RFID-считыватели, считыватели пластиковых карт, биометрические считыватели. Считыватели бесконтактных карт (или биометрические) обычно являются неотъемлемой частью СКУД и проходных систем.

На эффективность функционирования каждой СКУД и ее компонентов оказывают прямое влияние технология контроля доступа и квалификация оперативно-технического персонала.

Системы контроля и управления доступом в зависимости от комплектующих и диапазона функций делятся на три группы.

- *Автономные системы*. Основной характеристикой автономной системы является автономный контроллер. Он не связан с другими контроллерами, считыватель отделяется, имеется автономный источник питания. Действие устройства обеспечивает замок с электронным управлением. При срабатывании считывателя происходит сбор информации. Замок связан с хабом, который передаёт информацию на действующую станцию. Основная функция автономной системы — сбор и хранение информации.
- *Сетевые системы*. Основной характеристикой сетевой системы является удалённое управление функциями контроллеров на центральном компьютере. Программное обеспечение позволяет не только накапливать информацию, но и анализировать её. Система осуществляет комплексный подход к системе безопасности. Она контролирует и управляет одновременно такими системами, как видеонаблюдение, охранная сигнализация, система пожаротушения, система экстренного оповещения или аварийного освещения. Возможна работа в системе как проводных, так и беспроводных сетей. Сетевые системы наиболее эффективны при организации безопасности крупных объектов.
- *Биометрические системы*. Биометрические системы являются самой функциональной организацией системы контроля и удалённого доступа, так как имеют высокий уровень безопасности. Основная задача биометрических систем заключается в осуществлении биометрической аутентификации. К идентифицирующим признакам биометрического устройства контроля доступа относятся био-

метрические параметры человека, такие, как отпечатки пальцев, геометрия рук, рисунок сетчатки глаза и т. д. На основании этих параметров СКУД принимает решение о предоставлении доступа к объекту только тому лицу, которое является носителем кода (биометрических параметров) [2].

Основные назначения и требования к разрабатываемой СКУД

Целью разработки СКУД является автоматизация контролируемого пропуска людей на охраняемый объект и пропускного режима персонала и посетителей на территорию предприятия для создания условий выполнения требований установленного режима на объекте и обеспечения безопасности дежурного персонала, ведение учёта рабочего времени сотрудников и контроля за исполнением трудовой дисциплины.

В комплекс функций, выполняемых СКУД, входят: формирование и выдача управляющих команд в процессе считывания идентификационного признака (идентификационного кода), хранящегося в памяти подсистемы, для исполнительных устройств; открывание дверей в ручном режиме для возможности прохода при аварийных ситуациях, пожарах, технических неисправностях с выдачей сигнала тревоги; передача данных о состоянии системы к АРМ, учёт периодов пребывания сотрудников на каждом объекте.

Разрабатываемый модуль MonibioAcces интегрируется со СКУД предприятия в качестве исполнительного устройства в информационной системе. СКУД должна обслуживать проходную дверь КПП. В случае запуска системы оповещения о пожаре проходная дверь должна открываться автоматически либо согласно команде оператора, отдаваемой в ручном режиме. Контроль открывания проходной двери КПП предполагает проход через неё по реакции входного считывателя на права доступа пользователя [3].

Для надёжного функционирования системы должна быть обеспечена возможность непрерывной работы с учётом перерывов, необходимых для технического обслуживания. Должна быть обеспечена возможность резервного копирования или кластерного исполнения решения. Уровень надёжности достигается совокупностью применяемых организационных и организационно-технических мероприятий, а также с помощью программно-аппаратных средств. Безопасность технических средств, на которых реализованы компоненты ИС, должна проявляться в обеспечении защиты от воздействий электрического тока, акустических шумов и т. п., а также осуществляться в соответствии с требованиями по эксплуатации, предъявляемыми к оборудованию его разработчиками.

Автоматизированная СКУД MonibioAcces — это способ обеспечения трудовой дисциплины, порядка и безопасности на объекте, обладающий высокой эффективностью. Эффект, ожидаемый от системы, и оценка целесообразности создания автоматизированной учётно-пропускной подсистемы на предприятии с интегрированием биометрической системы контроля и управления доступом отражены на рис. 1.

Рис. 1. Достоинства создаваемой информационной системы

Согласно рис. 1 достоинство проектируемой информационной системы заключается не только в выполнении основной функции системы — организации пропуска. Автоматизированная учётно-пропускная подсистема на предприятии с интегрированием биометрической системы контроля и управления доступом удобна тем, что не надо носить идентификатор; невозможно пройти по чужому идентификатору.

Общая характеристика разрабатываемой СКУД

Создаваемая информационная система относится к классу ИСПД. Такая ИС хранит совокупность ПД в базе данных, а также включает комплекс информационных технологий и технических средств, предназначенных для обработки таких ПД с помощью автоматизированных средств. ИСПД содержит как непосредственно персональные данные, так и средства, применяемые для их обработки и защиты.

Создаваемая ИСПД MonibioAcces содержит ПД, к которым относятся фамилии, имена, отче-

ства, года, месяцы, даты и места рождения, адреса, семейное, социальное, имущественное положение, данные об образовании, профессии, доходах, почтовые адреса, номера телефонов и прочую информацию о сотрудниках, а также базы данных, в которых хранятся ПД, серверы, т. е. оборудование, на котором хранятся базы, программы, где данные обрабатываются, компьютеры, на которых работают сотрудники, защитные программы.

Определение уровня защищённости персональных данных для создаваемой ИСПД

Уровнем защищённости ПД называется комплексный показатель, характеризующий процесс выполнения требований, направленных на устранение угроз безопасности ИСПД. На рис. 2 представлены критерии, определяющие уровень защищённости ПД [4].

Рис. 2. Критерии оценки уровня защищённости ПД

Создаваемая СКУД относится к классу ИСПД, т. к. в ней будут обрабатывать данные физиологических и биологических особенностей человека, составляющих основу для установления личности. Также эти особенности будут использованы оператором в процессе установления личности субъекта ПД. В создаваемой ИСПД не будут обрабатывать сведения, которые относятся к специальным категориям ПД.

Механизм действия системы ИСПД MonibioAcces

Механизм:

- в базе данных сохраняется эталонная модель, основанная на биометрических характеристиках человека. Для этого используется биометрический образец отпечатка пальца;
- сохранённые данные преобразуются в математический код. Таким образом формируется база данных, представляющая собой набор кодов до 1000 бит, фиксирующих уникальные биометрические характеристики пользователей;
- при считывании отпечатков пальцев сканер не распознаёт само изображение, а преобразовывает его в цифровой код, который затем сравнивает с загруженной ранее эталонной моделью;
- восстановить реальный идентификатор по его цифровой модели не представляется возможным, поскольку в процессе его создания применяется шифрование: шаблоны посещаемости шифруются и подписываются с помощью датчика, а все данные о шаблоне хранятся в частной флэш-памяти. При этом не требуется хранение папиллярного узора пальца, т. к. вместо него хранится короткий идентификационный код, созданный на основе характерных особенностей отпечатков пальцев. Этот код не позволяет осуществлять воссоздание узора для последующего сравнения с отпечатками пальцев.

ИСПД MonibioAcces в качестве модуля СКУД интегрируется в единую систему СКУД предприятия на аппаратном и программном уровнях. Аппаратную часть (устройства СКУД) подключают в сеть под управлением одного сервера. Программные средства (ПО) управляют модулями СКУД, обеспечивая их согласованное, синхронное функционирование и обмен данными между модулями СКУД.

Моделирование функциональных требований к системе

Диаграмма потоков данных (ДПД, или DFD) — основное средство моделирования функциональных требований к системе. Главной целью DFD является демонстрация преобразования каждым процессом системы входных данных в выходные, а также выявление отношений между процессами. В этой нотации описывается не столько непосредственно процесс, сколько движение потоков данных. Для интерпретации DFD-диаграмм нужно придерживаться следующих правил: функции отвечают за преобразование входящих потоков данных в выходящие; хранилища данных не могут изменять потоки данных, а применяются только для хранения поступающих объектов.

На рис. 3 изображена контекстная диаграмма потоков данных проектируемой ИС.

На рис. 3 представлены следующие внешние сущности: "Пользователь", "Администратор". Процесс "Регистрация пользователя" принимает от внешней сущности "Пользователь" следующие потоки данных: "Данные пользователя" и "Сохраненный образ отпечатка пальца пользователя", а на выходе отправляет поток данных "Сгенерированный отпечаток пальца пользователя" и поток данных "Статистика зарегистрировавшихся пользователей" внешней сущности "Администратор".

Рис. 3. Контекстная диаграмма потоков проектируемой ИС

Суть применения DFD заключается в том, что источники информации (внешние сущности) создают информационные потоки (потоки данных), которые переносят данные к подсистемам или процессам, отвечающим за преобразование информации и создание новых потоков, передающих данные другим процессам или подсистемам, накопителям данных или внешним сущностям — потребителям информации [5].

На рис. 4 представлена диаграмма потоков данных первого уровня, образованная после декомпозиции контекстной диаграммы.

Рис. 4. Декомпозиция контекстной диаграммы потоков проектируемой ИС

Заключение

Разработанная биометрическая система контроля и управления доступом на КПП предприятия представляет собой совокупность технических средств и организационных мероприятий, направленных на контроль доступа к объектам СКУД и отслеживание перемещений людей по охраняемой территории.

В заключение необходимо отметить, что программное обеспечение разрабатываемой ИС MonibioAcces представляет собой комплекс программных продуктов, организующих прямое взаимодействие системы с контроллером управления доступом. Клиентско-серверная архитектура ПО и использование при реальной разработке дополнительных клиентских мест могут обеспечить гибкое управление системой на объекте. Программа СКУД MonibioAcces подразумевает использование специализированных модулей, выполняющих функции, обеспечивающие высокий уровень безопасности. При необходимости расширения функционала или ёмкости системы могут формироваться дополнительные клиентские места и программные модули (готовые решения). Таким образом, предложенная в рамках данной статьи ИС имеет колоссальный потенциал и актуальность при решении задач из области контроля и управления доступом на современных предприятиях.

Литература

1. *Ворона В. А., Костенко В. О.* Биометрические технологии идентификации в системах контроля и управления доступом // Computational nanotechnology. 2016. № 3. С. 224—241.
2. *Максимов Р. Л., Рафиков А. Г.* Разработка автоматической СКУД повышенной безопасности на базе типового решения скуд BioSmart с использованием автоматного подхода // Вопросы кибербезопасности. 2015. № 5(13). С. 73—80.
3. *Маслова М. А.* Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. Т. 4. № 1. С. 31—37.
4. *Полякова Е. Н., Дорофеева А. С.* Обзор современных систем разграничения доступа к ресурсам вычислительной системы // Вестник Курганского государственного университета. Серия "Технические науки". 2016. № 3(42). С. 122—127.
5. *Спеваков А. Г.* Методы идентификации личности человека по морфологическим признакам: Сб. мат. IX Междунар. конф. "Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание–2010". 2010. Курск, 18—20 мая 2010 г. С. 53—54.

Development of the project of an automated checkpoint system at the enterprise with the integration of a biometric access control and management system

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

The main purpose of this article is a technical description of a project related to the development of an automated access control system at an enterprise. The scientific novelty of the presented work consists in the development of a system that has no analogues, including a wide range of capabilities in the aspect of access control and management. The author uses theoretical and empirical research methods. In order to obtain more detailed information and up-to-date data, scientific works of domestic and foreign authorship used in the work.

Keywords: access control, information, biometric system, information security, checkpoint system.

Bibliography — 5 references. *Received September 20, 2021*

ДОВЕРЕННАЯ СРЕДА

УДК 004.056.53
DOI: 10.52190/2073-2600_2021_4_13

Технология SMM и ее применение в компьютерной безопасности

М. В. Пахомов
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

В статье рассмотрен один из наиболее привилегированных режимов выполнения кода на компьютерах архитектуры x86 System Management Mode (SMM). Описана корректная конфигурация режима SMM, определены возможные функции безопасности с использованием SMM и указаны плюсы и минусы использования этой технологии для обеспечения безопасности. Проведен анализ и дана оценка целесообразности применения данной технологии в компьютерной безопасности.

Ключевые слова: System Management Mode, System Management Interruption, средство защиты информации, компьютерная безопасность, регистр SMI_EN, кольца защиты, режим исполнения кода, архитектура x86.

Архитектура x86 подразумевает наличие как минимум трех различных уровней привилегий для выполнения инструкций процессором [1]. Эти уровни привилегий называются кольцами защиты (англ. *protection rings*), Код, исполняемый в центральном кольце («ring 0»), обладает наибольшим доступом в операционной системе (ОС), а во внешнем кольце («ring 3») — наименьшим [1]. Эти уровни привилегий предназначены для реализации аппаратного разграничения доступа процесса к ресурсам ЭВМ (например, к портам ввода-вывода) и реализованы в ЭВМ в виде различных режимов работы центрального процессора (ЦП).

Однако кроме стандартных уровней привилегий для ОС, существуют также более привилегированные уровни (обладающие большим доступом, чем «ring 0»), которые нумеруются в отрицательную область чисел, с соответствующими режимами работы ЦП: «ring -1» — режим гипервизора и «ring -2» — System Management Mode (SMM) [1]. Также существует режим «ring -3», основанный на технологиях Intel Management Engine (ME) для процессоров Intel и AMD Secure Technology для процессоров AMD [2, 3]. В свою очередь, режимы гипервизора и SMM подразумевают использование технологий гипервизора и SMM, в которых используются выделенная (недоступная из менее привилегированных режимов) память и независимое от ОС программное обеспечение (ПО): ядро, приложения и драйвера.

При этом уже в режиме супервизора (т. е. на уровне «ring 0») исполняемые процессором инструкции обладают практически полным доступом к ресурсам ЭВМ и этот доступ может контролироваться только более привилегированными режимами [1]. Вместе с тем выполнение инструкций в режимах «rings -1, -2, -3» для ОС прозрачно и не отслеживаемо напрямую [4, 5]. Поэтому с одной стороны, такие технологии являются ключевыми для атак низкого уровня [6, 7] и могут представлять угрозы для средств защиты информации (СЗИ), функционирующих с привилегиями не ниже «ring 0», а с другой стороны, с помощью таких технологий можно расширить функциональность существующих СЗИ либо попытаться реализовать полнофункциональное СЗИ на основе таких технологий.

Используемые методы исследования

В данной статье из ранее упомянутых режимов будет рассматриваться только SMM. Цель работы — оценка перспективы использования технологии SMM в разработке СЗИ. В работе используются такие методы исследования, как анализ, абстрагирование, сравнение и эксперимент. Объектом исследования является SMM. Предмет исследования — возможность использования механизмов SMM для разработки СЗИ.

Обзор литературы

1. Описание SMM

SMM является привилегированным режимом выполнения кода у x86 совместимых процессоров (Intel, AMD), впервые реализованным компанией Intel в своих процессорах в середине 90-х годов [8]. С момента создания и до сих пор этот режим используют для совершения действий, незаметных и практически не отслеживаемых для ОС, но при этом выполняемый код обладает полным досту-

Пахомов Михаил Вадимович, студент.
E-mail: pahomov.mv@phystech.edu

Статья поступила в редакцию 18 октября 2021 г.

пом к памяти и всем подключенным устройствам [5].

Изначально SMM применяли в области управления питанием компонентов ЭВМ: обработчики событий в SMM собирали статистику по использованию устройств и в случае их долговременного простоя отключали [8]. То есть первоначально в задачи SMM не входило решение проблем обеспечения безопасности, а привилегированный режим был обусловлен необходимостью в постоянном контроле всех устройств ЭВМ. На данный момент задача управления питанием компонентов ЭВМ выполняется не с помощью SMM, а при помощи ОС [8].

Для переключения процессора в SMM используются System Management Interruptions (SMIs), которые генерируются компонентами материнской платы либо различными драйверами, приложениями (в том числе приложениями из ОС) или пользователями с административными правами в ОС [5]. К типовым системным SMI, которые поддерживаются в большинстве ЭВМ (в частности, согласно документации, у компьютеров с 8/9/200/300 сериями чипсетов Intel [9, 10, ч. 12.8.3.7; 11, 12, ч. 5.2.4]), можно отнести следующие прерывания и соответствующие им события [5, 9, 10, ч. 12.8.3.7; 11, 12, ч. 5.2.4]:

- GPIO Unlock SMI. Генерируется при снятии бита Lock (*GLE*) с регистров управления выводами GPIO. Обработчик проверяет ПО, снявшее бит, и если оно не авторизованное, выставляет бит обратно;
- TCO SMI. Генерируется при различных событиях. Обработчик прерывания выполняет действия согласно источнику прерывания:
  - Intel TCO watchdog-таймером обратного отсчета при опускании таймера до нуля. Этот таймер должен взводиться ОС каждые несколько секунд. Если таймер опустится до нуля, то произойдет прерывание, обработчик которого произведет перезагрузку системы;
  - при выставлении бита *BIOSWE* у регистра BIOS Control, отвечающего за возможность читать и писать в ПЗУ, где находится код BIOS'а. Если бит выставляется в SMM, то прерывание не будет сгенерировано, так как выполняемый код уже в SMM режиме; если бит выставляется в любом другом режиме, то прерывание будет сгенерировано, после чего будет вызван обработчик, который просто выставит бит обратно. Такой механизм реализован для защиты от перезаписи прошивки ЭВМ из любого режима, кроме SMM;
- APMC (APM Control) SMI. Генерируется при записи в APM_CNT I/O порт (почти всегда это порт 0xB2). Срабатывание такого прерывания может быть вызвано администратором ОС при помощи записи в ранее указанный порт. Количество обработчиков может быть 256. При этом при вызове можно указывать номер желаемого обработчика;
- IOTR (IO Trap) SMI. Генерируется при обращении к портам CPU I/O. Обработчик позволяет эмулировать Legacy-устройства (например, клавиатуру), которые раньше использовали I/O порты;
- xHCI (Extensible Host Controller Interface) SMI. Генерируется USB-контроллером при различных событиях;
- Periodic SMI. Генерируется чипсетом по таймеру с периодичностью 8/16/32/64 (период настраивается с помощью битов *PER_SMI_SEL*).

2. SMM memory (SMRAM)

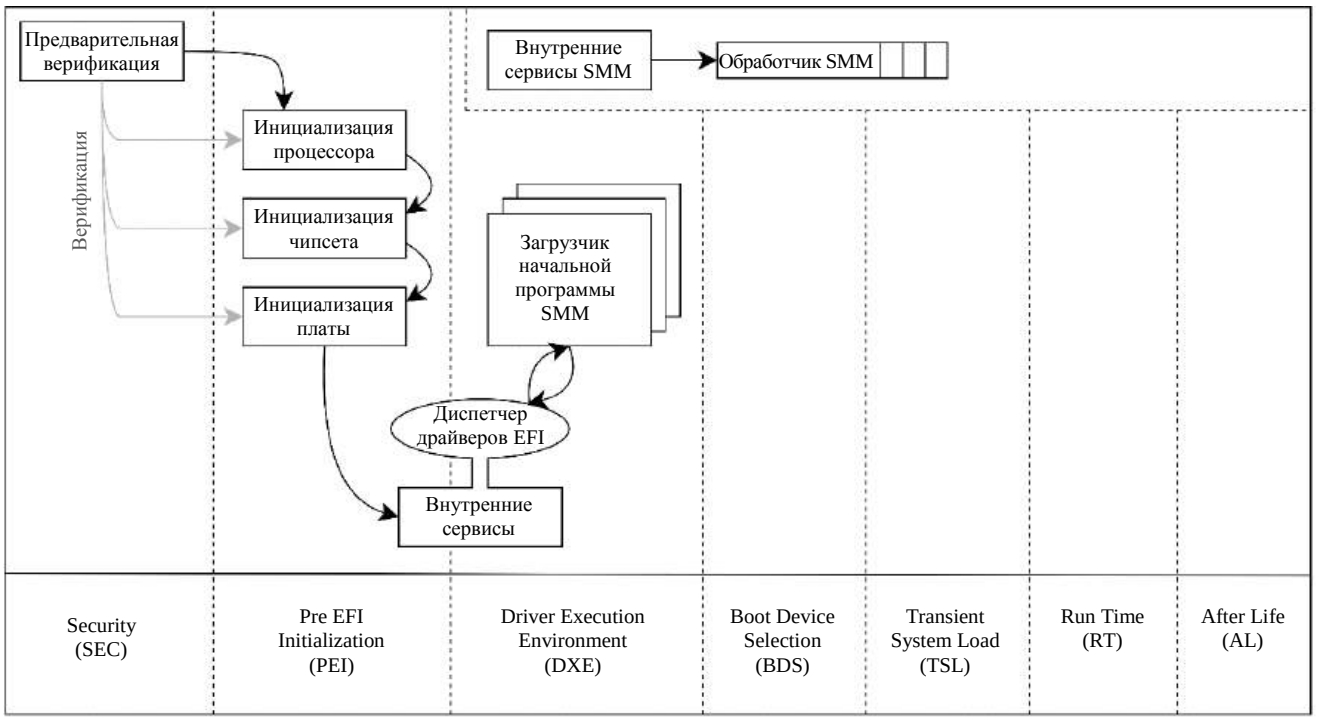
Для изолированности среды выполнения операций в режиме SMM используется память SMM memory (SMRAM), в которой хранятся все необходимые данные для работы SMM: код и обработчики прерываний, а также содержимое регистров (процессор сохраняет контекст при переключении в SMM). Если какая-либо операция выполняется не в режиме SMM, а в обычном режиме (менее привилегированном), то эта память недоступна, т. е. нельзя как прочитать данные из этого пространства, так и записать туда что-либо. SMRAM может состоять из следующих областей (вывод об использовании или не использовании сделан по отношению к современным ЭВМ со стандартной конфигурацией SMM) [5, 8]:

- ASEG [0x000A0000-0x000BFFFF] не используется;
- HSEG [0xFEDA0000-0xFEDBFFFF] не используется;
- TSEG (настраиваемый диапазон) используется.

3. Инициализация SMRAM

Целесообразно рассматривать инициализацию SMRAM и работу SMM с использованием UEFI BIOS, а не Legacy BIOS, так как большинство современных ЭВМ используют именно интерфейс UEFI, а Intel вовсе планирует исключить поддержку Legacy BIOS из своих устройств в ближайшие годы [13].

Весь код SMM (в том числе SMI-обработчики) хранится в коде UEFI BIOS, который находится в ПЗУ. Этот код выгружается в SMRAM и конфигурируется однократно при включении ЭВМ на стадии SMM, которая, в свою очередь, является частью фазы DXE (все стадии изображены на рисунке) [14]. После этого SMM-фаза активна в течение всего временного интервала активности ЭВМ параллельно другим Run Time (RT) фазам.



Фазы загрузки системы с UEFI

В процессе инициализации SMRAM выполняются инициализация физической памяти, настройка TSEG, копирование SMM-кода в физическую память, настройка таблицы дескрипторов. Одним из важнейших заключительных этапов является корректное выставление регистров, ответственных за корректную работу памяти и её защиту.

4. Регистры SMM

Для корректной работы SMRAM и настройки доступа к этой памяти используется несколько регистров. Основным регистром является System Management RAM Control (*SMRAMC*) регистр [15, ч. 3.29]. Значение *SMRAMC* выставляется при инициализации SMRAM, после чего регистр блокируется до следующего рестарта ЭВМ [16]. Среди битов этого регистра наиболее важны биты *D_OPEN* и *D_LCK*, которые должны быть установлены в 0 и 1 соответственно на любой корректно сконфигурированной системе, чтобы SMRAM-память была доступна только из кода, выполняемого в SMM.

Существуют производные регистры для обеспечения корректного доступа к памяти, которые созданы вследствие обнаружения различных векторов атак на SMM (эти регистры также должны быть корректно сконфигурированы и заблокированы аппаратным обеспечением):

- System Management Range Registers (*SMRR*) определяет области памяти, в которых запись не из SMM игнорируется, а тип памяти является некэшируемым. Должен быть корректно выставлен вендорами. Атака — SMM cache poisoning [17];
- *TSEGMB*-регистр у DMA-контроллеров дублирует информацию о местоположении TSEG, после чего запрещается писать в эту область с помощью DMA. Должен быть корректно выставлен вендорами. Атака — DMA [18];
- *SMI_LOCK* бит регистра General PM Configuration, *SMM_BWP* бит регистра BIOS Control отвечают за генерацию SMI при прошивании BIOS. Атака — отключение генерации SMI, после чего перепрошивка BIOS неавторизованным ПО [19].

Результаты

1. Функции безопасности с использованием SMM

SMM предназначен для обработки прерываний, которые сгенерированы либо системой (системные SMI), либо прошивкой/драйверами/приложениями, обладающими доступом с правами администратора в ОС (программные SMI) при помощи записи в APM_CNT I/O порт. Таким образом, возможно создание лишь двух типов функций (обработчиков SMI) на основе SMM:

- создание обработчика программных SMI. Вызывать такой обработчик можно с помощью ПО в ОС;

- расширение обработчика системных SMI. Вызываться такой обработчик будет автоматически при каких-то событиях (зависит от типа SMI).

При этом, учитывая особенности SMM (привилегированность, изолированность среды выполнения инструкций SMM, хранение кода SMM в BIOS), можно говорить о применении обработчиков SMI для создания функций, которым необходимо одно из свойств:

- выполнение привилегированных инструкций;
- выполнение инструкций в изолированной среде по отношению к программной среде в ОС;
- возможность хранения секретных данных малого размера (например, токены, сертификаты, криптографические ключи) в защищенном пространстве, т. е. использование части памяти ПЗУ, где хранится код BIOS, как небольшого хранилища информации, к которому можно получить доступ с помощью SMI-обработчиков.

Далее рассматриваются более подробно возможные функции безопасности, которые потенциально можно реализовать с помощью обработчиков SMI.

1.1. Создание обработчика программных SMI

Для вызова обработчика программных SMI необходим корректно выставленный бит *APMC_EN* регистра *SMI_EN* [9, 10, ч. 12.8.3.7; 11, 12, ч. 5.2.4]. Этот бит является R/W и может быть перезаписан в любой момент, если не реализована функциональность блокировки регистра *SMI_EN*. Таким образом, не следует полагаться на гарантированное срабатывание прерывания из-за отсутствия встроенной функциональности блокировки.

Обработчик программных SMI подходит для реализации функций, которые требуется вызывать из ОС для выполнения заведомо определенных привилегированных инструкций. Примеры возможных функций безопасности:

- выполнение мгновенной перезагрузки/выключения системы при выявленных попытках несанкционированного доступа;
- проверка переданных учетных данных и расширение прав доступа пользователя;
- генерация дочерних сертификатов/ключей на основе корневого сертификата/ключа без возможности прочитать корневой сертификат/ключ;
- включение/отключение/проверка компонентов системы и периферийных устройств (например, проверка контрольной суммы кода BIOS или отключение одного из USB-устройств через интерфейс xHCI);
- настройка регистров, которые контролируют доступ к компонентам системы и периферийным устройствам (например, включение/выключение возможности записи на жесткий диск).

1.2. Расширение обработчика системных SMI

Для вызова обработчика системных SMI необходим корректно выставленный бит включения прерываний регистра *SMI_EN* для требуемого типа прерываний [9, 10, ч. 12.8.3.7; 11, 12, ч. 5.2.4]. Большинство таких битов являются R/W и аналогично биту *APMC_EN* могут быть перезаписаны в любой момент, если отсутствует функциональность блокировки регистра *SMI_EN*. Таким образом, подобно программным SMI, нельзя полагаться на гарантированное срабатывание большинства системных SMI при отсутствии функциональности блокировки. Вместе с тем для некоторых прерываний предусмотрена встроенная функциональность блокировки соответствующего бита. Так, например, для всех современных ЭВМ архитектуры x86 такими битами являются *GPIO_UNLOCK_SMI_EN* и *TCO_EN*.

На базе таких обработчиков можно реализовать более специфичные функции с автоматически генерируемыми прерываниями различными компонентами системы при наступлении конкретных событий (зависит от компонента и типа SMI). Примеры возможных функций безопасности (обработчики):

- TCO SMI можно модифицировать для обработки запросов на перезапись прошивки;
- GPIO Unlock SMI можно модифицировать либо заменить своим обработчиком для контроля доступа ОС к GPIO-контактам;
- xHCI SMI (*xHCI_SMI_EN* бит является R/W) можно модифицировать либо дополнить необходимыми функциями, чтобы обрабатывать различные события, связанные с USB-устройствами [20, ч. 4.22.1];
- Periodic SMI (*PERIODIC_EN* бит является R/W) можно модифицировать либо дополнить необходимыми функциями, чтобы выполнять указанный код многократно с установленным периодом.

2. Плюсы и минусы SMM для СЗИ

Плюсы и минусы SMM разделены на фундаментальные и технические. Первые особо важны, так как они являются архитектурной особенностью режима, а следовательно, никаким образом

не могут быть значительно изменены в последующих обновлениях прошивки в отличие от технических атрибутов SMM.

2.1. Плюсы SMM

Фундаментальные:

- привилегированный доступ. В базовом сценарии SMM предоставляет максимальный доступ к системе среди прочих встроенных в систему технологий (за исключением технологий, которые базируются на РКБ);
- дешевизна и высокая бесперебойность. Решение на базе SMM не нуждается в дополнительном аппаратном оборудовании, а реализуется в уже существующем окружении, что положительно сказывается на бесперебойности СЗИ и количестве возможных аппаратных неисправностей, а также на стоимости самого решения.

Технические:

- ранняя стадия старта функционирования. SMM-код загружается и запускается в DXE-фазе загрузки UEFI. Эта фаза идет после фаз SEC и PEI и до фазы Boot Device Selection (BDS) (см. рисунок) [21]. С одной стороны, наличие двух фаз перед запуском SMM является, определенно, минусом, но с другой стороны, это позволяет коду SMM работать с памятью (которая инициализируется в PEI) и работать с устройствами системы. При этом полноценно функционировать SMM начинает после блокирования SMRAM до окончания фазы DXE, т. е. в конце фазы DXE SMRAM уже находится в заблокированном состоянии, и SMM может обрабатывать приходящие запросы. Поэтому в фазе BDS можно говорить о полном функционировании технологии SMM;
- встроенная защита кода SMM от перезаписи. Одной из основных задач SMM на текущий момент является обработка запросов системы на прошивание BIOS'а, где и хранится код SMM. Таким образом, при правильной конфигурации SMM можно защитить SMM-код от несанкционированных воздействий (не рассматривается прошивание памяти с помощью аппаратного воздействия).

2.2. Минусы SMM

Фундаментальные:

- доверие к вендору. При использовании SMM необходим РКБ для построения доверенной системы (в том числе для того, чтобы контролировать недоверенный процессор [22]) либо необходимо доверять процессору (который в таком случае будет выполнять некоторые задачи РКБ) и, как следствие, доверять вендору. Также, поскольку системные SMI генерируются различными компонентами системы (например, xHCI-контроллером, отвечающим за взаимодействие с USB), необходимо доверять этим контроллерам в части срабатывания прерываний при наступлении конкретных событий.

Технические:

- платформозависимость. Технология SMM сильно платформозависима и разработана только для x86-архитектуры. Также не менее важным является факт, что вендоры (в том числе Intel, AMD) не гарантируют наличие тех или иных системных SMI в системе по умолчанию (это можно проследить в документации [9, 10, ч. 12.8.3.7; 11, 12, ч. 5.2.4]);
- ограничения по памяти. Согласно документации под сегмент TSEG SMRAM может быть выделено 1, 2 или 8 MB (мегабайт) [16, ч. 3.37], что ставит ограничения на разрабатываемый код;
- большинство битов в регистре *SMI_EN* являются R/W, поэтому нельзя полагаться на срабатывание конкретных SMI. Для устранения этого недостатка требуется разработать собственную логику в SMM, которая сможет блокировать необходимый бит.

Обсуждение

Таким образом, наиболее целесообразным и простым использованием SMM является применение этой технологии для реализации небольшого хранилища данных либо функций, к которым будет ограничен доступ на чтение и изменение посредством SMI обработчиков. При этом обеспечить взаимодействие с данной частью памяти и получить доступ к ней можно напрямую из ОС. Примеров реализации коммуникации кода ОС и SMM-кода в свободном доступе достаточно много [14, 23, 24].

С другой стороны, можно использовать автоматически генерируемые SMI, создаваемые Platform Controller Hub'ом (PCH). Однако этот способ является эффективным только в случае блокировки битов, отвечающих за срабатывание прерываний. Поэтому необходимо также реализовать дополнительную функциональность, которая будет отвечать за неизменность этих битов. Документация Intel не декларирует возможностей по блокировке таких битов [9, 10, ч. 12.8.3.7; 11, 12, ч. 5.2.4], а примеры атак на ЭВМ [25] с изменением таких битов еще раз подтверждают наличие векторов

атак в случае реализации СЗИ через SMI. Существует патент по реализации блокировки регистра *SMI_EN* [26], но он скорее описывает архитектурную возможность по аппаратному улучшению чипсета (в частности, южного моста чипсета), нежели возможность по реализации блокировки регистра с помощью программных средств. Таким образом, предлагаемый вариант блокировки в патенте может быть целесообразен для вендоров компьютерной техники, поскольку они могут вносить существенные изменения в структуру элементов ЭВМ, но не является целесообразным для разработчиков СЗИ.

Заключение

Из изложенного можно сделать вывод, что поскольку выполняемый в SMM код обладает достаточно привилегированным доступом в ЭВМ, этот режим остается крайне интересным для исследования на уязвимости в целях выработки рекомендаций по корректному конфигурированию. При этом из-за архитектурных особенностей данной технологии реализация каких-либо новых инструментов безопасности с использованием SMM представляет собой сложную и нецелесообразную задачу. Поэтому в современных ЭВМ необходимо правильно конфигурировать SMM и не следует полагаться на эту технологию при разработке СЗИ.

Литература

1. *Domas C.* The Memory Sinkhole [Электронный ресурс]. URL: https://www.blackhat.com/docs/us-15/materials/us-15-Domas-The-Memory-Sinkhole-Unleashing-An-x86-Design-Flaw-Allowing-Universal-Privilege-Escalation-wp.pdf (дата обращения: 14.11.2020).

2. *Oster J. E.* Getting Started with Intel® Active Management Technology (Intel® AMT) [Электронный ресурс]. URL: https://software.intel.com/content/www/us/en/develop/articles/getting-started-with-intel-active-management-technology-amt.html (дата обращения: 18.11.2020).

3. О безопасности UEFI, часть заключительная [Электронный ресурс]. URL: https://habr.com/ru/post/268423/ (дата обращения: 18.11.2020).

4. *Jiewen Y., Zimmer J. V.* A Tour Beyond BIOS Launching STM to Monitor SMM in EDK II [Электронный ресурс]. URL: https://software.intel.com/content/dam/develop/external/us/en/documents/a-tour-beyond-bios-launching-stm-to-monitor-smm-in-efi-developer-kit-ii-819978.pdf (дата обращения: 18.11.2020).

5. О безопасности UEFI, часть вторая [Электронный ресурс]. URL: https://habr.com/ru/post/267197/ (дата обращения: 18.11.2020).

6. *Rauchberger J., Luh R., Schrittwieser S.* LONGKIT – A Universal Framework for BIOS/UEFI Rootkits in System Management Mode // Conference: 3rd International Conference on Information Systems Security and Privacy. P. 346—353.

7. Банк данных угроз безопасности информации. SMM [Электронный ресурс]. URL: https://bdu.fstec.ru/search?q=SMM (дата обращения: 18.11.2020).

8. SMM и SMRAM или 128 Кб потусторонней памяти: исследовательская работа № 5 [Электронный ресурс]. URL: https://xakep.ru/2008/07/29/44663/ (дата обращения: 18.11.2020).

9. Intel® 8 Series/C220 Series Chipset Family Platform Controller Hub (PCH) [Электронный ресурс]. URL: https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/8-series-chipset-pch-datasheet.pdf (дата обращения: 18.11.2020).

10. Intel® 9 Series Chipset Family Platform Controller Hub (PCH) [Электронный ресурс]. URL: https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/9-series-chipset-pch-datasheet.pdf (дата обращения: 18.11.2020).

11. Intel® 200 (Including X299) and Intel® Z370 Series Chipset Families Platform Controller Hub (PCH). Volume 2 [Электронный ресурс]. URL: https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/200-series-chipset-pch-datasheet-vol-2.pdf (дата обращения: 18.11.2020).

12. Intel® 300 Series and Intel® C240 Series Chipset Families Platform Controller Hub (PCH). Volume 2 [Электронный ресурс]. URL: https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/300-series-chipset-pch-datasheet-vol-2.pdf (дата обращения: 18.11.2020).

13. Intel to Remove Legacy BIOS Support from UEFI by 2020 [Электронный ресурс]. URL: https://www.anandtech.com/show/12068/intel-to-remove-bios-support-from-uefi-by-2020 (дата обращения: 09.05.2021).

14. Building reliable SMM backdoor for UEFI based platforms [Электронный ресурс]. URL: http://blog.cr4.sh/2015/07/building-reliable-smm-backdoor-for-uefi.html (дата обращения: 18.11.2020).

15. 8th and 9th Generation Intel® Core™ Processor Families and Intel® Xeon E Processor Family [Электронный ресурс]. URL: https://www.intel.com/content/dam/www/public/us/en/documents/datasheets/8th-gen-core-family-datasheet-vol-2.pdf (дата обращения: 18.11.2020).

16. Intel® Platform Innovation Framework for EFI System Management Mode Core Interface Specification (SMM CIS) [Электронный ресурс]. URL: https://www.intel.ru/content/dam/doc/reference-guide/efi-smm-cis-v091.pdf (дата обращения: 18.11.2020).

17. Attacking SMM Memory via Intel® CPU Cache Poisoning [Электронный ресурс]. URL: https://invisiblethingslab.com/resources/misc09/smm_cache_fun.pdf (дата обращения: 18.11.2020).

18. Attacking UEFI Boot Script [Электронный ресурс]. URL: https://bromiumlabs.files.wordpress.com/2015/01/venamis_whitepaper.pdf (дата обращения: 18.11.2020).

19. О безопасности UEFI, части нулевая и первая [Электронный ресурс]. URL: https://habr.com/ru/post/266935/ (дата обращения: 18.11.2020).

20. eXtensible Host Controller Interface for Universal Serial Bus (xHCI) [Электронный ресурс]. URL: https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/extensible-host-controler-interface-usb-xhci.pdf (дата обращения: 18.11.2020).

21. Устройство файла UEFI BIOS, часть полуторная: UEFI Platform Initialization [Электронный ресурс]. URL: https://habr.com/ru/post/185764/ (дата обращения: 18.11.2020).

22. *Елькин В. М.* Контроль недоверенного процессора: Мат. XXIII Научно-практической конференции "Комплексная защита информации". Суздаль, 22—24 мая 2018 г. — М.: Медиа Групп "Авангард", 2018. С. 209—211.

23. System Management Mode Hacks [Электронный ресурс]. URL: http://phrack.org/issues/65/7.html (дата обращения: 18.11.2020).

24. Использование Intel Processor Trace для трассировки кода System Management Mode [Электронный ресурс]. URL: https://habr.com/ru/company/dsec/blog/481692/ (дата обращения: 18.11.2020).

25. Advanced x86: Introduction to BIOS & SMM. SMI Suppression [Электронный ресурс]. URL: https://opensecuritytraining.info/IntroBIOS.html (дата обращения: 18.11.2020).

26. *Ziarnik G. P., Durham M. R., Piwonka M. A.* Pattern № US9483426B2, United States (US). Locking a system management interrupt (SMI) enable register of a chipset. Application № US14/364,706. PCT Filed 31.01.2012. PCT № PCT/US2012/023225. PCT Date 12.06.2014; Publication Date 01.11.2016. Assignee: Hewlett-Packard Development Company, L.P.

SMM technology and its application in computer security

M. V. Pakhomov
Moscow Institute of Physics and Technology (National Research University),
Dolgoprudny, Moscow region, Russia

System Management Mode (SMM) is a highly privileged mode on most x86 computers, and there are many ways to exploit this mode to attack devices. In this article, the correct configuration of the mode is described, possible security functions using SMM are identified, and the pros and cons of using the technology for security are indicated. The result of the work was the analysis and assessment of the feasibility of using the technology in computer security.

Keywords: System Management Mode, System Management Interruption, information security tool, computer security, SMI_EN register, protection rings, code execution mode, x86 architecture.

Bibliography — 26 references. *Received October 18, 2021*

УДК 004.056
DOI: 10.52190/2073-2600_2021_4_20

Rule-based (RBR) метод корреляции событий безопасности в рамках шаблона взаимодействия "брокеры сообщений"

[1] *П. А. Иванов*; [1, 2] *И. В. Капгер*, канд. техн. наук
[1] ФГБОУ ВО «Национальный исследовательский университет «МЭИ», Москва, Россия
[2] ФГБОУ ВО «Пермский национальный исследовательский политехнический университет», г. Пермь, Россия

Рассматривается подход к использованию метода корреляции событий безопасности, предназначенный для выявления инцидентов безопасности при взаимодействиях устройств в системах, построенных с использованием шаблона "брокеры сообщений". Особенностью подхода является разбиение процесса корреляции на подпроцессы в целях упрощения нахождения взаимосвязанных событий.

Ключевые слова: кибербезопасность, мониторинг безопасности, корреляция событий, Интернет вещей, брокеры сообщений.

Для систем, в рамках которых регистрируется большое количество данных, требующих корреляционного анализа, процесс корреляции может потребовать обработки и накопления значительных массивов событий, получаемых от объектов мониторинга. Подобная ситуация характерна для систем, включающих большое количество узлов сети или узлов, отправляющих данные с высокой частотой, например системы в концепции Интернета вещей.

Различные подходы к корреляции событий объединяет разбиение процесса на этапы, включающие первичную обработку получаемых данных, процессы их нормализации и анализа, а также постобработку полученных результатов [1].

Объектом рассмотрения является система, интеграционные взаимодействия в которой построены на базе шаблона "брокеры сообщений". Данный шаблон подразумевает наличие компонента, выполняющего роль интеграционного сервера, обеспечивающего передачу сообщений между подключенными к нему устройствами.

Сбор данных для корреляционного анализа может осуществляться как на самом брокере сообщений, так и на узловых устройствах, участвующих в процессе взаимодействия. Оптимальной точкой сбора будет именно брокер, поскольку он выступает интеграционной компонентой для всех взаимодействий.

Иванов Павел Алексеевич, магистр.
E-mail: pashaivan17@gmail.com
Капгер Игорь Владимирович, доцент кафедры "Безопасность и информационные технологии", доцент кафедры "Автоматика и телемеханика".
E-mail: Kapger@mail.ru

Статья поступила в редакцию 9 июля 2021 г.

Основной проблемой при корреляции большого количества событий является сложность выявления взаимосвязанных событий, имеющих отношение к безопасности, из общего потока событий для обработки и анализа. Угроза безопасности может быть выявлена как на основании нескольких простых событий, так и на основании множества событий, имеющих разный характер и происходящих в разные временные промежутки.

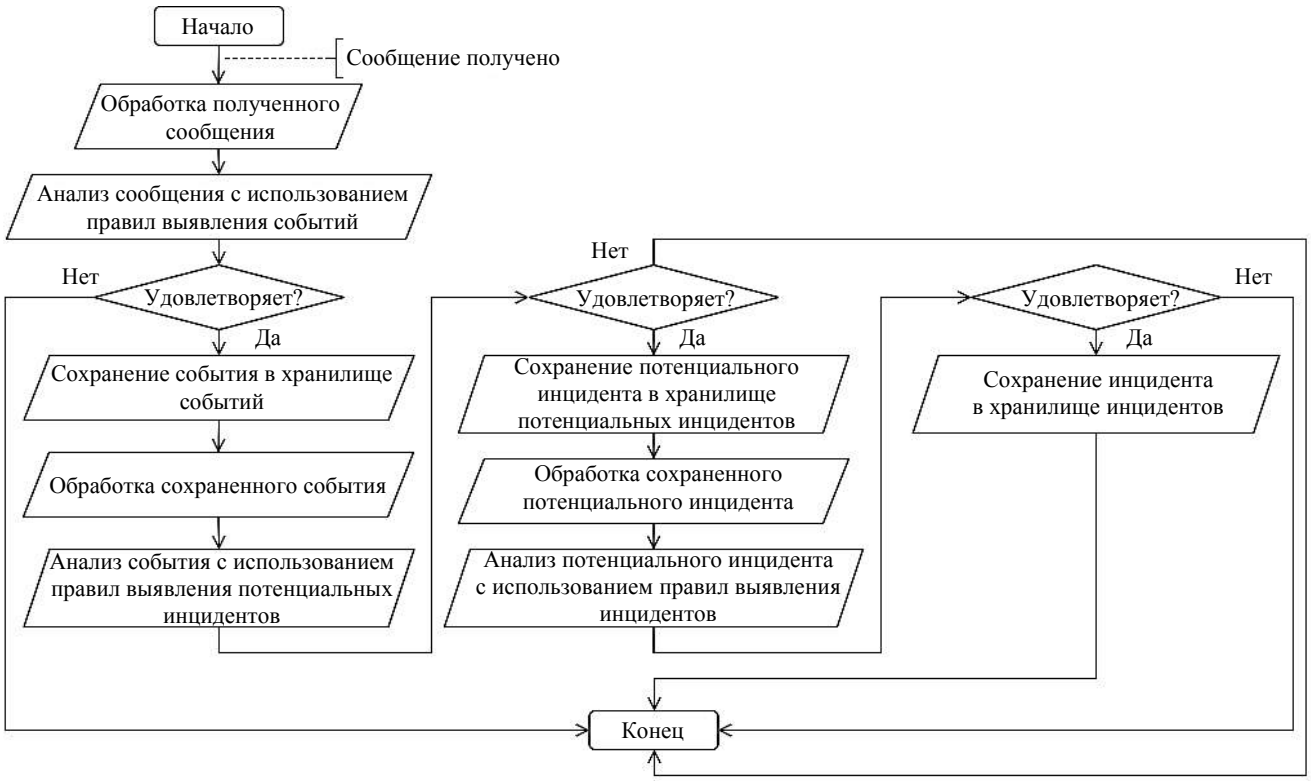
Для решения данной проблемы предлагается разбиение процесса корреляции на подпроцессы, что позволит упростить корреляционный анализ и избежать накопления избыточного количества событий, требующихся для выявления угроз.

В целях выявления взаимосвязей между событиями используются различные сигнатурные и бессигнатурные методы корреляции. В сфере информационной безопасности наиболее распространенным и эффективным является метод корреляции на основе правил (Rule-based, RBR). Данный метод наиболее эффективен при обнаружении угроз. Он используется в подавляющем большинстве систем мониторинга и выявления инцидентов безопасности [2].

Корреляция на основании правил подразумевает, что правило содержит в себе условия, при соблюдении которых можно говорить о положительном коэффициенте корреляции между событиями. При этом большее количество условий (либо их комплексность) прямо пропорционально величине коэффициента корреляции.

Корреляция событий в целях выявления инцидента безопасности как факта, подтверждающего угрозу безопасности, разбивается на несколько процессов (этапов) (см. рисунок) для выявления:

- события безопасности;
- потенциального инцидента безопасности;
- инцидента безопасности.



Порядок выполнения этапов корреляционного анализа

Данная логика подразумевает последовательное выделение событий, имеющих отношение к безопасности, из общего количества событий. Разбиение процесса корреляции в данном случае предполагает и проработку соответствующих групп правил.

Собранные данные, прошедшие процесс нормализации (приведения к формату, позволяющему произвести корреляционный анализ), анализируются с использованием правил выявления событий безопасности. Данные правила подразумевают несколько условий, при совпадении с которыми простое событие следует отнести к событию безопасности. В случае выявления совпадения с данными правилами регистрируется событие безопасности, которое перемещается в выделенную область хранилища.

В следующем подпроцессе корреляции исходными данными для анализа являются эти события безопасности, которые анализируются на предмет соответствия правилам выявления потенциальных инцидентов безопасности. В случае выявления совпадения с данными правилами регистрируется потенциальный инцидент безопасности, который перемещается в выделенную область хранилища.

В последнем подпроцессе корреляции исходными данными для анализа являются потенциальные инциденты безопасности, которые анализируются на предмет соответствия правилам выявления инцидентов безопасности (или подтвержденных инцидентов), по результатам чего выявленные инциденты перемещаются в соответствующую им область хранилища.

Каждое сохраненное и классифицированное в рамках подпроцессов событие (инцидент) может быть приоритезировано в зависимости от его характеристик.

Предложенная градация является условной. При необходимости процесс может быть разбит на большее или меньшее количество подпроцессов. Степень дробления зависит от характера данных, поступающих от устройств. Об угрозе безопасности может свидетельствовать, например, значительный уход значений определенного показателя за пределы разумного. В таком случае будет достаточно первого этапа корреляции, на котором будет зафиксировано отклонение данного показателя. Если эта угроза может быть выявлена на основании ухода значений нескольких показателей, требуется второй этап корреляции, в рамках которого будут использоваться результаты первого этапа. Если эта угроза характеризуется ещё и многократными попытками передать управляющий сигнал на другое устройство, требуется третий этап корреляции, в рамках которого все факторы будут выявлены исходя из результатов анализа, полученных на предыдущих этапах.

Зависимость между случайными событиями имеет функциональный характер, т. е. является строго функциональным отношением, связывающим содержание этих событий. Появление собы-

тия *X*, которое функционально приводит к появлению события *Y*, говорит о положительной корреляции данных событий и, соответственно, об угрозе информационной безопасности. Чем больше событий функционально зависят от других событий, тем больше их коэффициент корреляции [3]. В данном случае можно говорить о том, что вероятность обнаружения угрозы безопасности пропорционально зависит от величины коэффициента корреляции.

Корреляция на основании правил подразумевает, что правило содержит условия, при соблюдении которых можно говорить о положительном коэффициенте корреляции между событиями *X* и *Y*. При этом увеличение количества условий (либо их комплексности) приводит к увеличению коэффициента корреляции. Количество или комплексность условий зависит от угроз, описываемых данными правилами.

Предложенный подход за счёт разбиения процесса корреляции позволит получить величину коэффициента корреляции на основании большого числа условий и при этом нескольких независимых подпроцессов анализа. Это как увеличит эффективность процесса, так и позволит избежать значительного количества ложных срабатываний, поскольку каждый инцидент будет подкреплен суммой коэффициентов корреляции, определенных при срабатывании суммы условий в рамках нескольких проверок.

Литература

1. *Федорченко А. В., Левшун Д. С., Чечулин А. А., Котенко И. В.* Анализ методов корреляции событий безопасности в SIEM-системах. Ч. 1 // Труды СПИИРАН. 2016. Вып. 47. С. 5—27.

2. Корреляция SIEM — это просто. Сигнатурные методы [Электронный ресурс]. SecurityLab. URL: https://www.securitylab.ru/analytics/431459.php (дата доступа: 10.04.2021).

3. *Харченко М. А.* Корреляционный анализ: учеб. пособие для вузов. — Воронеж: Изд-во ВГУ, 2008. — 31 с.

Rule-based (RBR) event correlation method to "message broker" interaction pattern

[1] *P. A. Ivanov,* [1, 2] *I. V. Kapger*
[1] Moscow Power Engineering Institute (MPEI), Moscow, Russia
[2] State National Research Politechnical University of Perm, Perm, Russia

This article describes an approach to using the Rule-based (RBR) correlation method of security events intended for security incident detection in systems that based on a "security broker" interaction pattern. A feature of the approach is a process fragmentation into subprocesses to simplify the security analysis.

Keywords: cybersecurity, cybersecurity monitoring, event correlation, Internet of Things, message broker.

Bibliography — 3 references. *Received July 9, 2021*

УДК 519.24; 53; 57.017
DOI: 10.52190/2073-2600_2021_4_23

Преобразователь образов голосовых паролей дикторов в криптографический ключ на основе комитета предварительно обученных сверточных нейронных сетей

А. Е. Сулавко, канд. техн. наук; *Д. П. Иниватов; Д. Г. Стадников, А. Г. Чобан*
ФГБОУ ВО «Омский государственный технический университет», г. Омск, Россия

Разработан метод преобразования голосового пароля в длинный криптографический ключ или сильный пароль для надежной биометрической аутентификации диктора. Предложен новый способ ансамблирования классификаторов, который может быть использован в целях снижения количества ошибок распознавания образов, в том числе совместно с такими методами, как бэггинг, бустинг, стекинг. Пять предварительно обученных многослойных сверточных нейронных сетей объединены в комитет. Каждая сеть обучалась на усредненных спектрах голосовых образов, вычисляемых при помощи быстрого оконного преобразования Фурье с использованием различных оконных функций (прямоугольной, Барлетта, Гаусса, Блэкмана, Хемминга). Сети извлекали векторы признаков голосовых паролей, которые поступали на вход нейросетевому преобразователю биометрия—код, обученному по алгоритму ГОСТ Р 52633.5. Достигнутый уровень ошибок составил EER = 0,0144.

Ключевые слова: многослойные нейронные сети, глубокое обучение, ансамбли моделей, автоматическое обучение нейронных сетей, параметры голоса диктора, автокодировщики, ядро свертки, биометрическая аутентификация.

Общество стоит на пороге цифровой революции. Цифровизация происходит повсеместно и касается почти всех сфер деятельности. Закрепляются тренды, связанные с глобализацией технологий удаленного доступа (телемедицина, дистанционное обучение). Все больше профессий принимает характер удаленной работы. В такой информационной среде крайне важно доказать аутентичность виртуального образа удаленного пользователя (работника, партнера, студента).

С учетом событий, связанных с пандемией вируса COVID-19, предпочтительными становятся методы бесконтактной аутентификации. Однако эффективность методов распознавания лиц в условиях масочного режима резко снижается. Традиционные средства аутентификации также не в полной мере удовлетворяют современного потребителя: они либо контактные (как отпечаток пальца или пин-код), либо подвержены "человеческому фактору" (пароль можно забыть, ненамеренно скомпрометировать).

Сулавко Алексей Евгеньевич, доцент, старший научный сотрудник.
E-mail: sulavich@mail.ru
Иниватов Даниил Павлович, аспирант.
E-mail: sulavich@mail.ru
Стадников Денис Геннадьевич, магистрант.
E-mail: sdg250598@inbox.ru
Чобан Адиль Гаврилович, магистрант.
E-mail: adil_choban@mail.ru

Статья поступила в редакцию 25 ноября 2021 г.

Один из вариантов решения проблемы надежной бесконтактной аутентификации основан на использовании голосовых параметров диктора.

Голосовой пароль можно привязать к бесконтактной смарт-карте, на которой в защищенном виде будет храниться длинный криптографический ключ или сильный пароль (для аутентификации), привязанный к голосовым параметрам владельца. Потеря карты не приведет к компрометации голосового пароля, а компрометация голосового пароля (например, при скрытой записи на диктофон) — к компрометации криптографического ключа, размещенного на карте. При этом голосовой пароль может быть изменен пользователем в любой момент.

Исследование посвящено разработке метода преобразования голосового пароля в длинный криптографический ключ или сильный пароль для надежной биометрической аутентификации диктора. Разработанный метод основан на применении аппарата искусственных нейронных сетей. Также в работе предлагается новый способ ансамблирования моделей, который может быть использован в целях снижения количества ошибок распознавания образов, в том числе совместно с такими методами, как бэггинг (бутстрэп-агрегирование), бустинг, стекинг.

Предобработка голосовых образов

Любой биометрический образ предварительно обрабатывается для устранения незначимой информации и повышения отношения сигнал/шум.

Далее из образа извлекаются признаки — биометрические параметры, которые должны содержать информацию, пригодную для идентификации (верификации) личности человека. Распознавание биометрического образа выполняется в определенном пространстве признаков, которое задается при обучении классификатора. Все образы должны иметь единый формат при поступлении на вход классификатора (в виде вектора признаков определенной длины).

По сути, этап предварительной обработки (предобработки) можно назвать ортогонализацией образа. Назовем промежуточное представление образа, полученное после предобработки, но еще не являющееся вектором признаков, *репрезентацией* образа.

Применительно к голосовым паролям ортогонализация часто выполняется с помощью быстрого преобразования Фурье (БПФ). Однако БПФ имеет недостатки: ограниченная информативность анализа нестационарных (и квазистационарных) сигналов, проявление эффекта Гиббса, "размазывание" особенностей сигналов (разрывов, ступенек, пиков и т. п.) по всему частотному диапазону спектра (появляются "паразитные" высокочастотные составляющие, явно отсутствующие в исходном сигнале при наличии в нём скачков и разрывов). Из-за указанных недостатков амплитудный спектр звукового сигнала обычно не используется непосредственно в качестве вектора признаков.

Для выявления локальных особенностей нестационарных и квазистационарных сигналов часто применяется быстрое оконное преобразование Фурье (Short-time Fourier transform, STFT). Фурье-спектрограммы могут использоваться в качестве репрезентаций голосовых образов и подаваться на вход глубоким сверточным нейронным сетям для извлечения из них биометрических признаков. Такая практика широко применяется [1]. Вейвлет-преобразования дают лучшее разрешение по времени на низких частотах и по частоте на высоких [2], но тем не менее редко используются в биометрических системах из соображений производительности.

Как правило, чем больше размерность входных данных, тем больший объем выборки требуется для обучения многослойной нейронной сети. Поэтому в настоящей работе вместо спектрограмм использован усредненный по всем окнам амплитудный спектр (рис. 1). В усредненном спектре информация о локальных особенностях сигнала интегрируется, а случайные выбросы частично сглаживаются. Интегральный спектр голосового сигнала зависит от голоса диктора и речевого сообщения (рис. 2). Таким образом, если один и тот же диктор произносит определенный голосовой пароль, то усреднённые спектры звуковых сигналов оказываются схожими. В любом другом случае усредненные спектры имеют существенные отличия.

В настоящем исследовании использовалось пять типов окон: прямоугольное, треугольное (окно Барлетта), окна Гаусса, Блэкмана и Хемминга. Данные оконные функции имеют существенные отличия, чем и обусловлен выбор. Из рис. 2, *в* видно, что для одного и того же примера голосового пароля диктора усредненные спектры, полученные с помощью разных оконных функций, отличаются.

Таким образом, усредненные спектры на базе различных окон можно рассматривать как репрезентации образа, из которых могут быть получены признаки, дополняющие друг друга.

Безусловно, спектры голосовых сигналов от разных оконных функций в определенной степени коррелируют (для разных испытуемых по-разному). Однако связь далеко не функциональна (в среднем коэффициент корреляции колеблется от 0,3 до 0,9). Поэтому разные репрезентации одних и тех же образов *могут использоваться для обучения различных классификаторов*, которые могут быть объединены в комитет. Архитектура классификаторов может быть идентичной (например, в качестве базового классификатора можно взять "наивного" Байеса), а может и кардинально отличаться от других. Эффект от такого объединения схож с эффектом, получаемым при бутстрэп-агрегировании (когда каждый классификатор обучается на разных подмножествах обучающей выборки, что приводит к улучшению стабильности и точности алгоритмов машинного обучения и помогает избежать переобучения). Однако *предложенный подход позволяет использовать все обучающие примеры для настройки классификаторов*. Это полезно, если обучающая выборка ограничена в объеме (что особенно актуально для приложений биометрии).

Идея создания комитетов (ансамблей) классификаторов основана на теореме Кондорсе. Если решения классификаторов независимы и вероятность правильного решения каждого из них больше 0,5, то с увеличением их количества вероятность правильного решения комитета возрастает и стремится к единице. Чем ниже доля ошибок для каждого классификатора в отдельности, тем ниже доля ошибок для комитета. Чем ниже коррелированность решений классификаторов, тем больший синергетический эффект можно получить (интенсивнее снижается количество ошибок при комплексировании).

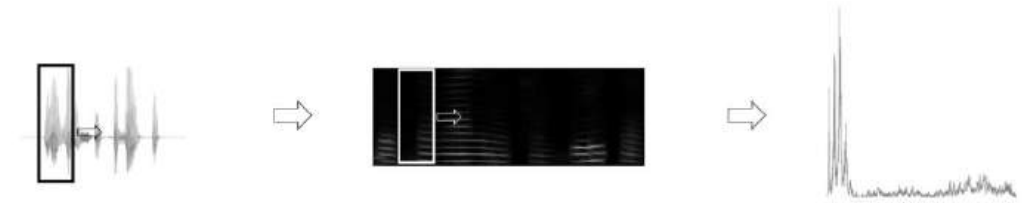
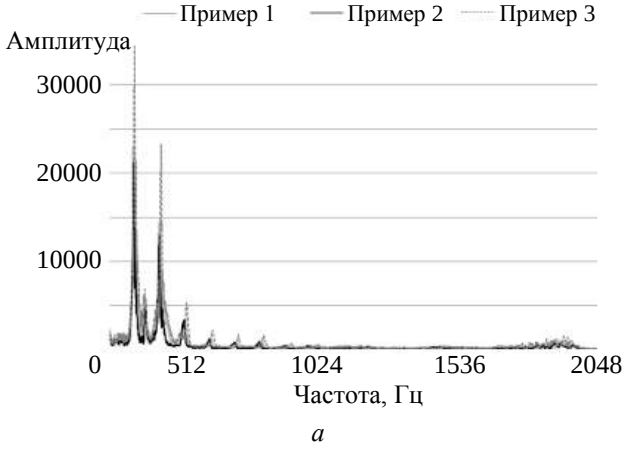
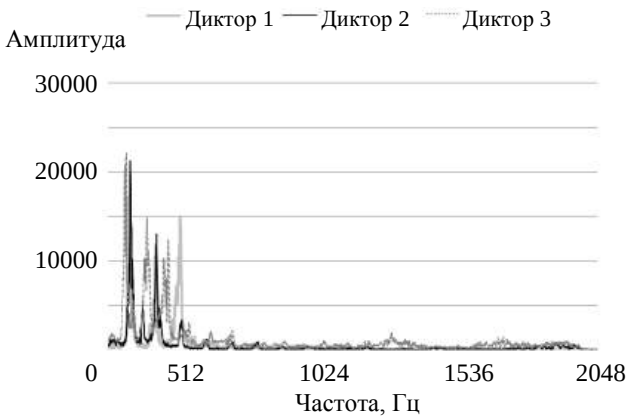


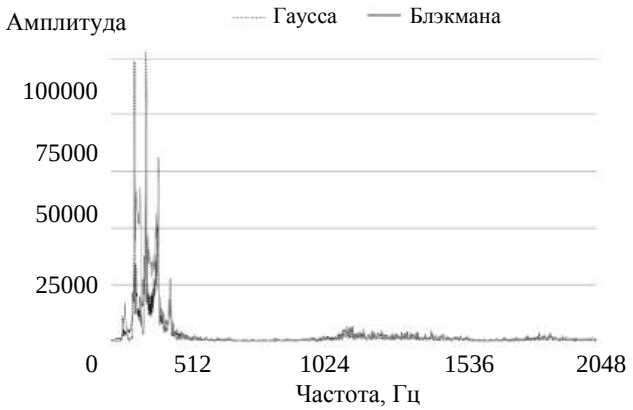
Рис. 1. Построение усредненного амплитудного спектра голосового пароля



а



б



в

Рис. 2. Усредненные спектры голосовых сигналов (размер окна 0,5 с):
а — один диктор и пароль (прямоугольное окно);
б — разные дикторы и пароли (прямоугольное окно);
в — один диктор, один пример пароля, разные типы окон

Преобразование голосового пароля в длинный криптографический ключ или сильный пароль с помощью нейронных сетей

Преобразование биометрического образа в бинарную последовательность возможно на базе двух принципиально разных подходов: "нечеткий экстрактор" и искусственные нейронные сети. Нечеткие экстракторы основаны на квантовании "сырых" (или предобработанных) биометрических данных и применении кодов, исправляющих ошибки, для корректировки нестабильных разрядов в бинарном представлении биометрического образа. По результатам проведенных ранее исследований этот подход [3] значительно уступает нейронным сетям [4] по вероятностям ошибок. Использование нечетких экстракторов для генерации ключей шифрования на основе голосовых паролей непродуктивно, так как число нестабильных бит в речевом сигнале (спектре или спектрограмме) значительно (такой подход дает очень высокий средний процент ошибок — порядка 20 % [5]).

Нейросетевой преобразователь "биометрия-код" (НПБК) представляет собой искусственную нейронную сеть, которая обучается для того, чтобы вырабатывать криптографический ключ или сильный пароль при поступлении на ее входы биометрического образа пользователя. Количество входов этой нейронной сети равно числу признаков, а количество выходов — длине личного клю-

ча (пароля). НПБК строится персонально для каждого пользователя и обучается на примерах его биометрических образов ("Свой"), а также примерах образов, не принадлежащих данному пользователю ("Чужие"). Чтобы на практике НПБК мог функционировать, алгоритм его обучения должен быть полностью автоматическим и гарантировано приводить к полной настройке (без тупиков и зацикливания).

Когда на вход НПБК поступает образ "Свой", на выходе НПБК должен возникать ключ (пароль) пользователя (владельца НПБК). Когда на вход НПБК поступает биометрический образ любого другого субъекта (в том числе злоумышленника), на выходе НПБК должна возникать почти случайная последовательность бит. Чтобы на выходе нейронной сети появлялся бинарный вектор, требуется, чтобы каждый нейрон последнего слоя имел пороговую функцию активации Хевисайда. Функция активации в скрытых слоях гипотетически может быть любой.

Построение НПБК с большим количеством бинарных выходов на базе многослойных нейронных сетей затруднительно. Как правило, в классических нейронных сетях, ориентированных на классификацию образов, количество выходных состояний связано с числом классов образов. Если следовать этой логике, то при длине ключа (пароля) пользователя, равной 256 бит (такие требования предъявляются к ключам электронной подписи в ГОСТ Р 34.10-2012), количество классов нейронной сети должно составлять $2^{256} \approx 1{,}158 \cdot 10^{77}$.

Чем ниже качество биометрического образа, тем больший объем выборки требуется для обучения многослойной нейронной сети. В задачах биометрической аутентификации объем выборки, как правило, ограничен 10—20 примерами (пользователя нельзя заставлять слишком много раз повторять голосовой пароль при регистрации). При этом информативность образов голоса значительно ниже, чем, например, отпечатка пальца, лица [6]. Поэтому даже сеть с одним бинарным выходом не всегда возможно обучить на 20 примерах образов "Свой" (все зависит от качества голосовых образов конкретного пользователя).

Из-за высокой сложности автоматизации процесса обучения многослойных нейронных сетей НПБК принято строить на базе однослойных или двухслойных персептронов и обучать их без применения алгоритмов, основанных на градиентном спуске. Такой подход заложен в ГОСТ Р 52633.5.

В настоящей работе предложено комплексировать многослойные сверточные нейронные сети и классический НПБК, что позволяет повысить точность распознавания диктора и преобразования голосового пароля в ключ (пароль). Комплексирование выполнялось по принципу *стекинга* — использования сверточных сетей для выработки признаков для НПБК.

В состав НПБК можно включить предварительно обученные глубокие сети со специальной архитектурой. *Автокодировщик* — это глубокая сверточная нейронная сеть, которая обучается на больших объемах данных (рис. 3). Архитектура автокодировщика такова, что он способен находить закономерности в произвольных данных и извлекать информативные признаки. Далее эти признаки могут быть поданы на вход НПБК, который обучается в соответствии с принципами, изложенными в ГОСТ Р 52633.5.

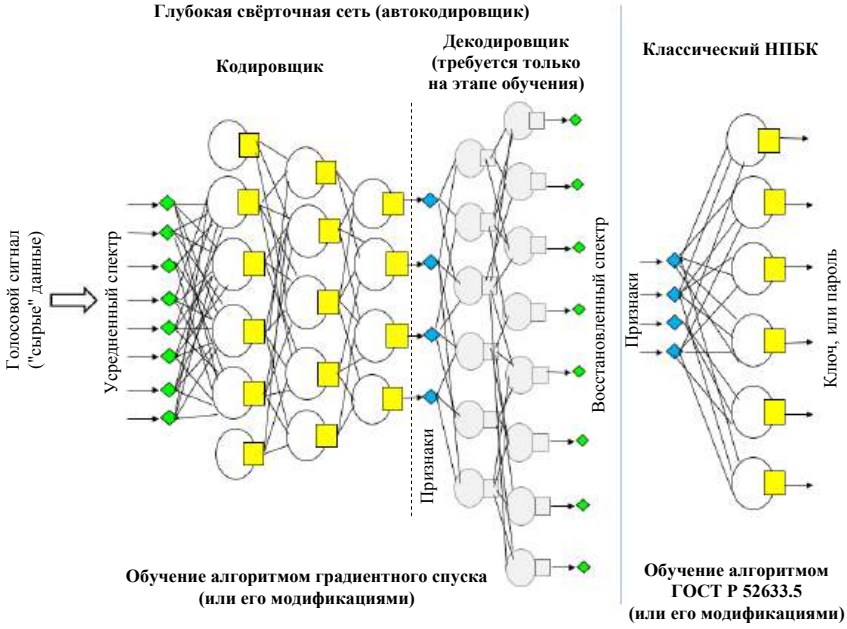


Рис. 3. Структурная схема предложенной модели классификатора, объединяющей сверточную сеть и классический НПБК

Автокодировщик состоит из *кодировщика* (преимущественно сверточные слои (ConvL), которые сжимают входные данные до более компактного описания) и *декодировщика* (преимущественно транспонированные сверточные слои (TConvL), которые восстанавливают данные). Размерность входного слоя должна соответствовать размерности выходного, а скрытые слои имеют меньшую размерность. Данное свойство автокодировщика позволяет выделять наиболее информативные признаки образа и одновременно снижать размерность пространства признаков (хотя могут использоваться и расширяющиеся архитектуры). Во время обучения на вход и выход сети подается усредненный спектр голосового пароля. После обучения декодировщик необходимо удалить (в противном случае злоумышленник может использовать его для восстановления исходных данных биометрического образа из компактного описания).

В качестве выходов обученной нейронной сети принимаются выходы нейронов последнего слоя *кодировщика*. Значения этих выходов можно рассматривать как вектор биометрических признаков, извлекаемых из голосового образа.

Архитектура сверточной нейронной сети для извлечения признаков голосового пароля

Количество слоев нейронных сетей обычно стараются повысить, а число признаков сократить. Чем больше размерность входных данных, тем большим количеством параметров должна обладать сеть, способная эффективно их обработать. Нейронные сети с большим числом параметров потенциально могут дать более высокую точность решений, но при этом возрастает объем обучающей выборки. Построение оптимальной архитектуры — это поиск компромисса между размерностью входа, объемом сети и объемом обучающей выборки.

Эффективность различных моделей нейронных сетей тестируется на специально организованных соревнованиях. В 2014 г. в рамках конкурса ImageNet Challenge 2014 (ILSVRC-2014) была предложена архитектура глубокой сверточной сети VGG16, описанная в работе [7]. Проведено исследование влияния глубины свёрточной сети на её точность в задаче распознавания больших изображений. Основным результатом является тщательная оценка возможностей сетей с очень маленькими сверточными фильтрами. Показано, что можно добиться существенного улучшения точности распознавания, увеличив глубину до 16—19 весовых слоев. Эти выводы легли в основу представленного на конкурсе результата, где команда авторов работы [7] заняла призовые места. Доказано, что полученные результаты хорошо обобщаются на другие наборы данных.

В настоящем исследовании архитектура VGG16 использовалась как основа для разработки автокодировщика, которая была скорректирована с учетом специфики поставленных задач (анализ голосовых паролей). Прежде всего, для анализа звуковых файлов требуется использовать *одномерные свертки* вместо двухмерных, ориентированных на изображения. Было сформировано множество архитектур, производных от VGG16 (с измененным количеством слоев, функциями активации на некоторых слоях, параметрами ядер свертки). Для каждой архитектуры выполнялось обучение. В процессе обучения контролировалось качество восстановления входного вектора на различных эпохах, а также анализировались такие параметры, как информативность признаков скрытого описания и их взаимная коррелированность. Под информативностью признака понимается площадь пересечения функций плотности вероятности его значений для классов образов "Свой" и "Чужие". Чем меньше площадь пересечения этих функций, тем более информативен признак с точки зрения верификации идентификации личности. Подробнее с методикой оценки информативности признаков можно ознакомиться в работе [8]. Сети обучались до тех пор, пока не происходило переобучение. Наилучшие результаты (по точности восстановления, наиболее высокой средней информативности признаков и низкой коррелированности признаков) получены при использовании архитектуры, описанной в табл. 1.

Объем обучающей выборки для автокодировщиков составлял 2250 примеров (670 дикторов). Использовался алгоритм оптимизации градиентного спуска Adam (Adaptive Moment Estimation). В качестве функции ошибки применялась бинарная кросс-энтропия.

Размерность 128 на выходе кодировщика означает, что он способен извлекать 128 признаков. При этом бóльшая часть пар признаков (около 70 %) имеет парные коэффициенты корреляции менее 0,3 по модулю. При увеличении количества выходов кодировщика (признаков) их коррелированность возрастает, а средняя информативность снижается.

Таблица 1

Архитектура перспективного автокодировщика для извлечения признаков из голосовых спектров

Тип слоя	Параметры слоя
Кодировщик	
Входной	Размерность 2048
ConvL (1D)	Число фильтров 4; окно свёртки 12; шаг свёртки 4
ConvL (1D)	Число фильтров 8; окно — 3; шаг — 2
Пакетная нормализация	
ConvL (1D)	Число фильтров 8; окно — 4; шаг — 2
ConvL (1D)	Число фильтров 16; окно — 3; шаг — 2
Пакетная нормализация	
ConvL (1D)	Число фильтров 16; окно — 3; шаг — 2
ConvL (1D)	Число фильтров 32; окно — 3; шаг — 2
Пакетная нормализация	
ConvL (1D)	Число фильтров 32; окно — 3; шаг — 2
ConvL (1D)	Число фильтров 32; окно — 3; шаг — 2
Пакетная нормализация	
ConvL (1D)	Число фильтров 64; окно — 3; шаг — 2
ConvL (1D)	Число фильтров 128; окно — 3; шаг — 2
Полносвязный слой	Число нейронов 128; функция активации линейная
Декодировщик	
Входной	Размерность 128
TConvL (1D)	Число фильтров 128; окно — 8; шаг — 4
TConvL (1D)	Число фильтров 64; окно — 3; шаг — 2
Пакетная нормализация	
TConvL (1D)	Число фильтров 32; окно — 5; шаг — 2
TConvL (1D)	Число фильтров 16; окно — 3; шаг — 2
Пакетная нормализация	
TConvL (1D)	Число фильтров 16; окно — 3; шаг — 2
TConvL (1D)	Число фильтров 8; окно — 3; шаг — 2
Пакетная нормализация	
TConvL (1D)	Число фильтров 4; окно — 3; шаг — 2
TConvL (1D)	Число фильтров 4; окно — 3; шаг — 2
Пакетная нормализация	
TConvL (1D)	Число фильтров 2; окно — 3; шаг — 2
TConvL (1D)	Число фильтров 1; окно — 3; шаг — 2

Комитет предварительно обученных сверточных нейронных сетей

Предлагается способ ансамблирования нескольких предварительно обученных сверточных нейронных сетей, которые обучаются на разных репрезентациях биометрических образов. Сформировано 5 автокодировщиков с идентичной архитектурой, представленной в табл. 1. Каждый автокодировщик ориентирован на извлечение признаков из спектров, получаемых с использованием определённой оконной функции (прямоугольное, Барлетта, Гаусса, Блэкмана или Хемминга). Все автокодировщики обучались по идентичной схеме (500 эпох, оптимизатор Adam, функция ошибки — бинарная кросс-энтропия) на основе единой обучающей выборки (из 2250 примеров). Однако при обучении каждого из них использовались усредненные спектры, вычисленные с учетом различных окон.

При аутентификации голосовой пароль преобразуется сразу в пять спектров, каждый из которых поступает на вход соответствующему кодировщику, вычисляющему вектор признаков. Далее векторы признаков объединяются и поступают на вход НПБК, который преобразует объединенный вектор в личный ключ или пароль пользователя (рис. 4).

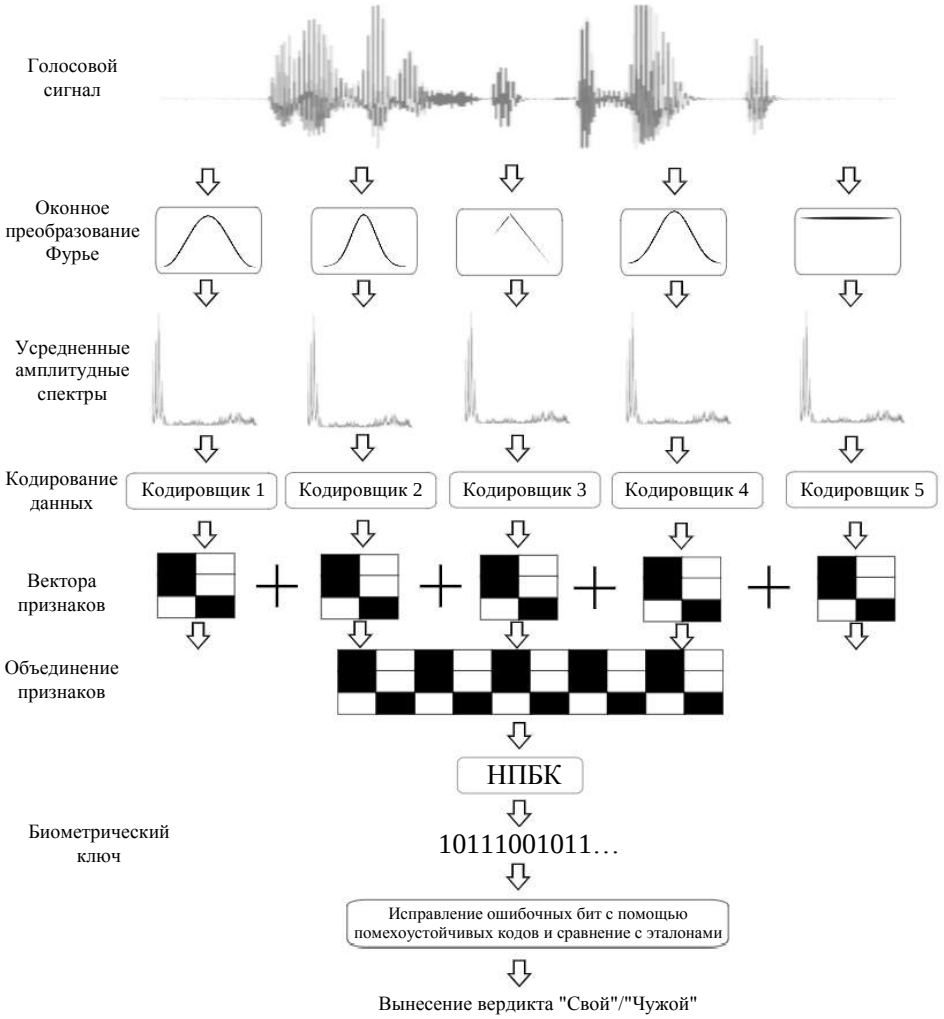


Рис. 4. Схема процесса аутентификации (извлечения ключа) на основе комитета сверточных сетей и НПБК

В общем случае разные репрезентации образа могут быть получены путем применения к "сырому" (необработанному) биометрическому образу нескольких методик обработки, отличающихся реализацией какого-либо нелинейного преобразования. Например, аналогично можно комплексировать сети, обучаемые на вейвлет-спектрограммах с применением различных базисных функций. Создавать ансамбли моделей на основе разных репрезентаций образа имеет смысл, если они имеют некоррелируемые отличия.

Нейросетевой преобразователь "биометрия—код"

Рассмотрим НПБК на базе однослойного персептрона.

Классический нейрон базируется на функционале и пороговой функции активации:

$$y = \sum_{j=1}^{n} \mu_j a_j; \qquad (1)$$

$$f(y) = \begin{cases} 0, \text{ если } y \le \mu_0; \\ 1, \text{ если } y > \mu_0. \end{cases} \qquad (2)$$

При обучении НПБК номера связанных с нейроном признаков определяют случайно, избегая повторного вхождения признаков в нейрон. Модули весов нейронов первого слоя вычисляют по формуле [9]

$$\mu_j = \left| m_s(a_j) - m_0(a_j) \right| / \sigma_s(a_j)\sigma_0(a_j). \qquad (3)$$

В приведенных формулах y — отклик нейрона на образ "Свой" или "Чужой"; $f(y)$ — ответ нейрона; a_j — значение j-го признака (входа нейрона); $m_0(a_j)$ и $\sigma_0(a_j)$ — математическое ожидание и среднеквадратичное отклонение значений j-го признака для образа "Свой"; $m_s(a_j)$ и $\sigma_s(a_j)$ — аналогичные показатели образов для "Чужих"; μ_0 — порог активации нейрона; n — количество входов нейрона. Если нейрон настроен на выход 1 при поступлении образа "Свой", то знак весового ко-

эффициента выбирается исходя из следующего правила: "+" при $m_s(a_j) < m_0(a_j)$, иначе "–". Если нейрон настраивается на нулевой бит, то знаки инвертируются.

Пороги нейронов (или нулевые веса) μ_0 настраиваются исходя из откликов y на примеры "Свой", не использовавшиеся при вычислении весов:

$$\mu_0 = m_0(y) - \sigma_0(y)\alpha.$$

После обучения параметры $m_0(a_j)$, $\sigma_0(a_j)$, $m_s(a_j)$, $\sigma_s(a_j)$ удаляются, чтобы не компрометировать эталон. Остаются таблицы связей и весов μ, которые называют *нейросетевым контейнером*.

После обучения ответ НПБК складывается из битовых значений на выходах нейронов (путем их конкатенации).

Обучающие и тестовые выборки

В соответствии с ГОСТ Р 52633.5 для обучения НПБК требуется не менее 10 примеров "Свой" и 64 независимых примера "Чужие" (от разных субъектов). Образы "Свой" — это голосовые пароли, воспроизведенные легитимным пользователем, который создает и обучает НПБК. Образы "Чужие" — это голосовые пароли (фразы), воспроизведенные другими людьми. Тестовая и обучающая выборки не должны пересекаться.

Кроме того, требуется обучить автокодировщики. *Обучающая выборка автокодировщиков не должна пересекаться с обучающими и тестовыми примерами образов "Свой", подготовленными для НПБК.* При этом каждый автокодировщик может обучаться на одной и той же выборке, но с разными параметрами предобработки (разными окнами).

В рамках настоящего исследования использовали набор данных голосовых паролей из работы [4], который включал:

- голосовые образы 160 дикторов (пол и возраст распределены равномерно от 18 до 35 лет). Каждый диктор воспроизвёл определенный голосовой пароль 80 раз. Образы паролей собраны в два этапа с интервалом в несколько недель. Данные 140 дикторов использовали при обучении и тестировании преобразователей "биометрия—код". Для построения каждого НПБК использовано по 15 примеров "Свой" и 139 примеров "Чужой" (каждый из испытуемых является "Чужим" по отношению ко всем остальным). Образы остальных 20 испытуемых (1600 примеров) использовали для обучения автокодировщиков;
- примеры других 650 голосовых паролей, воспроизведенных другими субъектами (от каждого диктора по одному примеру). Эти данные в основном взяты из открытых источников (в частности, из базы VoxForge [http://www.voxforge.org]). Они использовались в качестве тестовой выборки "Чужие" при оценке надежности НПБК и для обучения автокодировщиков, что вполне допустимо (так как тестовая и обучающая выборки НПБК не пересекались).

Объемы выборок составили:

– обучающая выборка автокодировщиков — 2250 (1600 + 650);

– обучающие выборки "Свой" и "Чужие" для каждого НПБК — 15 и 139 примеров соответственно;

– общий объем тестовых выборок "Свой" и "Чужие" (количество опытов для оценки FRR и FAR) — 9100 и 91000 примеров, соответственно.

Все звуковые файлы имели частоту дискретизации 8 кГц и один канал (моно).

Типы ошибочных решений преобразователя "биометрия—код"

Существуют два показателя в биометрических системах, которые определяют надежность защиты: вероятности ошибок ложного отказа (FRR) и ложного допуска (FAR). Биометрические системы обычно сравниваются по коэффициенту равной вероятности ошибок EER (при FRR ≈ FAR) или по средней точности MAC = 1 – (FRR + FAR)/2. Однако на практике показатели FRR и FAR должны быть сбалансированы (FAR стараются сделать как можно меньше, FRR может достигать 20—25 %). Для этого нужно задать *порог принятия*, который определяет допустимое количество ошибочных бит в ответе ПБК (бит, не совпадающих с соответствующими битами ключа или пароля легитимного пользователя). В реальной практике для установки ненулевого порога требуется дополнительно корректировать ответ ПБК, например с помощью кодов, исправляющих ошибки, и хранить синдромы ошибок. *Нулевой порог* означает, что система принимает ответ как правильный, только если он строго равен ключу пользователя (расстояние Хемминга между ответом НПБК и ключом равно нулю).

Для определения FRR требуется провести опыты с тестовыми образами легитимного пользователя ("Свой"), для определения FAR — с тестовыми образами нарушителей ("Чужих"). Показатели FRR и FAR измеряются процентом или вероятностью, которую можно вычислить статистически как отношение количества ошибок к числу соответствующих опытов.

Результаты эксперимента

В рамках эксперимента проводилось тестирование моделей классификаторов при различных параметрах НПБК (количество нейронов и их входов) при использовании как одного кодировщика, так и всех сразу (рис. 4).

Повышение числа выходов НПБК L приводит к уменьшению вероятностей ошибок (табл. 2). Однако темп роста качества решений постепенно снижается и почти останавливается. Дальше повышать количество нейронов в НПБК не имеет смысла. В рассматриваемой задаче при $L > 1024$ вероятность ошибок снижается незначительно, кроме случая использования комитета сверточных сетей. Чем больше входов у нейронов, тем больше корреляция между выходами НПБК и, соответственно, выше EER. Слишком малое количество входов ($n < 5$) делает нейроны неэффективными и ослабляет защиту эталона от компрометации.

Из табл. 2 видно, что при использовании комитета сверточных сетей коэффициент равной вероятности ошибок снижается по сравнению с использованием только одной наиболее сильной сети (соответствующей треугольному окну). Даже относительно слабые кодировщики способны снижать вероятность ошибок комитета (табл. 2). Эффект увеличения надежности решений при комплексировании сетей не очень значителен, однако он присутствует. Данные для сравнения полученного результата с достигнутыми ранее представлены в табл. 3.

Таблица 2

Результаты тестирования НПБК

Тип окна (кодировщика)	n	L	EER
Прямоугольное	10	128	0,017
Прямоугольное	10	256	0,0163
Прямоугольное	10	512	0,0168
Прямоугольное	10	1024	0,0169
Прямоугольное	10	2048	0,0170
Прямоугольное	5	512	0,0151
Прямоугольное	5	1024	0,0150
Прямоугольное	5	2048	0,015
Прямоугольное	2	1024	0,0183
Барлетта (треугольное)	5	512	0,0141
Барлетта (треугольное)	**5**	**1024**	**0,0131**
Барлетта (треугольное)	5	2048	0,0131
Блэкмана	5	512	0,0204
Блэкмана	5	1024	0,0201
Блэкмана	5	2048	0,0244
Хемминга	5	512	0,0245
Хемминга	5	1024	0,0234
Хемминга	5	2048	0,023
Гаусса	5	512	0,0319
Гаусса	5	1024	0,029
Гаусса	5	2048	0,0291
Комитет (5 кодировщиков)	5	512	0,0132
Комитет (5 кодировщиков)	5	1024	0,0128
Комитет (5 кодировщиков)	**5**	**2048**	**0,0124**

Таблица 3

Достигнутые показатели надежности для методов распознавания дикторов

Метод	FRR	FAR	EER
Метод, разработанный в ЦРТ (обобщённый метод моментов + машина опорных векторов + совместный факторный анализ + вариационный байесовский анализ) [10]			0,022
Нечеткий экстрактор [5]			0,2
Сверточные нейронные сети (с 3D-свертками) [11]			0,211
Сверточные нейронные сети [1]			0,03
Сверточные нейронные сети [12]			0,105
Гибкие нейронные сети [4]	0,245	<0,0001	
Предложенный метод (комитет сверточных сетей + НПБК)	0,088	<0,0001	0,0124

Лучший из полученных результатов иллюстрирует рис. 5. Видно, что вероятности ошибок FRR и FAR могут быть сбалансированы посредством изменения порога принятия — допустимого количества ошибочных бит в ответе НПБК (не совпадающих с соответствующими битами ключа/пароля пользователя). Например, при FAR < 10^{-4} показатель FRR = 0,148, что гораздо ниже, чем при использовании НПБК, но без обработки образов сверточными сетями (FRR = 0,245).

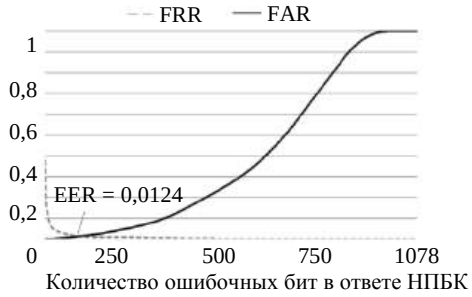


Рис. 5. Вероятности ошибок аутентификации (преобразования образа в ключ) в зависимости от порога (при использовании комитета из пяти сверточных сетей)

На практике для корректировки ошибочных разрядов ответа НПБК могут применяться коды, исправляющие ошибки (в частности, предложенные в работе [13]). Это необходимо для того, чтобы не хранить ключ (пароль) пользователя в явном виде.

Разработанный метод дает низкий процент ошибочных решений, а также потенциально высокую защищенность биометрического эталона и ключа пользователя при хранении. Чтобы восстановить голосовой пароль субъекта в исходном виде требуется:

- взломать НПБК, что даст доступ к вектору признаков (компактному описанию образа). Принципы построения машин по извлечению знаний из НПБК и методы защиты нейросетевых контейнеров описаны в [4, 9];
- восстановить по вектору признаков усредненный спектр, что затруднительно при условии, что декодировщик удален после обучения автокодировщика;
- восстановить по усредненному спектру голосовой сигнал, что не представляется возможным, так как данные об изменении речевого сигнала с течением времени усреднены (обратное преобразование Фурье может дать лишь фрагментарную информацию).

Заключение

Разработан метод преобразования голосового пароля в длинный криптографический ключ или сильный пароль для надежной биометрической аутентификации диктора. Предложен новый способ ансамблирования классификаторов (в частности, сверточных нейронных сетей), основанный на обучении каждого классификатора на разных репрезентациях биометрических образов. Разные репрезентации образа могут быть получены путем применения к "сырому" биометрическому образу нескольких методик обработки, отличающихся реализацией какого-либо нелинейного преобразования. В настоящей работе объединено пять автокодировщиков, каждый из которых обучался на усредненных спектрах голосовых образов, вычисляемых при помощи STFT с использованием различных оконных функций (прямоугольной, Барлетта, Гаусса, Блэкмана, Хемминга). Каждый автокодировщик извлекал из усредненного спектра вектор из 128 признаков. Далее эти векторы объединялись и поступали на вход нейросетевому преобразователю "биометрия—код", обучаемому по алгоритму ГОСТ Р 52633.5.

Полученный результат говорит о работоспособности предложенного способа создания ансамблей моделей. Его можно использовать отдельно или совместно с другими методами ансамблирования (бэггинг, бустинг, стекинг). Таким образом, при распознавании голосовых паролей нет смысла в поиске наиболее подходящей оконной функции для более точного представления амплитудно-частотных характеристик сигнала. Следует использовать как можно больше окон для получения разных репрезентаций голосового образа, каждая из которых содержит долю новой информации.

Также можно утверждать, что признаки, извлекаемые из голосовых паролей при помощи предварительно обученных сверточных нейронных сетей, весьма информативны (что позволяет повысить надежность решений при биометрической аутентификации). Сверточные нейронные сети можно эффективно комплексировать с другими классификаторами, обучение которых более устойчиво на малых выборках биометрических образов.

Достигнутый уровень ошибок аутентификации по голосовому паролю составил EER = 0,0124 (для моносигнала с частотой дискретизации 8 кГц), систему можно настроить, например, на FRR = 0,088 при FAR < 10^{-4}. При наличии обучающей выборки большего объема с более высоким уровнем репрезентативности вместо усредненного спектра можно задействовать спектрограммы. В этом случае синергетический эффект от объединения сверточных нейронных сетей должен быть более показательным.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ), проект № 6.

Литература

1. *Yanick Lukic, Carlo Vogt, Oliver D¨urr, Thilo Stadelmann.* Speaker identification and clustering using convolutional neural networks: IEEE 26th In-ternational Workshop on Machine Learning for Signal Processing (MLSP). SALERNO, ITALY. 13—16 September 2016.
2. *Горшков Ю. Г.* Обработка речевых и акустических биомедицинских сигналов на основе вейвлетов. Монография. — М.: Радиотехника, 2017. — 240 с.
3. *Сулавко А. Е., Еременко А. В., Борисов Р. В.* Генерация криптографических ключей на основе голосовых сообщений // Прикладная информатика. 2016. № 5. С. 76—89.
4. *Сулавко А. Е.* Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей // Компьютерная оптика. 2020. Т. 44. № 1. С. 82—91. DOI: 10.18287/2412-6179-CO-567.
5. *Monrose F., Reiter M. K., Li Q., Wetzel S.* Cryptographic key generation from voice: Proceedings of the 2001 IEEE Symposium on Security and Privacy, 2001.
6. *Ложников П. С.* Биометрическая защита гибридного документооборота. — Новосибирск: Изд-во СО РАН, 2017. — 130 с.
7. *Simonyan K., Zisserman A.* Very deep convolutional networks for large-scale image recognition [Электронный ресурс]. Режим доступа: arXiv preprint arXiv:1409.1556, 2014.
8. *Sulavko A. E., Zhumazhanova S. S., Fofanov G. A.* Perspective Neural Network Algorithms for Dynamic Biometric Pattern Recognition in the Space of Interdependent Features: 2018 Dynamics of Systems, Mechanisms and Machines, Dynamics. 13—15 November, 2018. — Omsk, Russia. P. 1—12. DOI: 10.25206/2310-9793-2018-6-4-130-145.
9. *Ахметов Б. С., Иванов А. И., Фунтиков В. А., Безяев А. В., Малыгина Е. А.* Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа. — Алматы: ТОО "ИздательствоLEM", 2014. — 144 с.
10. *Матвеев Ю. Н.* Технологии биометрической идентификации личности по голосу и другим модальностям // Вестник МГТУ им. Н. Э. Баумана. Сер. "Приборостроение". 2012. № 3(3). С. 46—61.
11. *Amirsina Torfi, Jeremy Dawson, Nasser M. Nasrabadi.* Text-independent speaker verification using 3d convolutional neural networks: IEEE In-ternational Conference on Multimedia and Expo (ICME). 23—27 July 2018.
12. *Hossein Salehghaffari.* Speaker Verification using Convolutional Neural Networks [Электронный ресурс]. Режим доступа: arXiv:1803.05427v2 [eess.AS]
13. *Безяев А. В., Иванов А. И., Фунтикова Ю. В.* Оптимизация структуры самокорректирующегося биокода, хранящего синдромы ошибок в виде фрагментов хеш-функций // Вестник УрФО. Безопасность в информационной сфере. 2014. № 3(13). С. 4—13.

Transformer of voice passwords of speakers into a cryptographic key based on a committee of pretrained convolutional neural networks

A. E. Sulavko, D. P. Inivatov, D. G. Stadnikov, A. G. Choban
Omsk State Technical University, Omsk, Russia

A method has been developed for converting a voice password into a long cryptographic key or a strong password for reliable biometric authentication. A new method of ensemble of classifiers is proposed, which can be used to reduce the number of pattern recognition errors, including in conjunction with methods such as bagging, boosting, and stacking. Five pre-trained multilayer convolutional neural networks are combined into a committee. Each network was trained on the average spectra of voice images calculated using the fast window Fourier transform using various window functions (rectangular, Barlett, Gauss, Blackman, Hamming). The networks extracted voice password feature vectors that were input to the perceptron based converter "biometrics to code", trained according to the GOST R 52633.5 algorithm. The achieved error level was EER = 0.0144.

Keywords: multilayer neural networks, deep learning, ensembles of models, automatic learning of neural networks, speaker voice parameters, auto-encoders, convolution core, biometric authentication.

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

УДК 004.75
DOI: 10.52190/2073-2600_2021_4_34

К вопросу актуальности создания доверенной среды для разграничения доступа к информации в облачных сервисах в рамках цифровизации современного образования

Е. Ю. Лушпа, канд. техн. наук
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Проведено изучение основных аспектов, касающихся создания доверенной среды в рамках современного цифрового образования. Акцентируется внимание на создании доверенной среды именно для разграничения доступа к информации, находящейся в облачных сервисах. Осуществлена одна из первых попыток исследования вопроса, связывающего создание доверенной среды в облачных сервисах, используемых современными образовательными порталами.

Ключевые слова: доверенная среда, информационная безопасность, разграничение доступа, облачные сервисы, цифровизация.

Основная проблематика представленной статьи заключается в низком уровне обеспечения информационной безопасности такого немаловажного и одного из наиболее актуальных сегментов современной жизнедеятельности человека, как цифровое образование. Тема цифровизации образования приобретает колоссальную актуальность, что вызвано множеством сопутствующих этому факторов. Одними из наиболее востребованных средств, используемых при реализации дистанционного образования, являются Web-технологии и сервисы.

Таким образом, происходит быстрый рост инфокоммуникационных технологий (ИКТ). Вместе с ними развиваются и средства информатизации образования. На данном этапе требуется предусмотреть проблемы, которые могут возникнуть при таком развитии, и принять системные меры для их предотвращения. В связи с этим органам управления образованием важно не только обеспечивать построение необходимой инфраструктуры (каналов связи, серверов, пользовательской аппаратуры), но и уделять как можно больше внимания содержательной части инфокоммуникационных образовательных услуг. Автором более подробно рассматривается вопрос, касающийся аспекта обеспечения высокого уровня информационной безопасности, что может быть достигнуто посредством разработки доверенной среды для разграничения доступа к информации в облачных сервисах.

Используются теоретические и эмпирические методы исследования. В целях получения более подробной информации и актуальных данных к работе привлечены научные исследования отечественного и зарубежного авторства. В результате использованы научные материалы таких авторов, как Маркин Д. О., Макеев С. М., Умбетов Т. К., Воронин А. А., Parashchuk I. B., Saenko I. B., Pantyukhin O. I., Movsesyan V. E. и другие. В каждой из данных работ затрагиваются фундаментальные вопросы, необходимые для воспроизведения общего анализа, касающегося обеспечения информационной безопасности посредством разработки и интеграции доверенной среды.

Таким образом, в используемой автором литературе раскрываются такие вопросы, как исследование уязвимостей доверенной среды исполнения приложении на основе технологии, разработка программного обеспечения, реализующего сервисы безопасности на основе средства доверенной загрузки и технологии, концепция доверенной передачи данных и другие.

Актуализируемая роль информационной безопасности в рамках развивающегося цифрового образования и Web-технологий

Информационные продукты являются основой в работе информационных технологий (ИТ). Именно посредством информации организовывается система последовательных операций в целях

Лушпа Евгений Юрьевич, доцент, профессор кафедры РВСН ВУЦ.
E-mail: euglushpa@list.ru

Статья поступила в редакцию 24 сентября 2021 г.

использования ресурсов и методов автоматизации различных процессов. Необходимо отметить, что существует множество подходов относительно проблемы классификации информационных технологий. Несмотря на всю распространенность, термин "информация" остается одним из самых обсуждаемых понятий в науке, а сам термин имеет множество различных значений в разных отраслях деятельности человека. В мире прослеживается колоссальная актуальность развития и использования Интернета и информационных технологий на всех уровнях жизнедеятельности современного человека. Образовательная сфера, в частности дистанционное образование, является одним из основных направлений, в котором активно интегрируются и распространяются информационные технологии.

Таким образом, посредством развития средств коммуникации наметился повышенный интерес к различного рода методам дистанционного обучения и цифровизации образования в целом. Одним из примеров преимуществ цифровизации образования является то, что обучаемому нет необходимости затрачивать свое время на перемещение к месту занятий, а сам урок можно начинать и проводить в любое удобное для него время. В настоящее время учебные и педагогические процессы частично или полностью реализуются посредством использования различных средств информационных технологий, а также переходят на дистанционную форму обучения посредством интеграции различных Web-технологий [1].

Актуальность развития и внедрения цифровых технологий в образовании заключается в перспективных возможностях, связанных с повышением качества и эффективности современного образовательного процесса. Стремительное развитие информационного общества, проявление и широкое распространение технологий мультимедиа, электронных информационных ресурсов, сетевых технологий позволяют использовать информационные технологии в качестве средства обучения, общения, воспитания, интеграции в мировое пространство. Совокупность традиционных и информационных направлений внедрения информационной технологии создает предпосылки для реализации новой интегрированной концепции применения ИТ в образовании.

Основанные на облачных вычислениях технологии являются одними из самых инновационных и востребованных продуктов в современном образовательном процессе. Облачные технологии являются средствами, предназначенными для хранения и обработки информации посредством объединения в себе аппаратных средств, каналов связи, а также иную техническую поддержку пользователей. Процесс работы в данных технологиях преследует цель понижения расходов, а также повышения эффективности учебной деятельности современной образовательной системы. Основная концепция облачных технологий заключается в предоставлении пользователю хостинга, имеющего удаленный доступ к услугам, вычислительным ресурсам и интернет-приложениям. Исходя из этого каждый из участников образовательного процесса получает возможность колоссально снизить расходы, направленные на инфраструктуру современных ИТ, а также оперативно реагировать на изменения и развитие вычислительных потребностей с помощью облачных сервисов.

Продолжая изучение актуальности, необходимо рассмотреть функциональные особенности Web-сервисов. Так, к примеру, в аспекте технической реализации для систем облачных вычислений характерно использование средств виртуализации, обеспечивающих возможность самообслуживания потребителей и динамической масштабируемости вычислительных ресурсов. Использование средств виртуализации приводит к появлению дополнительных лиц и факторов, воздействующих на системы облачных вычислений и являющихся источниками угроз информационной безопасности, специфическими для технологии облачных вычислений. Так, сбои в работе средств виртуализации могут привести к нарушению изоляции и потере обрабатываемой информации, а уязвимости системы управления виртуальной средой создают возможность для несанкционированного доступа к вычислительным ресурсам или данным со стороны других потребителей системы облачных вычислений.

Универсальность доступа к информационным сервисам по каналам информационно-телекоммуникационных сетей расширяет круг возможных сценариев реализации угроз информационной безопасности со стороны пользователей информационно-телекоммуникационных сетей. В то же время данная особенность систем облачных вычислений подразумевает перенос процессов обработки информации в защищенные и отказоустойчивые центры обработки данных провайдера, что значительно снижает вероятность реализации угроз информационной безопасности посредством физического доступа к компонентам системы облачных вычислений и сокращает потери от реализации угроз. Так, к примеру, к следствиям недостаточного уровня информационной безопасности образовательной среды в Web-сервисах можно отнести: несанкционированный доступ к порталу; хищение персональных данных обучаю-

щихся и преподавателей; подмену информации; кражу интеллектуальной собственности; направление пользователей посредством незаконно размещенной рекламы на различные онлайн-сервисы, казино, игры и другое.

Актуальность создания доверенной среды в облачных сервисах, используемых во время образовательного процесса

Как было указано ранее, существует целый класс проблем, которые могут возникнуть при использовании Web-ресурсов во время обучения. В первую очередь необходимо предотвратить нецелевое использование ресурсов, затрачиваемых на построение инфраструктуры, необходимой для информатизации образования. Как известно, доступность развитых инфокоммуникационных технологий (ИКТ) не является достаточным условием успешного решения задач, для которых эти технологии внедряются. Как показывает практика, если процесс развития массовых ИКТ не контролируется, основная часть возникающих возможностей используется не для решения социальных задач, а для предоставления услуг развлекательного характера. Согласно прогнозам, к 2022 г. следует ожидать, что доля информации, передаваемой пользователями в онлайн-играх, по отношению к общему трафику увеличится более чем в 2 раза. Очевидно, что среди детской и подростковой аудитории этот эффект будет выражаться еще сильнее. В связи с этим без средств контроля и ограничений создаваемые в процессе информатизации возможности будут использоваться неэффективно [2].

К проблеме нецелевого использования ресурсов относится также наблюдаемое явление увеличения количества передаваемых данных в расчете на одну оказанную услугу. Стремительное развитие ИКТ часто дает иллюзию неограниченной емкости каналов связи, в результате чего вместе с действительно необходимой информацией передается большое количество данных, несущих рекламную или декоративную функцию (например, баннеры или многочисленные элементы графического оформления веб-страниц). По этой причине лишь малая часть передаваемого трафика несет полезную нагрузку.

Также возникающей проблемой является риск уменьшения качества получаемого образования. ИКТ потенциально позволяют предоставить учащимся доступ к огромному количеству информации по самым разным предметам. Однако это является преимуществом только в случае, если учащийся уже имеет какие-либо систематические знания в данной предметной области. Кроме того, в этом случае он должен обладать развитыми навыками поиска нужных данных из разнородных источников. В противном случае у учащегося не будет сформировано целостное представление об изучаемом предмете. В связи с этим имеет смысл предоставлять доступ к большим базам знаний только на высших ступенях обучения, а также для учебно-методического персонала. Для школьного обучения, по мнению автора, вместо практикуемого сейчас свободного доступа к Интернету целесообразнее развивать специальные системы, позволяющие использовать ограниченное количество учебных пособий, соответствующих комплексному плану обучения.

Таким образом, одним из наиболее эффективных решений, способствующих устранению данной проблемы, является создание доверенной среды в облачных сервисах, используемых во время образовательного процесса. Именно посредством данной технологии предоставляется возможность снизить количество хакерских угроз, а также уменьшить влияние кибератак практически до нуля [3].

Организация доверенной среды для разграничения доступа к информации в облачных образовательных сервисах

При организации информационной защиты облачных инфраструктур от несанкционированного доступа необходимо организовать пространство для надежного и безопасного функционирования этих технологий: создать доверенную среду (доверенную вычислительную или программно-аппаратную). В рамках понятия "доверенности" предполагается, что есть некий объект — система или процесс (среда, окружение, платформа, сеанс, загрузка), в поведении которых пользователь облачных технологий полностью уверен. Это объект, которому пользователь может доверять на сто процентов. Ожидаемое поведение данного объекта всегда совпадает с реальным. Доверенная система облачных технологий — система, которая использует доверенные аппаратные и программные средства для разграничения привилегий абонентов облачных инфраструктур и обеспечения одновременной обработки информации разных категорий секретности группой пользователей без нарушения прав доступа [4].

Основываясь на изложенной информации, можно сформулировать понятие "доверенная среда" (доверенная вычислительная или программно-аппаратная среда) облачных технологий. Это вза-

имоувязанная по времени и задачам совокупность систем и средств разграничения доступа, идентификации и аутентификации, межсетевых экранов, средств антивирусной защиты и криптографических стандартов. Она отвечает политике безопасности и создает защищенное "облачное пространство". Для формирования такой среды необходимо выполнение двух основных условий: вся аппаратная часть облачных инфраструктур должна быть полностью досконально проверена и перепроверена или создана самостоятельно на отечественной элементной базе; все программные средства, созданные для работы на этом оборудовании, должны быть написаны самостоятельно либо тщательно, детально и "придирчиво" проверены.

Исходя из всего этого необходимо отметить, что доверенная среда облачных инфраструктур — некое информационно-техническое, киберфизическое пространство, сформированное на основе комплекса технических и организационных мер и способное обеспечить его участникам предсказуемый и безопасный результат информационного взаимодействия. Важно, что при этом степень доверенности среды определяется надежностью циркулирующего в ней и предоставляемого ею контента.

В качестве доверенного окружения для облачных инфраструктур обычно понимают взаимосвязанную совокупность доверенных средств связи (стационарных и мобильных), доверенных механизмов сетевой безопасности, доверенных платформ визуализации и виртуализации, доверенных алгоритмов аутентификации пользователей, средств (оборудования) обеспечения этой безопасности, доверенных механизмов и средств облачных вычислений и хранения данных, доверенных программных средств и программных приложений (операционных систем, библиотек, Web-сервисов и т. д.

Создание "доверенной платформы" образовательного процесса для облачных инфраструктур заключается в использовании отечественных комплексов оборудования для обеспечения устойчивости критически важных информационных систем и защиты информации. При этом принято считать, что составными частями доверенной платформы могут выступать аппаратное обеспечение, программное обеспечение и элементная база. Поэтому задача, стоящая перед создателями доверенной платформы для облачных инфраструктур, состоит в обеспечении отечественных организаций и предприятий аппаратными и программными средствами, которые гарантируют защищенность и отсутствие недокументированных (незадекларированных) возможностей внутри оборудования и программного обеспечения облачных технологий [5].

Заключение

Таким образом, в данной работе был рассмотрен вопрос, касающийся изучения основных аспектов создания доверенной среды в рамках современного цифрового образования. Изучены такие аспекты, как роль информационной безопасности в рамках развивающегося цифрового образования и Web-технологий, *актуальность создания доверенной среды в облачных сервисах*, используемых во время образовательного процесса, организация доверенной среды для разграничения доступа к информации в облачных образовательных сервисах.

В заключение необходимо отметить, что роль комплексов, модулей и иных средств доверенной загрузки в разграничении доступа и в обеспечении информационной безопасности облачных технологий достаточно велика и потенциал их применения объективно возрастает. Это системы, позволяющие без больших финансовых затрат, оперативно и гарантированно предотвращать несанкционированный доступ к программным и техническим ресурсам средств сбора, обработки, хранения и передачи информации в облачных инфраструктурах [6].

Литература

1. *Маркин Д. О., Чунг Х. Т.* Исследование уязвимостей доверенной среды исполнения приложений на основе технологии TRUSTZONE // Изв. ТулГУ. Технические науки. 2020. Вып. 9. С. 316—328.
2. *Маркин Д. О., Макеев С. М., Умбетов Т. К.* Технологическая карта по разработке программного обеспечения, реализующего сервисы безопасности на основе средства доверенной загрузки и технологии // Ученые записки ОГУ. Сер. "Гуманитарные и социальные науки". 2021. № 1. С. 199—204.
3. *Воронин А. А.* Концепция доверенной передачи данных // Бюллетень науки и практики. 2021. Т. 7. № 7. С. 164—173.
4. *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. Doi: 10.24411/2409-5419-2018-10188.
5. *Братченко А. И., Бутусов И. В., Романов А. А.* О проблемах обеспечения технологической независимости предприятий оборонно-промышленного комплекса // Военная мысль. 2018. № 6. С. 25—35.
6. *Лошкарёв А. В., Мовсесян В. Э.* Правовые аспекты регулирования цифровой среды доверия // Международный журнал гуманитарных и естественных наук. 2020. № 9—2(48). С. 172—175.

On the issue of the relevance of creating a trusted environment for differentiating access to information in cloud services within the framework of digitalization of modern education

E. Yu. Lushpa
Moscow Aviation Institute (National Research University), Moscow, Russia

The main purpose of this article is to study the main aspects related to the creation of a trusted environment within the framework of modern digital education. The author focuses on creating a trusted environment specifically for delimiting access to information located in cloud services. This work has a significant scientific contribution, which is expressed in one of the first attempts to study the issue linking the creation of a trusted environment in cloud services used by modern educational portals.

Keywords: trusted environment, information security, access control, cloud services, digitalization.

Bibliography — 6 references. *Received September 24, 2021*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26
DOI: 10.52190/2073-2600_2021_4_39

О выборе алгебраического носителя схем цифровой подписи на некоммутативных алгебрах

А. Б. Левина, канд. физ.-мат. наук; *А. А. Молдовян,* д-р техн. наук
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»,
Санкт-Петербург, Россия

Вопрос изучения строения конечных некоммутативных ассоциативных алгебр рассмотрен как этап разработки алгоритмов цифровой подписи, основанных на скрытой задаче дискретного логарифмирования. Для конкретной шестимерной алгебры описан подход к изучению строения алгебр, содержащих множество глобальных односторонних единиц. Показана связь глобальных односторонних единиц с гомоморфными отображениями алгебры в подалгебру пониженной размерности. Наличие таких отображений может быть эффективно использовано для взлома криптосхем, заданных над алгебрами данного типа. Полученные результаты показывают, что в качестве алгебраического носителя целесообразно использовать шестимерные алгебры с глобальной двухсторонней единицей.

Ключевые слова: информационная безопасность, постквантовая криптография, цифровая подпись, конечная ассоциативная алгебра, некоммутативная алгебра, двухмерная цикличность группы.

Разработка постквантовых двухключевых криптосхем, в том числе алгоритмов электронной цифровой подписи (ЭЦП), рассматривается как один из актуальных вызовов в области криптографии [1]. Одним из значительных событий в этой области является проведение Национальным институтом стандартов и технологий США (НИСТ) мирового конкурса, в рамках которого были рассмотрены и проанализированы 69 различных кандидатов на постквантовые стандарты на двухключевые криптосхемы [2]. Завершены три этапа конкурса, и сформулированы промежуточные итоги [3—5], один из которых состоит в том, что НИСТ расширяет свой конкурс в номинации алгоритмов ЭЦП и предлагает разработчикам дополнительно представить к рассмотрению постквантовые схемы ЭЦП, использующие другие механизмы по сравнению с механизмами, использованными в изначально представленных алгоритмах цифровой подписи [6].

В качестве примитива алгоритмов ЭЦП, использующих новые механизмы, может быть рассмотрена скрытая задача дискретного логарифмирования (СЗДЛ), различные формы которой представлены в работах [7—9]. В качестве алгебраического носителя СЗДЛ используются конечные некоммутативные ассоциативные алгебры (КНАА). Перспективным приемом построения схем ЭЦП на КНАА является подход, использующий прием удвоения проверочного уравнения [10], существенно расширяющий возможности разработки криптосхем данного типа.

Одним из важных этапов разработки алгоритмов ЭЦП на основе СЗДЛ является изучение строения КНАА, используемых в качестве алгебраического носителя. Например, по результатам исследования строения четырехмерных алгебр с глобальной двухсторонней единицей установлены ограничения, связанные с нецелесообразностью использования необратимых алгебраических элементов при построении схем ЭЦП на четырехмерных КНАА [11,12]. При задании СЗДЛ с использованием необратимых элементов требуется выбор шестимерных КНАА [13] в качестве алгебраического носителя.

В ряде случаев в качестве алгебраического носителя используются КНАА, содержащие множество глобальных односторонних единиц. В настоящей статье детально рассматривается строение конкретной шестимерной КНАА, заданной над полем $GF(p)$ и содержащей p^3 глобальных односторонних единиц, и кратко приведены результаты изучения строения шестимерных КНАА, содер-

Левина Алла Борисовна, доцент.
E-mail: alla_levina@mail.ru
Молдовян Александр Андреевич, профессор.
E-mail: maa1305@yandex.ru

Статья поступила в редакцию 15 ноября 2021 г.

жащих p^2 и p^4 глобальных односторонних единиц. По полученным результатам сформулированы рекомендации по выбору алгебраического носителя.

Исследуемая алгебра

Способ задания КНАА как m-мерного векторного пространства, заданного над полем $GF(p)$, с дополнительно определенной операцией векторного умножения, достаточно детально описан в работах [14, 15], принятые в которых обозначения используются в данной статье. Рассмотрим шестимерную алгебру, заданную правилом умножения базисных векторов по табл. 1.

Таблица 1

Правило умножения базисных векторов для случая $m = 6$, задающее алгебру с p^3 глобальными левосторонними единицами

∘	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_5$
$\mathbf{e}_1$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_1$
$\mathbf{e}_2$	$\mathbf{e}_2$	$\mathbf{e}_5$	$\mathbf{e}_4$	$\mathbf{e}_1$	$\mathbf{e}_0$	$\mathbf{e}_3$
$\mathbf{e}_3$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_5$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_3$
$\mathbf{e}_4$	$\mathbf{e}_4$	$\mathbf{e}_3$	$\mathbf{e}_0$	$\mathbf{e}_5$	$\mathbf{e}_2$	$\mathbf{e}_1$
$\mathbf{e}_5$	$\lambda\mathbf{e}_0$	$\lambda\mathbf{e}_1$	$\lambda\mathbf{e}_2$	$\lambda\mathbf{e}_3$	$\lambda\mathbf{e}_4$	$\lambda\mathbf{e}_5$

Нахождение левосторонних единиц 6-мерной КНАА, задаваемой табл. 1, по векторному уравнению

$$\mathbf{X}\circ\mathbf{A} = \mathbf{A}, \tag{1}$$

в котором $\mathbf{A} = (a_0, a_1, a_2, a_3, a_4, a_5)$ и $\mathbf{X} = (x_0, x_1, x_2, x_3, x_4, x_5)$, приводит к решению следующей системы из шести линейных уравнений с неизвестными координатами вектора $\mathbf{X}$:

$$\begin{cases} x_0a_0 + \lambda x_1a_2 + x_2a_4 + \lambda x_3a_4 + x_4a_2 + \lambda x_5a_0 = a_0; \\ x_0a_1 + \lambda x_1a_5 + x_2a_3 + \lambda x_3a_3 + x_4a_5 + \lambda x_5a_1 = a_1; \\ x_0a_2 + \lambda x_1a_4 + x_2a_0 + \lambda x_3a_0 + x_4a_4 + \lambda x_5a_2 = a_2; \\ x_0a_3 + \lambda x_1a_1 + x_2a_5 + \lambda x_3a_5 + x_4a_1 + \lambda x_5a_3 = a_3; \\ x_0a_4 + \lambda x_1a_0 + x_2a_2 + \lambda x_3a_2 + x_4a_0 + \lambda x_5a_4 = a_4; \\ x_0a_5 + \lambda x_1a_3 + x_2a_1 + \lambda x_3a_1 + x_4a_3 + \lambda x_5a_5 = a_5. \end{cases} \tag{2}$$

Выделим в этой системе следующие две независимые системы из трех линейных уравнений:

$$\begin{cases} (x_0 + \lambda x_5)a_0 + (\lambda x_1 + x_4)a_2 + (x_2 + \lambda x_3)a_4 = a_0; \\ (x_2 + \lambda x_3)a_0 + (x_0 + \lambda x_5)a_2 + (\lambda x_1 + x_4)a_4 = a_2; \\ (\lambda x_1 + x_4)a_0 + (x_2 + \lambda x_3)a_2 + (x_0 + \lambda x_5)a_4 = a_4; \end{cases} \tag{3}$$

$$\begin{cases} (x_0 + \lambda x_5)a_0 + (\lambda x_1 + x_4)a_2 + (x_2 + \lambda x_3)a_4 = a_0; \\ (x_2 + \lambda x_3)a_0 + (x_0 + \lambda x_5)a_2 + (\lambda x_1 + x_4)a_4 = a_2; \\ (\lambda x_1 + x_4)a_0 + (x_2 + \lambda x_3)a_2 + (x_0 + \lambda x_5)a_4 = a_4. \end{cases} \tag{4}$$

Легко видеть, что решение систем (3) и (4) можно найти, выполнив замену переменных по формулам $z_1 = x_0 + \lambda x_5$, $z_2 = \lambda x_1 + x_4$, $z_3 = x_2 + \lambda x_3$. После такой замены переменных система (3) приобретает вид

$$\begin{cases} z_1a_0 + z_2a_2 + z_3a_4 = a_0; \\ z_3a_0 + z_1a_2 + z_2a_4 = a_2; \\ z_2a_0 + z_3a_2 + z_1a_4 = a_4; \end{cases} \tag{5}$$

$$\begin{cases} z_1a_1 + z_3a_3 + z_2a_5 = a_1; \\ z_2a_1 + z_1a_3 + z_3a_5 = a_3; \\ z_2a_1 + z_2a_3 + z_1a_5 = a_5. \end{cases} \tag{6}$$

Системы (5) и (6) имеют одинаковое решение в виде тройки значений $z_1 = 1$ и $z_2 = z_3 = 0$ для всех возможных значений вектора $\mathbf{A}$ (для малой доли элементов $\mathbf{A}$ алгебры имеется множество других решений, которые не рассматриваем).

Выполнение обратной замены переменных показывает, что исходная система (2) имеет решения, удовлетворяющие условиям $x_0 + \lambda x_5 = 1$, $\lambda x_1 + x_4 = 0$ и $x_2 + \lambda x_3 = 0$, из которых легко получаем формулу, описывающую множество p^3 глобальных левосторонних единиц $\mathbf{L} = (l_0, l_1, l_2, l_3, l_4, l_5)$:

$$\mathbf{L} = (1 - \lambda k,\ d,\ -\lambda h,\ h,\ -\lambda d,\ k), \tag{7}$$

где d, h и k принимают всевозможные тройки значений из множества $\{0, 1, \ldots, p-1\}$.

Правосторонние единицы, соответствующие вектору $\mathbf{A} = (a_0, a_1, a_2, a_3, a_4, a_5)$, удовлетворяют векторному уравнению

$$\mathbf{A}\circ\mathbf{X} = \mathbf{A}, \tag{8},$$

рассмотрение которого приводит к системе уравнений, представимой в виде двух независимых систем из трех линейных уравнений с тремя неизвестными в каждой из них:

$$\begin{cases} (a_0 + \lambda a_5)x_0 + (\lambda a_1 + a_4)x_2 + (a_2 + \lambda a_3)x_4 = a_0; \\ (a_2 + \lambda a_3)x_0 + (a_0 + \lambda a_5)x_2 + (\lambda a_1 + a_4)x_4 = a_2; \\ (\lambda a_1 + a_4)x_0 + (a_2 + \lambda a_3)x_2 + (a_0 + \lambda a_5)x_4 = a_4; \end{cases} \tag{9}$$

$$\begin{cases} (a_0 + \lambda a_5)x_1 + (a_2 + \lambda a_3)x_3 + (a_4 + \lambda a_1)x_5 = a_1; \\ (\lambda a_1 + a_4)x_1 + (a_0 + \lambda a_5)x_3 + (a_2 + \lambda a_3)x_5 = a_3; \\ (a_2 + \lambda a_3)x_1 + (\lambda a_1 + a_4)x_3 + (a_0 + \lambda a_5)x_5 = a_5. \end{cases} \tag{10}$$

Каждая из последних трех систем имеет одинаковый главный определитель вида

$$\Delta_{\mathbf{A}} = \beta_1^3 + \beta_2^3 + \beta_3^3 - 3\beta_1\beta_2\beta_3, \tag{11}$$

где

$$\beta_1 = a_0 + \lambda a_5,\ \beta_2 = \lambda a_1 + a_4 \text{ и } \beta_3 = a_2 + \lambda a_3. \tag{12}$$

При условии $\Delta_{\mathbf{A}} \neq 0$ вектору соответствует единственная локальная правосторонняя единица $\mathbf{R_A}$, координаты которой являются решениями систем (9), (10). Можно показать, что $\mathbf{R_A}$ содержится в множестве глобальных левосторонних единиц, т. е. $\mathbf{L_A}$ является одновременно и локальной двусторонней единицей $\mathbf{E_A}$ для вектора $\mathbf{A}$ и всевозможных его степеней. Относительно $\mathbf{E_A}$ вектор $\mathbf{A}$ является локально обратимым. Существенный интерес представляет вопрос о числе локально обратимых векторов в рассматриваемой КНАА. Это число можно найти, рассматривая число элементов $\mathbf{A}$, координаты которых с учетом (12) удовлетворяют условию

$$\Delta_{\mathrm{A}} = \beta_1^3 + \beta_2^3 + \beta_3^3 - 3\beta_1\beta_2\beta_3 = 0. \qquad (13)$$

Сначала найдем число различных троек значений β_1, β_2 и β_3, для которых выполняется последнее уравнение. Каждой такой тройке соответствует система из трех уравнений с 6 неизвестными: a_0, a_1, a_2, a_3, a_4, a_5, которая дает p^3 различных решений (различных необратимых векторов), т. е. число решений уравнения (13). Для некоторой фиксированной пары значений β_2 и β_3 из p^2 возможных вариантов имеем кубичное уравнение:

$$\beta_1^3 - (3\beta_2\beta_3)\beta_1 + \left(\beta_2^3 + \beta_3^3\right) = 0, \qquad (14)$$

заданное в конечном простом поле $GF(p)$ относительно неизвестного значения β_1. Вопрос о числе решений уравнений такого вида исследовался в работе [16]. Следует рассмотреть два случая: число 3 делит значение $p - 1$ и число 3 не делит значение $p - 1$.

Случай 1: $3|p - 1$, т. е. 3 делит число $p - 1$. Дискриминантом кубичного уравнения является значение

$$\mathrm{Dt} = \frac{\left(\beta_2^3 + \beta_3^3\right)^2}{4} + \frac{\left(-3\beta_2\beta_3\right)^3}{27} = \frac{\left(\beta_2^3 - \beta_3^3\right)^2}{4},$$

которое является квадратичным вычетом. В соответствии с результатами [16] при $\mathrm{Dt} = 0$ уравнение (14) имеет два корня при ненулевых значениях β_2 и β_3, что (с учетом наличия 3 кубичных корней из ненулевого значения) соответствует $3(p - 1)$ вариантам пар значений (β_2, β_3), т. е. этот случай дает $6(p - 1)$ различных троек $(\beta_1, \beta_2, \beta_3)$, удовлетворяющих уравнению (14). При $\mathrm{Dt} \neq 0$ уравнение (14) имеет три корня [16] при ненулевых значениях β_2 и β_3.

Число вариантов с ненулевым дискриминантом равно $p^2 - 3(p - 1) - 1$ (минус 1 учитывает случай $\beta_2 = 0$ и $\beta_3 = 0$). Получаем еще $3(p^2 - 3p + 2)$ пар значений (β_2, β_3), соответствующих необратимым векторам. Всего таких пар для рассматриваемого случая получаем $3(p^2 - 3p + 2) + 6(p - 1) + 1$ (плюс 1 учитывает случай $\beta_2 = 0$ и $\beta_3 = 0$, в котором $\beta_1 = 0$), т. е. $3p^2 - 3p + 1$ вариантов. После вычитания последнего значения из p^3 получим число различных троек $(\beta_1, \beta_2, \beta_3)$, удовлетворяющих неравенству $\Delta_{\mathbf{A}} \neq 0$, которое равно $(p - 1)^3$. С учетом связи значений β_1, β_2 и β_3 с координатами вектора $\mathbf{A}$ легко видеть, что каждая из указанных троек $(\beta_1, \beta_2, \beta_3)$ задает p^3 различных обратимых векторов, т.е. рассматриваемая шестимерная алгебра содержит $\Omega = p^3(p - 1)^3$ локально обратимых векторов в случае выполнения условия делимости $3|p - 1$.

Случай 2: число 3 не делит значение $p - 1$. В соответствии с результатами [16] при $\mathrm{Dt} = 0$ уравнение (14) имеет два корня при ненулевых значениях β_2 и β_3, что (с учетом наличия 1 кубичного корня по модулю p) соответствует $p - 1$ варианту пар значений (β_2, β_3), т. е. этот случай дает $2(p - 1)$ различных троек $(\beta_1, \beta_2, \beta_3)$, удовлетворяющих уравнению (14). При $\mathrm{Dt} \neq 0$ уравнение (14) имеет один корень в $GF(p)$ при ненулевых значениях β_2 и β_3. Число вариантов с ненулевым дискриминантом равно $p^2 - (p - 1) - 1$ (минус 1 учитывает случай $\beta_2 = 0$ и $\beta_3 = 0$). Получаем еще $p^2 - p$ пар значений (β_2, β_3), соответствующих необратимым векторам.

Всего таких пар для рассматриваемого случая получаем $p^2 - p + 2(p - 1) + 1$ (плюс 1 учитывает случай $\beta_2 = 0$ и $\beta_3 = 0$, в котором $\beta_1 = 0$), т. е. $p^2 + p - 1$ вариантов. После вычитания последнего значения из p^3 получим число различных троек $(\beta_1, \beta_2, \beta_3)$, удовлетворяющих неравенству $\Delta_{\mathbf{A}} \neq 0$: $p^3 - (p^2 + p - 1) = (p - 1)(p^2 - 1)$. Каждая из этих троек задает p^3 различных обратимых векторов, т. е. рассматриваемая шестимерная алгебра содержит $\Omega = p^3(p - 1)(p^2 - 1)$ локально обратимых векторов в случае, если 3 не делит $p - 1$.

Строение алгебры

Строение алгебры. Для каждого локально обратимого вектора имеется единственная локальная двухсторонняя единица, а именно та, которая вычисляется из векторного уравнения (8) как локальная правосторонняя единица. Легко показать, что вычисленная правосторонняя единица $\mathbf{R_A}$ из уравнения (8) является единственной для вектора $\mathbf{A}$ и всевозможных сумм всевозможных целочисленных степеней этого вектора. Также легко доказать, что $\mathbf{R_A}$ содержится в множестве глобальных левосторонних единиц (7).

Рассмотрим подмножество векторов, относящееся к некоторой заданной локальной двухсторонней единице **E**. Очевидно, каждый из этих векторов локально обратим относительно **E**, а с учетом ассоциативности умножения делаем заключение, что это подмножество векторов образует мультипликативную группу. Всего существует p^3 разных глобальных левосторонних единиц, т. е. имеем разбиение локально обратимых векторов на p^3 различных групп, содержащихся в алгебре. Покажем, что все они изоморфны между собой.

Утверждение 1. Пусть задана глобальная левосторонняя единица **L**. Тогда формула $\varphi_{\mathbf{L}}(\mathbf{X}) = \mathbf{X} \circ \mathbf{L}$, где **X** пробегает все значения алгебры, задает гомоморфное отображение рассматриваемой шестимерной КНАА.

Доказательство:

$$\varphi_{\mathbf{L}}(\mathbf{X}_1 \circ \mathbf{X}_2) = (\mathbf{X}_1 \circ \mathbf{X}_2) \circ \mathbf{L} = \mathbf{X}_1 \circ \mathbf{L} \circ \mathbf{X}_2 \circ \mathbf{L} =$$
$$= (\mathbf{X}_1 \circ \mathbf{L}) \circ (\mathbf{X}_2 \circ \mathbf{L}) = \varphi_{\mathbf{L}}(\mathbf{X}_1) \circ \varphi_L(\mathbf{X}_2);$$
$$\varphi_{\mathbf{L}}(\mathbf{X}_1 + \mathbf{X}_2) = (\mathbf{X}_1 + \mathbf{X}_2) \circ \mathbf{L} = \mathbf{X}_1 \circ \mathrm{L} + \mathbf{X}_2 \circ \mathbf{L} =$$
$$= \varphi_{\mathbf{L}}(\mathbf{X}_1) \circ \varphi_{\mathbf{L}}(\mathbf{X}_2).$$

Утверждение 2. Пусть дан вектор **A**, такой, что $\Delta_{\mathbf{A}} \neq 0$. Тогда для любой пары различных глобальных левосторонних единиц $\mathbf{L}_i$ и $\mathbf{L}_j \neq \mathbf{L}_i$ выполняется условие $\mathbf{A} \circ \mathbf{L}_i \neq \mathbf{A} \circ \mathbf{L}_j$.

Доказательство. Предположим противное, т. е. $\mathbf{A} \circ \mathbf{L}_i = \mathbf{A} \circ \mathbf{L}_j$. Тогда $\mathbf{A} \circ \mathbf{L}_i - \mathbf{A} \circ \mathbf{L}_j = \mathbf{A} \circ (\mathbf{L}_i - \mathbf{L}_j) = 0$. В силу условия $\Delta_{\mathbf{A}} \neq 0$ получаем $\mathbf{L}_i - \mathbf{L}_j = 0 \Rightarrow$ $\Rightarrow \mathbf{L}_i = \mathbf{L}_j$. Полученное противоречие доказывает утверждение 2.

Утверждение 3. Пусть рассматриваемая КНАА содержит группу порядка Ω' с единицей **E**. Тогда алгебра содержит p^3 разных групп, единицами которых являются глобальные левосторонние единицы алгебры.

Доказательство. Пусть **A** — некоторый элемент заданной группы. Для произвольной глобальной левосторонней единицы **L** получаем $\varphi_{\mathbf{L}}(\mathbf{E}) = \mathbf{E} \circ \mathbf{L} = \mathbf{L}$ и $\varphi_{\mathbf{L}}(\mathbf{A}) = \mathbf{A} \circ \mathbf{L} = \mathbf{A}_{\mathbf{L}}$. При этом $\mathbf{A}_{\mathbf{L}}$ содержится только в группе с единицей, равной **L.** Если **L** пробегает все возможные значения глобальных левосторонних единиц, то получаем p^3 разных групп, единицами которых являются глобальные правосторонние единицы алгебры. Если **A** пробегает все Ω' значений заданной группы, то получаем, что в каждой группе содержатся Ω' различных векторов (включая единицу **L**).

Легко доказать, что других групп в алгебре не содержится. Достаточно учесть то, что любой необратимый вектор имеет своей локальной двухсторонней единицей одну из глобальных левосторонних единиц. Таким образом, в алгебре имеется p^3 различных изоморфных групп порядка Ω', что определяет число обратимых векторов, равное $\Omega = p^3\Omega'$, учитывая ранее полученные формулы $\Omega = p^3(p-1)(p^2-1)$ и $\Omega = p^3(p-1)^3$, записываем формулы для порядка групп, содержащихся в рассматриваемой КНАА:

$$\Omega' = (p-1)(p^2-1), \text{ если 3 не делит } p-1;$$
$$\Omega' = (p-1)^3, \text{ если } 3 | p-1.$$

Чтобы понять строение указанных изоморфных групп, воспользуемся тем, что рассматриваемая шестимерная алгебра содержит в качестве подалгебры множество векторов вида $\mathbf{V} = (v_0, 0, v_2, 0, v_4, 0)$ с операцией векторного умножения, задаваемого по ТУБВ вида, приведенного в табл. 2.

Таблица 2

ТУБВ для трехмерной подалгебры

∘	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$	$\mathbf{e}_4$	$\mathbf{e}_6$
$\mathbf{e}_0$	$\mathbf{e}_0$	0	$\mathbf{e}_2$	0	$\mathbf{e}_4$	0
$\mathbf{e}_1$	0	0	0	0	0	0
$\mathbf{e}_2$	$\mathbf{e}_2$	0	$\mathbf{e}_4$	0	$\mathbf{e}_0$	0
$\mathbf{e}_3$	0	0	0	0	0	0
$\mathbf{e}_4$	$\mathbf{e}_4$	0	$\mathbf{e}_0$	0	$\mathbf{e}_2$	0
$\mathbf{e}_6$	0	0	0	0	0	0

Видно, что данная конкретная подалгебра является трехмерной и коммутативной. С учетом указанного изоморфизма получаем разбиение множества локально обратимых векторов исходной шестимерной алгебры на p^3 изоморфных коммутативных групп. Свойства трехмерной алгебры, изоморфной подалгебре с векторным умножением, задаваемым по таблице 2, ранее были изучены в работе [17].

Результаты исследования строения других алгебр

Исследование других конкретных шестимерных КНАА, содержащих множество глобальных левосторонних или правосторонних единиц, показало, что алгебра, содержащая p^h ($h = 2, 3, 4$) единиц, разбивается на подалгебры размерности $m = 6 - h$, число которых составляет p^h. Подалгебры пересекаются строго в нулевом векторе. Гомоморфизм шестимерной алгебры, задаваемый операцией умножения на глобальную одностороннюю единицу (умножение справа в случае левосторонних единиц и умножение слева в случае правосторонних единиц), отображает шестимерную алгебру в ее подалгебру с двухсторонней единицей,

совпадающей с односторонней единицей, задающей гомоморфизм. При этом мультипликативные группы подалгебр попарно не пересекаются и являются изоморфными между собой.

Наличие указанных гомоморфизмов может быть использовано при анализе схем ЭЦП следующим образом. Открытые параметры криптосхемы, включая элементы открытого ключа, отображаются в элементы, принадлежащие подалгебре меньшей размерности. В результате анализ исходного алгоритма сводится к анализу криптосхемы, заданной над алгеброй размерности 2, 3 или 4 (в зависимости от типа шестимерной алгебры, использованной в качестве алгебраического носителя), которая содержит глобальную двухстороннюю единицу. Более того, гомоморфные образы исходной алгебры во многих случаях представляют собой коммутативные подалгебры, из-за чего СЗДЛ в этих случаях сводится к решению обычной задачи дискретного логарифмирования.

Заключение

Выполнено исследование строения шестимерных КНАА, содержащих большие множества глобальных односторонних единиц, и показано, что существующие гомоморфизмы, связанные с единичными элементами указанного типа, могут быть эффективно использованы при криптоанализе двухключевых криптосхем. Поэтому для реализации известных схем ЭЦП, основанных на вычислительной сложности СЗДЛ, основной интерес представляют алгебры с глобальной двухсторонней единицей. Для использования механизмов, связанных с наличием большого множества глобальных односторонних единиц, требуется предложить новые подходы. В частности, могут представлять интерес криптосхемы на множестве гомоморфизмов в шестимерных алгебрах, содержащих p^4 глобальных односторонних единиц.

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации №075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015).

Литература

1. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]. Режим доступа: Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения: 11.11.2021).

2. *Alagic G., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., Liu Y.* (2019), Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD [Электронный ресурс]. Режим доступа: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (дата обращения: 11.11.2021).

3. *Moody D., Alagic G., Apon D., Cooper D., Dang Q., Kelsey J., Liu Y., Miller C., Peralta R., Perlner R., Robinson A., Smith-Tone D., Alperin-Sheriff J.* (2020), Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD [Электронный ресурс]. Режим доступа: https://doi.org/10.6028/NIST.IR.8309 (дата обращения: 11.11.2021).

4. Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms [Электронный ресурс]. Режим доступа: csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (дата обращения: 11.11.2021).

5. *Moody D.* (2021). NIST Status Update on the 3rd Round [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/CSRC/media/Presentations/status-update-on-the-3rd-round/images-media/session-1-moody-nist-round-3-update.pdf.

6. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.

7. *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. https://doi.org/10.21638/11701/spbu10.2020.410.

8. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* A novel method for development of post-quantum digital signature schemes // Информационно-управляющие системы. 2020. № 6. С. 21—29. DOI: 10.31799/1684-8853-2020-6-21-29.

9. *Moldovyan D. N.* New Form of the Hidden Logarithm Problem and Its Algebraic Support // Bulletin of Academy of Sciences of Moldova. Mathematics. 2020. № 2(93). P. 3—10.

10. *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.

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

12. *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.

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

14. *Молдовян Д. Н., Костина А. А., Курышева А. А.* Протокол слепой подписи, основанный на скрытой задаче дискретного логарифмирования в коммутативной алгебре // Вопросы защиты информации. 2021. № 1. С. 16—25. DOI: 10.52190/2073-2600_2021_1_16.

15. *Молдовян Д. Н., Молдовян А. А., Костина А. А.* Постквантовая схема цифровой подписи с двойным маскированием операции экспоненциирования // Вопросы защиты информации. 2020. № 2. С. 41—48.

16. *Moldovyan N. A., Moldovyan A. A., Shcherbacov V. A.* Generating Cubic Equations as a Method for Public Encryption // Bulletin of Academy of Sciences of Moldova. Mathematics. 2015. № 3(79). P. 60—71.

17. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and related systems. 2009. V. 17. P. 271—282.

On the choice of algebraic carrier for digital signature schemes on non-commutative algebras

A. B. Levina, A. A. Moldovyan
St. Petersburg Electrotechnical Univeristy "LETI", St. Petersburg, Russia

The issue of studying the structure of finite non-commutative associative algebras is considered as a stage of developing digital signature algorithms based on a hidden discrete logarithm problem. For a particular six-dimensional algebra, an approach to the study of the structure of algebras containing many global single-sided units is described. Connection of global single-sided with homomorphic mappings of algebra in a reduced-dimension subalgebra is shown. The presence of such mappings can be effectively used to break the signature schemes set above algebras of the said type. The results obtained show that six-dimensional algebras with a global two-sided unit are preferable as an algebraic carrier of the signature algorithms.

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

Bibliography — 17 references. *Received November 15, 2021*

УДК 003.26
DOI: 10.52190/2073-2600_2021_4_45

Новый подход к разработке алгоритмов цифровой подписи на основе скрытой задачи дискретного логарифмирования

А. А. Молдовян, д-р техн. наук; *Н. А. Молдовян*, д-р техн. наук;
Д. Н. Молдовян, канд. техн. наук
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербург, Россия

А. А. Костина
Санкт-Петербургский федеральный исследовательский центр РАН, Санкт-Петербург, Россия

Предложен новый подход к построению алгоритмов цифровой подписи, основанных на скрытой задаче дискретного логарифмирования, отличающийся тем, что один из элементов подписи S входит в проверочное уравнение, заданное в конечной некоммутативной алгебре, не менее двух раз. При этом обеспечивается вычислительная трудность решения проверочного уравнения относительно неизвестного S при фиксировании всех остальных параметров. Описан алгоритм, разработанный в рамках данного подхода.

Ключевые слова: информационная безопасность, постквантовая криптография, цифровая подпись, конечная ассоциативная алгебра, некоммутативная алгебра, двухмерная цикличность группы.

Алгоритмы электронной цифровой подписи (ЭЦП), основанные на вычислительной трудности задачи дискретного логарифмирования (ЗДЛ) и задачи факторизации (ЗФ), нашли широкое практическое применение для обеспечения защиты информации в информационно-телекоммуникационных системах. Для обычных компьютеров не известны полиномиальные по времени алгоритмы решения ЗДЛ и ЗФ, поэтому до появления на практике квантовых компьютеров указанные алгоритмы являются стойкими.

Однако за последние годы достигнут значительный прогресс в теории и технологии квантовых вычислений, который сделал актуальным предположение, что в достаточно близком будущем квантовый компьютер будет доступен и сможет применяться для решения ЗФ и ЗДЛ. Поскольку для квантового компьютера известны полиномиальные алгоритмы решения ЗФ и ЗДЛ [1, 2], реализация указанного прогноза сделает небезопасным применение криптографических алгоритмов и протоколов с открытым ключом, основанных на ЗФ и ЗДЛ [3, 4]. Это порождает проблему разработки постквантовых двухключевых криптосхем, стойкость которых основана на задачах других типов, являющихся вычислительно трудными при решении как на обычных, так и на квантовых компьютерах.

Национальный институт стандартов и технологий США (НИСТ) в конце 2016 г. анонсировал программу по разработке к 2024 г. проекта на постквантовые стандарты открытого согласования ключей и ЭЦП, в рамках которой был объявлен всемирный конкурс [5] по разработке криптосхем упомянутого типа. Из 69 предложенных кандидатов на постквантовые криптосхемы на участие во втором этапе конкурса были отобраны 17 схем открытого согласования ключа и 9 схем ЭЦП [6]. По результатам второго этапа для более детального исследования стойкости на третьем этапе были выбраны три алгоритма ЭЦП и четыре алгоритма открытого согласования ключей в качестве финалистов конкурса [7].

Главным недостатком постквантовых схем ЭЦП, выбранных в качестве финалистов конкурса НИСТ, является большой суммарный размер открытого ключа и цифровой подписи. Для устранения этого недостатка представляет интерес подход к разработке постквантовых схем ЭЦП, основанный на использовании вычислительной сложности скрытой задачи дискретного логарифмирования (СЗДЛ) [8].

Молдовян Александр Андреевич, профессор.
E-mail: maa1305@yandex.ru
Молдовян Николай Андреевич, профессор.
E-mail: nmold@mail.ru
Молдовян Дмитрий Николаевич, доцент.
E-mail: mdn.spectr@mail.ru
Костина Анна Александровна, научный сотрудник.
E-mail: anya@hotbox.ru

Статья поступила в редакцию 24 сентября 2021 г.

Разработка схем цифровой подписи (ЭЦП) на основе СЗДЛ, задаваемой в достаточно разнообразных формах [9, 10], является достаточно новым направлением постквантовой криптографии. Стандартная ЗДЛ состоит в нахождении целочисленного значения x из уравнения $Y' = G^x$, заданного в циклической группе простого порядка q, где G — генератор группы; Y' — заданный элемент. В схемах ЭЦП, основанных на ЗДЛ, Y' является открытым ключом, а x ($x < q$) — секретным ключом, связанным с открытым ключом. Известные формы СЗДЛ задаются в конечных некоммутативных группах. При разработке алгоритмов ЭЦП скрытая ЗДЛ возникает при выборе некоторой базовой циклической подгруппы, генерируемой секретным элементом G, и использовании Y' и G в качестве промежуточных значений при генерации элементов Y и Z открытого ключа, представляющих собой образы значений Y' и G, полученный путем выполнения над последним маскирующих операций ψ_1 и ψ_2, обладающих свойством взаимной коммутативности с операцией экспоненцирования: $Y = \psi_1(G^x)$ и $Z = \psi_2(G)$. Обычно в качестве носителей схем ЭЦП, основанных на СЗДЛ, используются конечные ассоциативные алгебры (КНАА), заданные над простым конечным полем $GF(p)$ [11, 12], а в качестве маскирующих операций ψ_1 и ψ_2 — автоморфные или гомоморфные отображения.

Расширение класса алгебраических носителей СЗДЛ и разработка новых ее форм представляют существенный интерес для разработки новых практичных постквантовых криптосхем [13, 14]. В данной работе предлагается новый подход к построению алгоритмов ЭЦП на основе СЗДЛ, приводящий к новым формам задания СЗДЛ, существенно отличающимся от известных тем, что при генерации элементов открытого ключа используются маскирующие операции, не обладающие свойством взаимной коммутативности с операцией экспоненцирования. При этом в качестве алгебраического носителя используется КНАА, а один из элементов подписи вычисляется в виде вектора **S**, входящего в проверочное уравнение два раза. В каждом из таких вхождений **S** умножается слева и справа на различные элементы открытого ключа, образуя произведение, возводимое в степень, вычисляемую в зависимости от рандомизирующих элементов подписи.

Идея и способ реализации подхода

В качестве алгебраического носителя предполагается использование КНАА над полем $GF(p)$ с простым числом $p = 2q + 1$ при 256-битном простом значении q, содержащей большое число изоморфных коммутативных групп, каждая из которых порождается базисом из двух векторов порядка $p - 1$. Например, может быть использована четырехмерная алгебра, строение которой изучено в [14].

Идея предлагаемого подхода состоит в задании проверочного уравнения в КНАА, включающего два (и более) вхождения одного из элементов подписи в виде вектора **S**, которые при фиксировании остальных параметров уравнения обеспечивают вычислительную невозможность нахождения значения **S** как неизвестного без знания секретного ключа, связанного с открытым ключом. При этом открытый ключ формируется в виде векторов, каждый из которых вычисляется путем умножения элементов скрытой (секретной) коммутативной группы слева и справа на секретные векторы произвольного вида. Благодаря последнему указанная пара умножений задает маскирующую операцию, свободную от свойства взаимной коммутативности с операцией возведения в степень. Однако пары векторов, используемые при вычислении различных элементов открытого ключа, связаны между собой таким образом, что при знании векторов, использованных для вычисления открытого ключа, при соответствующем задании вектора **S** можно вычислительно эффективно найти значение **S**, удовлетворяющее проверочному уравнению. Вектор **S** играет роль подгоночного элемента подписи.

Принципиальная реализуемость представленной общей идеи иллюстрируется следующей упрощенной схемой ЭЦП. Выберем в качестве скрытой группы циклическую группу, генерируемую некоторым случайным вектором **G** порядка q, и случайное неотрицательное число $x < q$. Затем выберем попарно неперестановочные векторы **A**, **B** и **D**, каждый из которых неперестановочен с **G**. Затем вычислим открытый ключ в виде пары векторов **Y** и **Z**: $\mathbf{Y} = \mathbf{A}\mathbf{G}^x\mathbf{B}$, $\mathbf{Z} = \mathbf{D}\mathbf{G}\mathbf{A}^{-1}$. Алгоритм генерации ЭЦП включает следующие шаги:

- сгенерировать случайное неотрицательное число $k < q$;
- вычислить вектор $\mathbf{R} = \mathbf{A}\mathbf{G}^k\mathbf{A}^{-1}$;
- используя некоторую специфицированную 512-битную хэш-функцию, вычислить пару 256-битных рандомизирующих элементов e_1 и e_2 подписи: $e_1 \| e_2 = f_H(M, \mathbf{R})$, где M — подписываемый электронный документ;
- вычислить число $d = k(e_1 - e_2) - x - 1 \bmod q$ и вектор $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^d\mathbf{D}^{-1}$.

Подписью к документу является тройка значений e_1, e_2 и **S**. Процедура проверки подлинности подписи включает следующие шаги:

- вычислить вектор $\mathbf{R}' = (\mathbf{YSZ})^{e_1}(\mathbf{Z}^{-1}\mathbf{S}^{-1}\mathbf{Y}^{-1})^{e_2}$;
- вычислить пару 256-битных значений e'_1 и e'_2: $e'_1 \| e'_2 = f_H(M, \mathbf{R}')$;
- если $e'_1 \| e'_2 = e_1 \| e_2$, то подпись признается подлинной. В противном случае подпись отвергается.

Нетрудно доказать корректность работы данной схемы подписи. Эта схема поясняет способ вычисления подгоночного элемента подписи **S**, однако она допускает подделку подписи путем вычисления альтернативного представления элементов открытого ключа для произвольного числа $x' < q$ и произвольно выбранной пары векторов $\mathbf{G}'$ и $\mathbf{A}'$, которое находится путем совместного решения следующей пары векторных уравнений при неизвестных значениях $\mathbf{B}'$ и $\mathbf{D}'$:

$$\mathbf{Y} = \mathbf{A}'\mathbf{G}'^{x'}\mathbf{B}' \text{ и } \mathbf{Z} = \mathbf{D}'\mathbf{G}'\mathbf{A}'^{-1}.$$

Это сводится к решению $2m$ линейных уравнений с $2m$ неизвестными, где m — размерность КНАА, используемой в качестве алгебраического носителя. Таким образом, следует устранить возможность нахождения альтернативных представлений элементов открытого ключа, которые дают возможность подделки подписи, используя заданный алгоритм генерации подписи.

Далее реализован один из способов устранения возможности нахождения альтернативных представлений элементов открытого ключа. В использованном способе вычисляются две пары открытых ключей, вычисляемых по двум различным элементам базиса скрытой коммутативной группы.

Алгоритм ЭЦП

В качестве скрытой группы используется коммутативная группа, базис которой включает два вектора: **G** и **H**, одного и того же порядка, равного значению q. Открытый ключ генерируется в виде набора из четырех векторов: **Y**, **Z**, **T** и **U**, для чего выбираются попарно неперестановочные векторы **A**, **B** и **D**, каждый из которых неперестановочен с векторами **G** и **H**, и пара случайных чисел $x < q$ и $w < q$. Указанные четыре элемента открытого ключа вычисляются по следующим формулам:

$$\mathbf{Y} = \mathbf{A}\mathbf{G}^{x}\mathbf{B},\ \mathbf{Z} = \mathbf{D}\mathbf{H}\mathbf{A}^{-1},\ \mathbf{T} = \mathbf{B}^{-1}\mathbf{G}\mathbf{A}^{-1} \text{ и } \mathbf{U} = \mathbf{A}\mathbf{H}^{w}\mathbf{D}^{-1}. \quad (1)$$

Совокупность всех значений, входящих в правые части формул (1), составляет секретный ключ.

Процедура генерации ЭЦП:

- сгенерировать пару случайных неотрицательных чисел $k < q$ и $t < q$;
- вычислить вектор $\mathbf{R} = \mathbf{A}\mathbf{G}^{k}\mathbf{H}^{t}\mathbf{A}^{-1}$;
- вычислить пару 256-битных рандомизирующих элементов e_1 и e_2 подписи: $e_1 \| e_2 = f_H(M, \mathbf{R})$, где M — подписываемый электронный документ;
- вычислить числа $d = (e_1 - e_2)^{-1}(k - xe_1 - e_2) \times \mod q$ и $\delta = (e_1 - e_2)^{-1}(t - we_2 - e_1) \bmod q$;
- вычислить вектор $\mathbf{S} = \mathbf{B}^{-1}\mathbf{G}^{d}\mathbf{H}^{\delta}\mathbf{D}^{-1}$.

Подписью к документу является тройка значений e_1, e_2 и **S** с общим размером ≈1536 бит (192 байт) при использовании в качестве алгебраического носителя КНАА, описанной в [14]. При этом размер открытого ключа составляет ≈4096 бит (512 байт).

Процедура проверки подлинности ЭЦП:

- вычислить вектор $\mathbf{R}' = (\mathbf{YSZ})^{e_1}(\mathbf{US}^{-1}\mathbf{T})^{e_2}$;
- вычислить пару 256-битных значений e'_1 и e'_2: $e'_1 \| e'_2 = f_H(M, \mathbf{R}')$;
- если $e'_1 \| e'_2 = e_1 \| e_2$, то подпись признается подлинной.

Доказательство корректности схемы ЭЦП.

Покажем, что правильно вычисленная подпись проходит проверочную процедуру как подлинная ЭЦП. Действительно, имеем следующие выкладки:

$$\begin{aligned}
\mathbf{R}' &= \left(\mathbf{YSZ}\right)^{e_1}\left(\mathbf{US}^{-1}\mathbf{T}\right)^{e_2} = \\
&= \left(\mathbf{A}\mathbf{G}^{x}\mathbf{B}\mathbf{B}^{-1}\mathbf{G}^{d}\mathbf{H}^{\delta}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}\mathbf{A}^{-1}\right)^{e_1} \times \\
&\times \left(\mathbf{A}\mathbf{H}^{w}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}^{-\delta}\mathbf{G}^{-d}\mathbf{B}\mathbf{B}^{-1}\mathbf{G}\mathbf{A}^{-1}\right)^{e_2} = \\
&= \left(\mathbf{A}\mathbf{G}^{x+d}\mathbf{H}^{\delta+1}\mathbf{A}^{-1}\right)^{e_1}\left(\mathbf{A}\mathbf{H}^{w-\delta}\mathbf{G}^{-d+1}\mathbf{A}^{-1}\right)^{e_2} = \\
&= \mathbf{A}\mathbf{G}^{e_1(x+d)+e_2(-d+1)}\mathbf{H}^{e_1(\delta+1)+e_2(w-\delta)}\mathbf{A}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{(e_1-e_2)d+e_1x+e_2}\mathbf{H}^{(e_1-e_2)\delta+e_1+e_2w}\mathbf{A}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{(k-e_1x-e_2)+e_1x+e_2}\mathbf{H}^{(t-e_2w-e_1)+e_1+e_2w}\mathbf{A}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{k}\mathbf{H}^{t}\mathbf{A}^{-1} = \mathbf{R} \ \Rightarrow\ e'_1\|e'_2 = e_1\|e_2.
\end{aligned}$$

Атака на основе альтернативного представления элементов открытого ключа в последней схеме устраняется за счет того, что она требует нахождения значений x', w', $\mathbf{G}'$ и $\mathbf{H}'$, таких, что система из следующих четырех векторных уравнений:

$$\mathbf{Y} = \mathbf{A}'\mathbf{G}'^{x'}\mathbf{B}',\ \mathbf{T} = \mathbf{B}'^{-1}\mathbf{G}'\mathbf{A}'^{-1},\ \mathbf{Z} = \mathbf{D}'\mathbf{H}'\,\mathbf{A}'^{-1} \text{ и } \mathbf{U} = \mathbf{A}'\mathbf{H}'^{w}\mathbf{D}'^{-1} \quad (2)$$

с тремя неизвестными: **A′**, **B′** и **D′** является совместной. Легко показать, что система (2) сводится к решению системы из 4*m* линейных уравнений в поле *GF*(*p*) с 3*m* неизвестными, которая при произвольном выборе значений *x′*, *w′*, **G′** и **H′** с вероятностью, близкой к 100 %, является несовместной.

Если предположить, что потенциальный атакующий знает секретные векторы **G** и **H**, то для нахождения альтернативного представления элементов открытого ключа ему потребуется найти числовые значения *x′* и *w′*, при которых система (2) будет иметь решения. При указанном предположении возникает задача нахождения дискретного логарифма в коммутативной группе, обладающей двухмерной цикличностью (группа, порождаемая двумя образующими, имеющими одно и то же значение порядка). Поскольку векторы **G** и **H** на самом деле неизвестны атакующему, можно говорить о СЗДЛ специального вида, существенно отличного от ранее известных форм СЗДЛ.

Стойкость описанной схемы ЭЦП к квантовым атакам определяется тем, что на основе элементов открытого ключа вычислительно сложно составить периодическую функцию, включающую период, зависящий от секретных значений *x* и *w*. После появления некоторой подлинной подписи **S** расширяются возможности составления периодических функций, однако периоды таких функций зависят от значений *d* и δ, вычисляемых в процессе генерации подписи в зависимости от случайных значений *k* и *t*. Поэтому неочевидно, как использовать высокую эффективность квантового компьютера для нахождения длины периодов периодических функций, принимающих значения в конечных группах, для решения предложенной версии СЗДЛ.

Заключение

Предложенный подход к построению алгоритмов ЭЦП на основе вычислительной сложности СЗДЛ был представлен частной схемой ЭЦП, однако он определяет новое направление в построении постквантовых алгоритмов ЭЦП со сравнительно малыми размерами подписи и открытого ключа. В частности, могут быть применены проверочные уравнения с тремя и более вхождениями элемента подписи **S**. Также в рамках подхода может быть применен прием удвоения проверочного уравнения [15] и в качестве скрытой группы может использоваться циклическая группа.

Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации №075-01024-21-02 от 29.09.2021 (проект FSEE-2021-0015) и при частичной финансовой поддержке бюджетной темы № 0060-2019-0010.

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. *Ekert A., Jozsa R.* Quantum computation and Shor's factoring algorithm // Rev. Mod. Phys. 1996. V. 68. P. 733.

3. *Smolin J. A., Smith G., Vargo A.* Oversimplifying quantum factoring // Nature. 2013. V. 499. №7457. P. 163—165.

4. *Yan S. Y.* Quantum Attacks on Public-Key Cryptosystems. — Springer, 2014. — 207 p.

5. Federal Register. Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Электронный ресурс]. Режим доступа: https://www.gpo.gov/fdsys/pkg/FR-2016-12-20/pdf/2016-30615.pdf (дата обращения: 16.09.2021)

6. Round 2 Submissions [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions (дата обращения: 16.09.2021).

7. Round 3 Finalists: Public-key Encryption and Key-establishment Algorithms [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (дата обращения: 16.09.2021).

8. *Молдовян Н. А., Абросимов И. К.* Постквантовые протоколы цифровой подписи на основе скрытой задачи дискретного логарифмирования // Вопросы защиты информации. 2019. № 2. С. 23—32.

9. *Moldovyan D. N., Moldovyan A. A., Moldovyan N. A.* A novel method for development of post-quantum digital signature schemes // Информационно-управляющие системы. 2020. № 6. С. 21—29. DOI: 10.31799/1684-8853-2020-6-21-29.

10. *Moldovyan D. N.* New Form of the Hidden Logarithm Problem and Its Algebraic Support // Buletinul Academiei de Stiinte a Republicii Moldova. Matematica. 2020. № 2(93). P. 3—10.

11. *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.

12. *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.

13. *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. https://doi.org/10.21638/11701/spbu10.2020.410

14. *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.

15. *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.

A new approach to the development of digital signature algorithms based on the hidden discrete logarithm problem

A. A. Moldovyan, N. A. Moldovyan, D. N. Moldovyan
St. Petersburg Electrotechnical Univeristy "LETI", St. Petersburg, Russia

A. A. Kostina
St. Petersburg Federal Research Center of the RAS, St. Petersburg, Russia

A new approach to the designing digital signature algorithms based on the hidden discrete logarithm problem is proposed. The approach is characterized in that one of the signature elements S is included in the verification equation set in a finite non-commutative algebra, at least two times. This ensures the computational difficulty of solving the verification equation relative to unknown S when fixing all other parameters. The algorithm developed under this approach is described.

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

Bibliography — 15 references. *Received September 24, 2021*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.73
DOI: 10.52190/2073-2600_2021_4_50

Методика оценки угроз безопасности информации ФСТЭК России как концепция исследования вопросов обеспечения безопасности объектов инфокоммуникационной инфраструктуры электронной коммерции

Е. В. Вайц, канд. техн. наук; *В. М. Сычев*
ФГБОУВО «Московский государственный технический университет имени Н. Э. Баумана (национальный исследовательский университет)», Москва, Россия

Обосновывается необходимость системного исследования источников угроз безопасности информации в сфере электронной коммерции, уязвимостей информации к проявлениям такого рода угроз и их деструктивного воздействия на информацию как предпосылки решения проблемы предотвращения ущерба от нарушения безопасности в среде информационной поддержки розничной торговли. Приводятся основные этапы оценки угроз безопасности информации, регламентируемые методическим документом ФСТЭК "Методика оценки угроз безопасности информации". Рассматривается возможность использования предыдущей версии данного документа для вероятностной оценки угроз безопасности информации информационных систем розничных сетей, ее уязвимостей к такого рода угрозам и соответствующих этим угрозам деструктивных воздействий на информацию. Формулируются направления совершенствования методического аппарата оценки угроз безопасности информации в системах рассматриваемого класса.

Ключевые слова: электронная коммерция, информационные системы розничных сетей, угрозы безопасности информации, вероятностная оценка угроз безопасности информации.

Наблюдаемый в последнее время существенный рост профессионализма криминальной среды в сфере информационных технологий представляет серьезную угрозу для одного из наиболее социально значимых их приложений — в электронной коммерции [1]. Естественно полагать, что материальный и репутационный ущерб от нарушения безопасности в среде информационной поддержки розничной торговли является колоссальным [2].

Этому способствуют объективно существующие уязвимости процедур хранения и обработки информации в информационных системах розничных сетей (ИС РС).

Естественно полагать, что эффективное предотвращение угроз безопасности информации в ИС РС может осуществляться лишь в условиях всестороннего и системного исследования их источников, уязвимостей к проявлениям и деструктивного воздействия на информацию.

В качестве концептуальной основы для такого исследования воспользуемся методическим документом "Методика оценки угроз безопасности информации", утвержденным 5 февраля 2021 г. ФСТЭК России [3]. Данная методика реализует сложившуюся концепцию определения угроз безопасности информации, возникновение которых возможно на объектах информационной инфраструктуры.

В соответствии с п. 2.15 методики оценка угроз безопасности информации включает следующие этапы:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- определение возможных объектов воздействия угроз безопасности информации;
- оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности.

Вайц Екатерина Викторовна, доцент кафедры "Защита информации".
E-mail: vaitcev@yandex.ru
Сычев Владимир Михайлович, старший преподаватель кафедры "Программное обеспечение ЭВМ и информационные технологии".
E-mail: vlr.sychev@gmail.com

Статья поступила в редакцию 31 мая 2021 г.

Очевидно, что проблема всестороннего и системного исследования угроз безопасности информации в ИС РС должна решаться в рамках третьего этапа. При этом в соответствии с п. 1.6 методики допускается разработка корпоративных методик оценки угроз безопасности информации, учитывающих особенности функционирования информационных систем в соответствующей области деятельности.

Следует заметить, что всестороннее и системное исследование угроз безопасности информации в ИС РС преследует цель адекватного отражения их свойств в рамках определенной метрики [4]. Случайный характер условий возникновения угроз, базирующийся на причинно-следственных отношениях между их источниками, уязвимостями информации к возникновению угроз и деструктивным воздействиям на информацию приводит к необходимости рассматривать в качестве такой метрики вероятность проявления угрозы [5].

Для этого воспользуемся положениями предыдущей версии данной методики — методикой определения актуальных угроз безопасности информации.

В соответствии с положениями данной методики отнесение тех или иных субъектов к источникам угроз осуществляется путем установления соответствия между целями деятельности этих субъектов и их возможностями. При этом процедура установления соответствия носит эмпирический характер.

Исходя из целей деятельности существует четыре источника угроз безопасности информации для ИС РС:

- криминальная среда;
- конкурирующие коммерческие организации;
- персонал ИС РС;
- производители оборудования для ИС РС и организации, осуществляющие его ремонт и обслуживание.

При этом возможности этих субъектов деятельности сводятся к реализации одного типа угроз — угроз несанкционированного доступа (НСД) к информации ИС РС.

Результатом определения уязвимостей информации ИС РС, через которые возможна реализация угроз НСД, является установление факта потенциальной возможности существования угрозы. Сама процедура определения реализуется путем экспертного анализа информационной среды ИС РС. Количественно уязвимость, через которую возможна реализация угрозы НСД, оценивается вероятностью наличия соответствующих условий для реализации. Оценка данной вероятности осуществляется экспертно специалистами в сфере компьютерной безопасности. Экспертная оценка представляется лингвистическими значениями, число которых L определяется соответствующим словарем значений, характеризующих возможности использования i-м источником угрозы НСД j-й уязвимости. Для приводимого в методике определения актуальных угроз безопасности информации словаря число L лингвистических оценок равно пяти: "да", "вполне вероятно", "возможно", "маловероятно", "нет". Каждому из L лингвистических значений ставится в соответствие вероятность p_{ij} использования i-м источником j-й уязвимости.

На основании данной вероятности определяется вероятность P_j реализации угрозы НСД через j-ю уязвимость:

$$P_j = 1 - \prod_{i=1}^{4} \alpha_{ij} \left(1 - p_{ij}\right), \qquad (1)$$

где α_{ij} — коэффициент соответствия, равный 1 в случае, когда j-я уязвимость соответствует i-му источнику угроз, и 0 в случае их несоответствия.

На основе существующей номенклатуры угроз НСД к информации [6] дадим вероятностную оценку k-й (k = 1, 2, …, K) угрозы рассматриваемого типа. Для этого воспользуемся выражением

$$P_k^{(y)} = 1 - \prod_{j=1}^{J} \beta_{jk} \left(1 - P_j\right), \qquad (2)$$

где $P_k^{(y)}$ — вероятность реализации k-й угрозы НСД к информации ИС РС;

β_{jk} — коэффициент, характеризующий возможности по реализации k-й угрозы НСД к информации ИС РС через ее j-ю уязвимость, равный 1, если реализация угрозы возможна, и 0, если реализация угрозы невозможна;

J — число уязвимостей информации, через которые возможна реализация угроз НСД к информации ИС РС.

Нарушение состояний защищенности ИС РС, вызванное реализацией угрозы НСД к информации этих систем оценивается вероятностью деструктивного воздействия:

$$P_k^{(д)} = 1 - \prod_{m=1}^{7} \gamma_{km} \left(1 - P_k^{(y)}\right), \qquad (3)$$

где m — индекс, обозначающий вариант деструктивного нарушения свойств информации в ИС РС (1 — нарушение конфиденциальности; 2 — нарушение целостности; 3 — нарушение доступ-

ности; 4 — нарушение конфиденциальности, затем целостности; 5 — нарушение конфиденциальности, затем доступности; 6 — нарушение целостности, затем доступности; 7 — нарушение конфиденциальности, затем целостности, после чего нарушение доступности);

γ_{km} — коэффициент, характеризующий возможности по реализации *m*-го (*m* = 1, 2, …, 7) варианта деструктивного нарушения свойств информации в ИС РС, равный 1, если *k*-я угроза реализует *m*-й вариант, и 0, если *m*-й вариант деструктивного нарушения свойств информации для *k*-й угрозы не характерен.

На этом возможности методики определения актуальных угроз безопасности информации в КСИИ по оценке их вероятностных характеристик исчерпываются. Несмотря на довольно глубокую проработку всех обстоятельств, связанных с возникновением угроз безопасности информации и их вредоносным воздействием на информационные ресурсы и процессы в рассматриваемом классе систем, представленный методический аппарат не обеспечивает учет тех случайных состояний, которые характеризуют динамику такого рода угроз. На это непосредственно указывается в п. 5 методики "Определение вероятностей реализации угроз": "вероятность угрозы характеризует динамику ее возникновения и реализации. … Такие модели в настоящее время отсутствуют, а их разработка представляет собой достаточно длительный процесс. Для парирования сложностей, связанных с отсутствием математических моделей расчета вероятностей реализации угроз, принято следующее допущение: … вероятность реализации угрозы в условиях отсутствия мер защиты приравнивается к единице, если данная угроза имеет место, и к нулю, если угроза отсутствует. Последнее допущение равносильно тому, что выбирается такое время, за которое реально существующая угроза может быть реализована с вероятностью, близкой к единице. В последующем предполагается расширить данную методику путем разработки необходимых математических моделей расчета вероятности реализации угрозы и устранить данное допущение".

Анализируя в целом "Методику оценки угроз безопасности информации" как концепцию исследования вопросов обеспечения безопасности объектов инфокоммуникационной инфраструктуры электронной коммерции, можно выявить два весьма серьезных обстоятельства, требующих уточнения ряда ее положений при использовании в качестве концептуальной основы для количественной характеристики нарушения информационной безопасности ИС РС вследствие реализации угроз НСД к информации этих систем.

Первое обстоятельство связано с эмпирическим характером процедуры оценки возможностей нарушителя по реализации угроз НСД к информации, основанной на экспертном анализе объектно-субъектных отношений между источниками такого рода угроз безопасности информации, ее уязвимостями к их реализации и нарушение состояний защищенности информации в ИС РС. Описательный характер процедуры анализа и ее субъективизм как следствие влияния мнения экспертов на оценочные решения не позволяет достоверно оценить, а следовательно, и адекватно характеризовать уровень угрозы. В связи с этим представляется целесообразной проработка всех аспектов вероятностной оценки угроз НСД к информации с ИС РС в рамках методического аппарата, уже достаточно хорошо зарекомендовавшей себя на практике методики определения актуальных угроз безопасности информации, как это показано в статье.

Второе обстоятельство связано с возможностью построения функциональных моделей угроз НСД к информации в ИС РС на основе выявленных закономерностей практики выявления инцидентов, связанных с реализацией такого рода угроз. Такого рода модели позволяют детализировать последовательность действий нарушителя при реализации угрозы а целях достижения своих целей. В отличие от приведенного в Приложении 11 "Методики оценки угроз безопасности информации" [3] перечня основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации, функциональные модели угроз НСД к информации отражают уже сложившиеся взгляды специалистов относительно сценариев их реализации. Это является основанием для отказа от процедуры экспертной оценки вариантов построения сценариев реализации угроз в пользу их однотипного функционального представления, детализированного с учетом возможных условий их реализации. Функциональные модели угроз НСД к информации приводятся в [7].

Кроме того, следует учитывать, что функциональная модель угрозы НСД к информации, помимо способа детализированного представления выполняемых действий нарушителя по реализации угрозы, является инструментом ее формализованного представления. Это позволяет разрабатывать на его основе математические модели временных характеристик угрозы. В свою очередь, такие мо-

дели позволяют решить и обозначенную проблему учета случайных состояний, характеризующих моменты времени возникновения угроз и моменты времени их обнаружения соответствующими средствами защиты информации, т. е. учета случайных состояний, характеризующих динамику угрозы на фоне процессов реагирования на ее проявление. Примеры таких моделей приводятся в [8, 9].

Заключение

Таким образом, очевидно, что утвержденный 5 февраля 2021 г. ФСТЭК России методический документ "Методика оценки угроз безопасности информации" [3] является концептуальной основой для реализации частных методик оценки угроз информационной безопасности. Как концепция исследования вопросов обеспечения безопасности объектов инфокоммуникационной инфраструктуры электронной коммерции данная методика может быть использована лишь в общем виде в рамках, обозначенных в ее положениях объектно-субъектных отношений между источниками такого рода угроз безопасности информации, ее уязвимостями к их реализации и нарушениями состояний защищенности информации в ИС РС, а также в рамках основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз НСД к информации этих систем.

Литература

1. *Гаврилов Л. П., Соколов С. В.* Мобильные телекоммуникации в электронной коммерции и бизнесе: учеб. пособ. для студентов вузов, обучающихся по специальности "Коммерция" (торговое дело). — М.: Финансы и статистика, 2006. — 336 с.
2. *Андриянов В. В., Зефиров С. Л., Голованов В. Б., Голдуев Н. А.* Обеспечение информационной безопасности бизнеса / ред. А. П. Курило. Изд. 2, перераб. и доп. — М.: Альпина Паблишерз, 2011. — 373 с.
3. Методика оценки угроз безопасности информации. Утверждена 5 февраля 2021 года ФСТЭК России.
4. *Скрыль С. В., Шелупанов А. А.* Основы системного анализа в защите информации: учеб. пособ. для студентов вузов. — М.: Машиностроение, 2008. — 138 с.
5. *Скрыль С. В., Гайфулин В. В., Домрачев Д. В., Сычев В. М., Грачёва Ю. В.* Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий. — М.: МИФИ, 2021. Т. 28 (№ 1). С. 84—94.
6. *Сычев А. М., Коробец Б. Н., Вайц Е. В. и др.* Безопасность операционных систем: учеб. пособ. для студ. учреждений высш. образования / под ред. Скрыля С. В. — М.: Изд. центр "Академия", 2021. — 256 с.
7. *Скрыль С. В., Гайфулин В. В., Сычев В. М. и др.* Методические аспекты построения функциональной модели угроз несанкционированного доступа к компьютерной информации // Промышленные АСУ и контроллеры. 2019. № 11. С. 48—59.
8. *Скрыль С. В., Сычев В. М., Мещерякова Т. В., Никитина Ю. С., Гайфулин В. В., Суворов А. А.* Математические модели временных характеристик угроз несанкционированного доступа к компьютерной информации // Промышленные АСУ и контроллеры. 2019. № 11. С. 60—65.
9. *Гайфулин В. В., Вайц Е. В., Сычев В. М. и др.* Киберустойчивость информационной инфраструктуры: модели исследования / под ред. Скрыля С. В. — М.: КНОРУС, 2021. — 254 с.

Methodology for assessing threats to information security by FSTEC of Russia as a concept for researching the security issues of objects of the infocommunication system of e-commerce

E. V. Vaitc, V. M. Sychev
Bauman Moscow State Technical University, Moscow, Russia

The article substantiates the need for a systematic study of the sources of information security threats in the field of e-commerce, information vulnerabilities to the manifestations of such threats and their destructive impact on information as a prerequisite for solving the problem of preventing damage from security breaches in the environment of information support for retail trade. The main stages of information security threat assessment, regulated by the FSTEC methodological document "Methodology for assessing information Security threats", are presented. We consider the possibility of using the previous version of this document for probabilistic assessment of information security threats of retail information systems, its vulnerabilities to such threats and the destructive effects on information corresponding to these threats. The directions of improving the methodological apparatus for assessing information security threats in the systems of the class under consideration are formulated.

Keywords: e-commerce, information systems of retail chains, information security threats, probabilistic assessment of information security threats.

Bibliography — 9 references. *Received May 31, 2021*

УДК 004.056.5
DOI: 10.52190/2073-2600_2021_4_54

К разработке двухуровневой модели защиты информационных потоков и систем на микро- и макроуровне

Е. Е. Филипова, канд. физ.-мат. наук; *Д. В. Титов*, канд. техн. наук
ФКОУ «Вологодский институт права и экономики ФСИН России», г. Вологда, Россия

Представлены математическое описание и особенности практического применения распространенных методов защиты, рассмотрены модели безопасности информационных систем. Предложена структура создания двухуровневой модели информационной безопасности, представленной на микро- и макроуровне.

*Ключевые слова: д*вухуровневая модель, защита информации, критерий, оценка, риск, киберугроза, шифр, ключ, криптоанализ, математическое описание, пространство состояний, модель безопасности.

Алгоритмы и программные средства, используемые для защиты информации в информационных средах, выходят на новый, качественный уровень. Эти качественные изменения происходят благодаря росту вычислительных возможностей при передаче потоков данных, с возможностью их анализа и реагирования на несанкционированное изменение. Современные принципы обеспечения информационной безопасности основаны на использовании комплексных систем защиты и безопасности, включающих подсистемы, наделенные определенными функциями.

Системы защиты в составе информационных систем функционируют как единое целое с набором входных и выходных параметров, постоянных коэффициентов. Допустим утверждение, что для исследований подобных сложных систем структуру системы защиты (системы безопасности) можно представить в виде двухуровневой модели с рассмотрением системы на микро- и макроуровне ее представления.

На макроуровне необходимо знать поведение всей системы, а также ее состояние в дискретные моменты времени. Следовательно, существует необходимость в построении адекватной модели, отражающей не только состояние системы в дискретные моменты времени, но также и степень защищенности к воздействию различного вида угроз информационной безопасности (кибервторжение, киберугроза и т. п.).

Филипова Елена Евгеньевна, доцент кафедры "Информатика и математика" инженерно-экономического факультета.
E-mail: lenphil@mail.ru
Титов Дмитрий Валерьевич, доцент кафедры "Информатика и математика" факультета психологии и права.
E-mail: titov_dv@mail.ru

Статья поступила в редакцию 3 ноября 2021 г.

Микроуровень в основном будет подчинен законам, методам, алгоритмам защиты данных по конкретному направлению безопасности (кодирование, шифрование, криптозащита, защита каналов передачи, создание "белого шума").

Приходим к следующим выводам: необходимы функционирование и анализ работы всей системы во времени. Задача представляется сложной. Попробуем сформулировать критерии оценки качества системы защиты, не прибегая к постановке задачи во времени с помощью дифференциальных уравнений. Выделим несколько критериев оценивания системы защиты на макроуровне.

Степень риска угроз безопасности. При использовании данного параметра уровню защиты системы можно дать количественную оценку, рассчитав определенные коэффициенты в дискретные моменты времени.

Как известно, под вычислением и управлением риском понимается процесс минимизации последствий от реализации риска и (или) процесс минимизации реализации риска информационной безопасности. Правила оценки рисков информационной безопасности описаны в ГОСТ Р ИСО/МЭК 27005.

Расчет параметра уровня риска системы производится по формуле

$$SL_d = 1 - \prod_{i=1}^{n} (1 - L_d), \qquad (1)$$

где L_d — величина, определяемая как произведение отношений:

$$L_d = \left(\frac{E_t}{100}\right)\left(\frac{P_r(X)}{100}\right), \qquad (2)$$

E_t — коэффициент, показывающий степень критичности киберугрозы для системы защиты; $P_r(X)$ — значение вероятности наступления данной киберугрозы.

Устойчивость алгоритмов защиты системы. Устойчивость системы защиты будет зависеть от устойчивости (или "стойкости") применяемых алгоритмов. В качестве исследуемых алгоритмов будем рассматривать криптографические методы и попытаемся выделить способы оценки криптографической стойкости.

Известно, что широкое применение так называемых скоростных алгоритмов преобразования информации требует проведения оценок их стойкости. При этом стойкость оценивается по отношению к конкретным видам вторжений или угроз. Следующим этапом будет обоснование использования защиты или оценка надежности алгоритма. Этот этап выполняется с помощью эксперимента с привлечением эмпирических методов.

Приходим к выводу, что нам потребуется моделировать различные угрозы и вторжения, причем различных видов, для того чтобы иметь хорошую статистическую выборку. Исследовать надежность системы можно с помощью оценки степени опасности негативных факторов. При использовании алгоритмов криптографической защиты такими факторами будут выступать:

- недостаточная длина ключа;
- некачественная процедура управления ключами;
- неверная инициализация генератора псевдослучайных чисел.

По мнению исследователей, наиболее подходящими для применения в компьютерных системах являются блочные шифры [1].

Отметим также, что в блочных алгоритмах шифрования существует следующее правило: входная последовательность битов разбивается на участки определенной длины. Например, входящее сообщение разбивают на участки (блоки) длиной в 64 бита в целях процессорной реализации, причем преобразование каждого блока совершается отдельно.

В нашем случае для оценки системы защиты на микроуровне необходимо выбрать модель с наиболее "стойкими" блочными шифрами.

Рассмотрим математическое описание конструкции блочных шифров с итерацией, или "итеративных" блочных шифров.

Правило шифрования запишем в следующем виде (преобразование осуществляется справа налево):

$$E_k(X) = \left(\beta_{q'_{r+1}} \circ \varphi_{q_r} \circ \ldots \circ \varphi_{q_1} \circ \varphi_{q'_0}\right)(x), \quad x \in V_n. \quad (3)$$

Правило дешифрования представлено в виде

$$D_k(Y) = \left(\alpha^{-1}_{q'_0} \circ \varphi^{-1}_{q_1} \circ \ldots \circ \varphi^{-1}_{q_r} \circ \beta_{q'_{r+1}}\right)(y), \quad x \in V_n. \quad (4)$$

Функция $\varphi(q, x)$ называется раундовой функцией, она будет иметь входное отображение $\alpha(x, q')$ и выходное отображение $\beta(x, q')$. Величину q_i называют i-м раундовым ключом алгоритма, q'_0, q'_{r+1} — ключи входного и выходного отображений. Доказательство алгоритма подробно рассмотрено в [2].

В последние годы имели место случаи взлома блочных шифров, включая метод управления временем и памятью, называемый "встреча посередине", реализованный Мерклом и Хеллманом [3]. Можно утверждать, что использование двойного или тройного шифрования с двумя ключами усложняет вскрытие шифра. В последнем случае блок обрабатывается три раза с помощью двух ключей: первым ключом, вторым ключом и снова первым ключом. При этом существует правило, согласно которому отправитель вначале производит шифрование первым ключом, а затем дешифрует вторым, после этого снова шифрует, но уже вторым ключом. Схема действий получателя аналогична отправителю. Процесс изображен на рис. 1.

Выполнение этих этапов является необходимым условием повышения надежности, так как у известного метода шифрования DES довольно малая длина ключа.

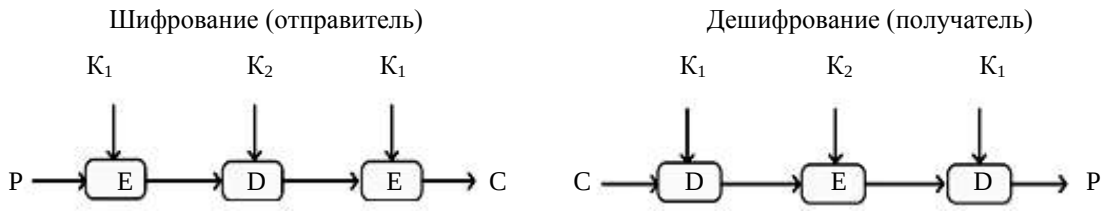


Рис. 1. Процесс тройного шифрования:
P — незашифрованное сообщение, E–D–E — этапы: шифрование, дешифрование, шифрование;
C — зашифрованное сообщение; $К_1$—$К_3$ — применяемые ключи

Использование метода шифрования, установленного ГОСТ 28147-89, также уместно, причем у него есть положительные отличия:

- длина ключа (256 бит вместо 56 у шифра DES);
- количество раундов для изменения одного бита при атаке (8 против 5);
- "раундовость" шифра выше (32 вместо 16), т. е. криптостойкость шифра выше, следовательно, потребуется больше времени на криптоанализ.

Использование моделей безопасности. Применение так называемых моделей безопасности обусловлено использованием системного подхода к исследованию путем рассмотрения защищаемой системы с помощью пространства состояний в дискретные моменты времени. Следовательно, можно утверждать, что существует конечное множество элементов, разделяемых на два подмножества:

- подмножество субъектов доступа *S*;
- подмножество объектов доступа *O*.

Информационная система будет обладать достаточной защищенностью только в том случае, когда субъекты не будут иметь возможности нарушать (обходить) установленную в системе политику безопасности.

Например, в юридических базах электронных документов, документальных информационных системах, в системах электронного документооборота широкое распространение получили парольные системы разграничения доступа.

Основные положения парольных систем можно сформулировать следующим образом.

- Система представляется следующим набором сущностей:

– множеством информационных объектов (документов)

$$O(o_1, \ldots, o_m); \quad (5)$$

– множеством пользователей

$$S(s_1, \ldots, s_n); \quad (6)$$

– множеством паролей доступа к объектам

$$K(k_1, \ldots, k_p). \quad (7)$$

- В системе устанавливается отображение множества *O* на множество *K*, задаваемое следующей функцией:

$$f_{ko} : O \to K. \quad (8)$$

- Допустимая область безопасного доступа задается множествами из трех элементов (*s, k, o*), каждый элемент которого соответствует владению пользователем паролем доступа к объекту. В результате устанавливается отображение множества *S* на множество *K*:

$$f_{ks} : S \to K. \quad (9)$$

Значением является набор паролей доступа к документам системы, известных пользователю *s*.

- Процессы доступа пользователей к объектам системы организуются в два этапа:
  – открытие документа;
  – закрытие (сохранение) документа.

Алгоритм реализован следующим образом: при открытии документа *o* пользователь *s* предъявляет монитору безопасности пароль доступа ks_0 к данному документу.

Запрос на доступ к данным будет разрешен, если выполняется условие

$$ks_0 = f_{k0}(o). \quad (10)$$

В случае успешного открытия пользователю предоставляются права работы по фиксированному набору операций с объектом (документом).

Эти преимущества парольных систем обусловливают их широкое применение в системах электронного документооборота (СЭД) и т. п.

Исходя из сказанного предложим двухуровневую структурную схему на микро- и макроуровне, которую можно использовать при создании систем защиты в небольших информационных системах для практического использования. Структура двухуровневой модели безопасности представлена на рис. 2.

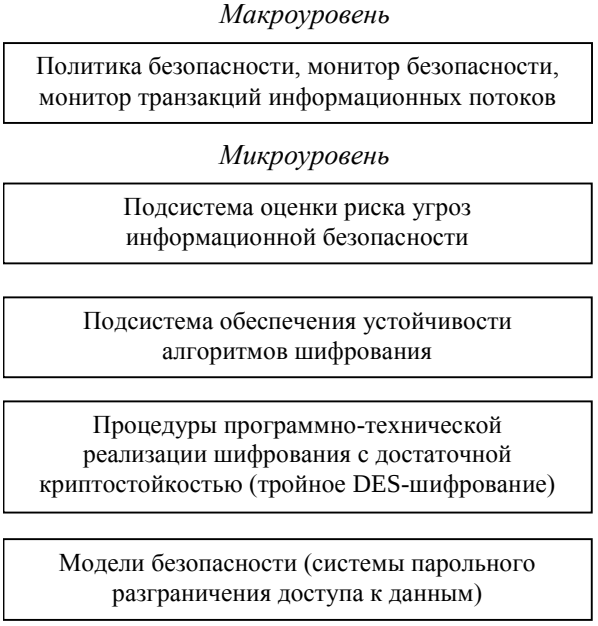


Рис. 2. Двухуровневое представление системы безопасности

Политика безопасности, включающая основополагающие положения защиты в информационной системе представляется в виде модели макроуровня. К содержанию макроуровня будем относить утвержденную политику безопасности, сервер с монитором безопасности и совершаемых транзакций, что дает возможность моделирования "очередей", поиска уязвимых мест в распределенной сети, а также контроль действия пользователей.

Обеспечение безопасности информационной системы на микроуровне обеспечивается исследованием и корректировкой системы защиты с учетом вероятности угроз, обязательным кодированием сообщений пользователей системы с использованием метода "тройного" шифрования с двойным ключом. В качестве надежного способа шифрования может выступать метод 3DES.

Заключение

Можно сделать вывод, что при исследовании структур систем защиты информации, становящихся все более сложными, представляется возможным их рассмотрение в виде двухуровневых моделей на макро- и микроуровне, конечная цель которых — минимизация риска угроз, моделирование неблагоприятных ситуаций (кибервторжений, атак), а также обеспечение всесторонней защиты данных от несанкционированного доступа.

Литература

1. *Ходжаев А. Г.* Оценка стойкости систем защиты информации и скоростные алгоритмы преобразования данных в системах: дисс. ... канд. техн. наук: 05.13.19. — М., 2001. — 203 с. РГБ ОД, 61 01-5/2577-2.
2. *Рацеев С. М.* Математические методы защиты информации. — Ульяновск: УлГУ, 2018.
3. *Жданов О. Н., Золотарев В. В.* Методы и средства криптографической защиты информации: учеб. пособие. — Красноярск: Сибирский государственный аэрокосмический университет им. академика М. Ф. Решетнева, 2007. — 17 с.

Towards the development of a two-level model for protecting information flows and systems at micro and macro level

E. E. Filipova, D. V. Titov
Vologda Institute of Law and Economics of the Federal Penitentiary Service of Russia,
Vologda, Russia

The mathematical description and features of the practical application of common protection methods are presented, security models of information systems are considered. The structure of creation of a two-level model of information security, presented at the micro and macro levels, is proposed.

Keywords: two-level model, information protection, criterion, assessment, risk, cyber threat, cipher, key, cryptanalysis, mathematical description, state space, security model.

Bibliography — 3 references. *Received November 3, 2021*

УДК 004.056
DOI: 10.52190/2073-2600_2021_4_58

Информационная безопасность как разумное и осознанное социальное решение

[1] *С. В. Потехецкий*, канд. техн. наук; [1, 2] *И. В. Капгер*, канд. техн. наук
[1] ФГБОУ ВО «Национальный исследовательский университет «МЭИ», Москва, Россия
[2] ФГБОУ ВО «Пермский национальный исследовательский политехнический университет», г. Пермь, Россия

Раскрываются проблемные вопросы информационной безопасности как разумного и осознанного социального решения. Сделан вывод, что решение вопросов информационной безопасности имеет важное социальное значение в условиях неопределённости. Высказано предположение, что решение вопросов информационной безопасности без реформирования системы воспитания и образования и с нарушением информационно-алгоритмической безопасности управления приведёт к внешнему управлению информационной безопасностью государства, общества и личности.

Ключевые слова: информационная безопасность, национальная безопасность, человек, энергоинформационная безопасность, социальное решение, необходимость, услуга, разум, осознание, информационное оружие, внешнее управление.

В условиях глобального и динамично развивающегося информационного противоборства широко используются информационные технологии для системного манипулирования общественным сознанием с определенными геополитическими целями. В связи с этим состояние национальной безопасности напрямую зависит от степени реализации стратегических национальных приоритетов, к числу которых относятся наука, технологии и образование. Безусловно, что специалисты в области информационной безопасности (ИБ) находятся на передовых рубежах обеспечения национальной безопасности, и их подготовка — задача государственной важности.

Широко известны высказывания Н. Ротшильда: "Кто владеет информацией, тот владеет миром", а также Ф. Бэкона: "Знание по своей сути есть власть". Сложившаяся в наше время парадигма мышления на основе теории общества потребления остро поставила вопросы ИБ государства, общества и личности как первостепенные с точки зрения обеспечения национальной безопасности.

Потехецкий Сергей Владимирович, старший научный сотрудник, доцент кафедры "Безопасность и информационные технологии".
E-mail: PotekhetskySV@mpei.ru
Капгер Игорь Владимирович, доцент кафедры "Безопасность и информационные технологии", доцент кафедры "Автоматика и телемеханика".
E-mail: Kapger@mail.ru

Статья поступила в редакцию 27 июля 2021 г.

Решение вопросов ИБ имеет важнейшее социальное значение в условиях информационного противоборства потому, что их разумное и осознанное решение приводит к формированию у людей мировоззрения, миропонимания и мироотношения. Жизнь человека происходит в условиях неопределённости, поэтому основной вопрос философии жизни о предсказуемости последствий принятия решений человеком нельзя оставлять без внимания [1]. Принятие решений в экономике, управлении, технике, экологии и других отраслях сопровождается определёнными рисками их последствий. Риски как сочетание вероятности события и его последствий, в свою очередь, зависят от точки зрения любого человека, принимающего субъективное решение на любую ситуацию.

Точка зрения человека всегда субъективна относительно объективного информационного окружения, поэтому справедливо высказывание Э. Бернейза о том, что "разум человека — это смесь унаследованных предрассудков, символов, клише и словесных формулировок, полученных от лидеров" [2]. Иметь свою точку зрения правильно, если она разумна и осознана. В противном случае индивиды могут находиться под внешним управлением, что зависит от их информационного обеспечения в процессе воспитания и образования, результатом чего, по образному выражению В. Г. Белинского, может стать превращение обучаемых в толпу: "Толпа есть сообщество людей, живущих по преданиям и рассуждающих по авторитетам". В этом случае безусловное восприятие системы команд по вертикали управления приво-

дит к деградации системного мышления человека, лишающей его творческого начала и полностью материализующей сознание. При этом из процесса принятия решений полностью исключается ум вместе с понятиями совести, нравственности и праведности.

Что же влияет на формирование мировоззрения, миропонимания и мироотношения современного человека, и каким образом он принимает то или иное решение при неопределённости и информационном противоборстве? Каким образом, кем и на основе чего осуществляется управление общественными институтами, к числу которых относятся семья, государство, наука и образование [3, с. 210—216]? При этом под общественным институтом следует понимать такое образование, которое несет специфический набор функций, которые другие общественные институты и отдельные лица не могут выполнять либо вообще, либо с уровнем качества, нужным для устойчивости общества и его развития. Здесь ИБ как разумное и осознанное социальное решение приобретает особую значимость.

Поскольку все четыре общественных института жёстко связаны между собой в единую систему как множество элементов, находящихся в отношениях и связях друг с другом, образующих определённую целостность и единство, достаточно сформировать в семье у ребёнка определённое мировоззрение, закрепить его через систему образования и воспитания в нужном направлении. Тогда и наука будет идти в этом направлении, лишая или, наоборот, укрепляя ИБ государственности и обеспечивая информационно-алгоритмическую безопасность управления. Миропонимание формирует мировоззрение и мироотношение субъекта к внешнему миру на основе принятия им решений в условиях неопределённости и информационного противоборства.

Именно поэтому усилия западных "партнёров" направлены на разрушение общественных институтов через информационное оружие. Замыкание на внешнее управление происходит в том числе через язык, т. к. слово — это материализованная мысль. Безусловно, правильным является в связи с этим мнение Р. Полборна о том, что "...Возможность управления человеком заложена в нем самом. Его психологические особенности, взгляды, убеждения, отношения, привязанности и т. п. обычно и используются для оказания на него воздействия" [4, с. 7]. Воздействуя информационным оружием на процессно-образное мышление человека [5], можно нарушить процесс обработки информации в триединстве информация—материя—мѣра (через "ять") и формировать материализованное мышление ("моя хата с краю").

Проводимые "реформы" системы образования в рамках "болонского процесса" в своей основе направлены на создание в РФ системы образования, аналогичной западным системам, задача которых — плодить законопослушных, но несостоятельных в познавательно-творческом отношении субъектов, не способных обеспечить суверенитет государства и живущих по принципу "где больше платят — там и родина". Но ведь подготовка кадров в области ИБ — это задача государственной важности и важнейшее социальное решение. Это может привести к внешнему управлению в подготовке кадров в сфере ИБ, как уже рассматривалось о проблемных вопросах подготовки [6]. ИБ с точки зрения достаточно общей теории управления [3, с. 410] — это устойчивое течение процесса управления объектом, а равно и самоуправления объекта в пределах допустимого отклонения от предписанного идеального режима в условиях не только стихийных воздействий окружающей среды, но и целенаправленных сторонних сил или внутренних попыток вывести управляемый объект из предписанного режима, которые могут маскироваться под проявления стихийной активности среды или под собственные шумы объекта и системы управления им. При этом результат управления может сопровождаться созданием помех и банальным перехватом управления объектом либо попытками уничтожения. В этом плане воздействие любого вида помех, организованных извне или "изнутри" объекта в условиях шумов, имеет определённое сходство с созданием помех каналу связи и передачи информации, который должен быть защищён.

Однобокий "технический" подход к подготовке профессионалов в сфере ИБ недопустим. Необходима систематическая плановая подготовка будущих профессионалов не только в сфере информационных технологий, но и в областях психологии, настоящего исторического прошлого России, экономики, формирования правильного миропонимания, мировоззрения и мироотношения, философии, социологии, объединённых общей методологической базой на основе единой концепции. Кроме того, необходимо изучение достаточно общей теории управления на основе системного подхода, дающего необходимый уровень матричной (системной) оценки и познания окружающего мира на основе творческого подхода к его изучению и миропониманию. При этом западные стандарты образования и воспитания должны быть полностью искоренены как чуждые менталитету

нашего народа. Поэтому информационная безопасность — это безусловная необходимость сегодняшнего непростого времени в условиях "цифровизации" и "цифровой трансформации", существенно сужающих возможные направления развития человеческого капитала в сравнении с цифровыми технологиями.

Главный акцент в битве в области ИБ — человек с его достоинствами и недостатками в воспитании и образовании. Поэтому энергоинформационная безопасность личности становится главной социальной проблемой в ряде других, имеющих первостепенное значение в современной жизни.

Управление невозможно, если поведение объекта непредсказуемо в достаточной мере. Устойчива ли система управления образованием (семья, детский сад, школа, средние и высшие учебные заведения) по предсказуемости поведения? Уже нет, хотя это является исходным материалом для подготовки профессионалов в области ИБ. Указанное обстоятельство, как это ни странно, связано с тем, что информация, обрабатываемая управленцем, сопровождается определёнными умолчаниями. В информации всегда должна быть истина с исключением ложной информации, навязываемой извне в виде подмены понятий о совести, нравственности, праведности и их замены на культ потребления в виде поклонения "золотому тельцу". В связи с этим ответ на вопрос, является ли решение проблем ИБ необходимостью, безусловно положителен. Каков уровень достаточности решения проблемы ИБ — это более важный по значимости вопрос, решение которого не очевидно.

Современный человек быстро привыкает к заимствованным словам, не особо вдаваясь в их смысл (*blockchain*, *bitcoin* и т. п.). Заимствования в виде ингамм проникают на подсознание человека через "легализацию" на уровне сознания, заставляя мыслить чуждыми категориями, не имеющими представления и смысла, кроме фонетики. Произнося ингаммы, индивид уродует своё миропонимание на западный манер. Мыслить такие ингаммы тоже заставляют по-западному, искажая мировоззрение, вследствие чего уже мироотношение становится агрессивным и непредсказуемым. Реализовано это через слово, являющееся материализованной, но чуждой менталитету русского человека, мыслью. Результат — нарушение энергоинформационной безопасности человека и принятие им ошибочных решений при обработке дезинформации с энергетическими затратами с отсутствием критериев принятия решений через внешнее управление.

Реальный человек из субъекта управления процессами превращается в информационный ресурс и начинает жить по вектору целей искусственно созданной для него виртуальной реальности. При этом цифровая экономика несет угрозу деградации интеллектуальных способностей. Об этом говорят открыто здравомыслящие учёные [7, 8]. Необходимо представлять себе последствия и все "блага" западной цифровизации, прогнозируя новейшие информационные угрозы.

Конечно, невозможно обеспечить этот процесс в условиях болонской системы, когда процесс воспитания и образования понимается как оказание услуг. Получение образовательных услуг превращено в платный процесс, что уравняло образование с покупкой товаров и свело роль педагога к нулю, превратив его в посредника между книгой и учеником при падении качества образования и воспитания. Применение болонской модели приводит к стандартизации образования, где не только исключается конкуренция идей и программ образования, но и реализуются процедуры оказания услуг, что негативно отражается на мотивации студентов к самостоятельной работе.

На основании изложенного можно сделать вывод о том, что информационная безопасность как разумное и осознанное решение имеет важнейшее социальное значение в условиях информационного противоборства. При этом решение вопросов информационной безопасности без реформирования системы воспитания и образования и с нарушением информационно-алгоритмической безопасности управления приведёт к внешнему управлению информационной безопасностью государства, общества и личности.

Литература

1. Достаточно общая теория управления. Изд. 2. — М.: Концептуал, 2014. — 416 с.
2. *Бернейс Э.* Пропаганда. — М.: Hippo Publishing, 2010. — 176 с.
3. Основы социологии: постановочные материалы учебного курса. — М.: Концептуал, 2015. — 496 с.
4. *Полборн Р.* Ты и Тобой: управление человеком. — М.: Московский психолого-социальный институт, 2007. — 531 с.
5. *Потехецкий С. В., Капгер И. В.* Управление информационной безопасностью в условиях неопределенности // Вопросы защиты информации. 2019. № 4. С. 45—48.
6. *Потехецкий С. В., Капгер И. В.* Проблемные вопросы подготовки кадров в сфере информационной безопасности // Вопросы защиты информации. 2019. № 3. С. 55—58.
7. *Аузан А.* Цифровая экономика: человеческий фактор [Электронный ресурс]. URL: https://philologist.livejour–nal.com/10991516.html (дата обращения: 22.03.2020).
8. *Катасонов В. Ю.* Мир под гипнозом цифры, или Дорога в электронный концлагерь. — М.: Б-ка РЭО им. С. Ф. Шарапова, 2018. — 419 с.

Information security as a reasonable and conscious social decision

[1] *S. V. Potekhetsky,* [1, 2] *I. V. Kapger*
[1] Moscow Power Engineering Institute (MPEI), Moscow, Russia
[2] State National Research Politechnical University of Perm, Perm, Russia

The problematic issues of information security as a reasonable and conscious social solution are revealed. It is concluded that the solution of information security issues is of the most important social importance in the conditions of uncertainty. It is suggested that the solution of information security issues without reforming the system of upbringing and education and with a violation of the information and algorithmic security of management will lead to external management of information security of the state, society and the individual.

Keywords: information security, national security, person, energy-information security, social solution, necessity, service, reason, awareness, information weapon, external management.

Bibliography — 8 references. *Received July 27, 2021*

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 на CD/DVD-диске с текстом в формате Word.

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;
- с отступлением в 2 строки представляется аннотация статьи;
- 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, следую-щих 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 $U_{вх}$, $I_{вых}$, $v_{гр}$ 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).

БЛАНК-ЗАКАЗ НА ПОДПИСКУ 2022 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Индекс издания (количество выпусков в год)	Цена 1 экз., руб.	Кол-во выпусков в год	Общая сумма, руб.
Оборонный комплекс — научно-техническому прогрессу России	4	1550,00		
Конструкции из композиционных материалов	4	1700,00		
Экология промышленного производства	4	1500,00		
Информационные технологии в проектировании и производстве	4	1750,00		
Вопросы защиты информации	4	1750,00		
В цену включены: НДС — 10 % и стоимость почтовой доставки.				

Поставка журналов подписчикам через издательство осуществляется почтовыми бандеролями с приложением всех необходимых бухгалтерских документов.

Наши реквизиты:

Полное наименование организации: _____

Сокращенное наименование организации: _____

ИНН/КПП _____

ОКПО _____

Расчётный счёт № _____ в _____

к/с _____ БИК _____

Юридический адрес: _____

Почтовый адрес: _____

Контактное лицо _____ тел. _____

E-mail: _____

(Для оформления счёта и бухгалтерских документов просьба заполнить все строчки).

Справочно:
Заполненный бланк-заказ просьба отправить по факсу: 8(495) 491-44-80 или
E-mail: secretariat@ntckompas.ru
Более подробную информацию об изданиях и подписке можно получить по телефону:
8 (495) 491-43-17
E-mail: ivleva@ntckompas.ru
Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.
ФГУП «НТЦ оборонного комплекса «Компас».