Индекс 79187

ISSN 2073-2600

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ

2

(133)

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**

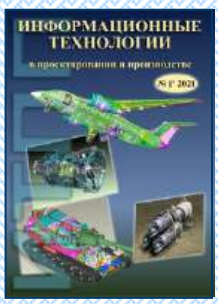
Издается с 1984 года

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

2 (133)

Москва 2021
Основан в 1974 г.

СОДЕРЖАНИЕ

Вопросы защиты информации: Науч.-практ. журн. / ФГУП «НТЦ оборонного комплекса «Компас», 2021.
Вып. 2 (133). С. 1—52.

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

Подписано в печать 04.06.2021. Формат 60x84 1/8.
Печать офсетная. Усл. печ. л. 6,0 . Уч.-изд. л. 6,2.
Тираж 400 экз. Заказ 1974. 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.

ИНЖЕНЕРНАЯ КРИПТОГРАФИЯ

УДК 004
DOI: 10.52190/2073-2600_2021_2_3

Квантово-криптографические методы шифрования как актуальное и эффективное средство обеспечения информационной безопасности в сетях IoT

Д. С. Карнута
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Рассмотрены криптографические методы шифрования в качестве средства обеспечения информационной безопасности в сетях Интернета вещей. Предпринята попытка доказать гипотезу, что квантово-криптографические методы шифрования имеют возможность на качественном уровне увеличить эффективность работы и функционирования систем по обеспечению информационной безопасности в сетях IoT. Детально изучены квантово-криптографические методы шифрования при решении задач из области информационной безопасности. В результате представленного исследования в полной мере раскрыта актуальность и приведена оценка эффективности использования криптографических методов шифрования в задачах информационной безопасности сетей Интернета вещей.

Ключевые слова: Интернет вещей, квантово-криптографическое шифрование, информационная безопасность, сети, информационные технологии.

Повсеместное развитие Интернета вещей (IoT) — одно из следствий прогресса в области развития информационных и цифровых технологий. Как и любая цифровая технология, Интернет вещей обеспечивает наиболее эффективную и упрощенную деятельность современного человека в различных аспектах. Одним из примеров развития IoT является разработка и интеграция систем "умного дома". "Умный дом" — это один из основных видов Интернета вещей, позволяющих человеку качественно повысить эффективность бытовой деятельности. Посредством Интернета вещей рационализируется работа бытовых приборов, повышается эффективность обслуживания электрических систем и т. д. [1].

Как и любая информационная технология, сети Интернета вещей являются достаточно уязвимыми к различным кибератакам, производимым в целях хищения персональной информации и иных неправомерных действий. Современные сети IoT нуждаются в интеграции инновационных средств защиты информации, способных повысить эффективность и бесперебойность работы их систем информационной безопасности.

Цель данной работы — детальное изучение вопроса обеспечения информационной безопасности в сетях IoT. Решены основные задачи, связанные с оценкой актуальности и эффективности интеграции квантово-криптографических средств защиты информации в сетях Интернета вещей [2].

Методы исследования

Основной задачей данного исследования является изучение актуальности использования квантово-криптографических методов шифрования информации для обеспечения информационной безопасности в сетях IoT. Для более предметного понимания описываемых процессов представлена принципиальная схема функционирования квантово-криптографического метода шифрования. Результатом являются оценка актуальности, изучение частного алгоритма шифрования, а также анализ и систематизация полученных знаний. Работа произведена посредством применения статистических данных и информации, а также эмпирических, теоретических и статистических методов исследования. В целях более полного раскрытия

Карнута Дмитрий Сергеевич, начальник учебной части — заместитель начальника кафедры УВП МО РФ ВУЦ.
E-mail: dima-karnuta@mail.ru

Статья поступила в редакцию 29 апреля 2021 г.

темы и получения достоверных данных взяты материалы из отечественных и зарубежных источников.

Использованы материалы Соколова М. Н., Смоляниной К. А., Якушевой Н. А., Полегенько А. М., Масловой М. А., Королькова А. В. и других. В каждой из публикаций рассмотрены отдельные вопросы, связанные с темой представленного исследования. Использование указанных источников необходимо для более детального и качественного изучения.

Представление об Интернете вещей

Интернет вещей — это сеть, в состав которой входят связанные между собой физические вещи или устройства, которые обладают встроенными датчиками, и программное обеспечение, с помощью которого происходит обмен данными между обществом и информационными системами посредством огромного числа стандартных протоколов связи [3].

Кроме датчиков, в состав сети могут входить исполнительные устройства, которые расположены внутри самих объектов и функционируют между собой с использованием беспроводных и проводных сетей. Данные устройства обладают следующими функциями: считывание; активация работы; программирование; идентификация; автоматизированная работа, возможная благодаря наличию интеллектуальных интерфейсов.

Ключевая концепция IoT заключается в способности подключения произвольных объектов, применяемых человеком в повседневной жизни (холодильник, велосипед, автомобиль и т. п.).

Выделяют два основных способа взаимодействия с IoT, которые и представлены на рис. 1.

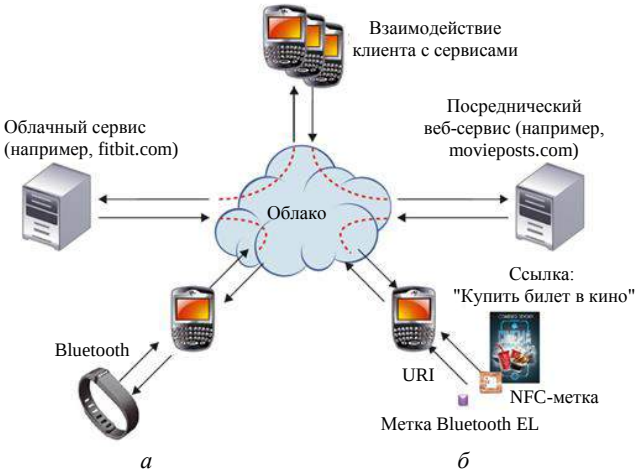


Рис. 1. Способы взаимодействия с IoT:
а — прямой; *б* — через посредника

В каждый из таких объектов необходимо установить внутренний датчик, выполняющий описанные функции. В качестве примера можно привести системы "умный дом" или "умная ферма" [4].

Актуальность вопроса информационной безопасности (ИБ) в сетях IoT

Основной проблемой, возникающей при использовании сетей IoT, является отсутствие защиты от несанкционированного воздействия. В лучшем случае такая атака со стороны злоумышленника может стать причиной нанесения вреда имуществу человека, а в самом худшем — причинить вред его здоровью.

Рассмотрим в качестве примера следующий вариант развития событий. Устройства, применяемые для контроля и управления электрической сетью, легко могут быть скомпрометированы злоумышленником благодаря абсолютно любому устройству, которое имеет выход в Интернет. Производя контроль над такими устройствами, хакер может осуществить отключение любого электрического оборудования (в том числе систем жизнеобеспечения, систем охраны на производстве), создать короткое замыкание или вызвать аварийную ситуацию на производстве [5].

Поэтому весьма актуальным является исследование безопасности Интернета вещей, в частности безопасности пользователя, его вещей и личной информации, которая передается, обрабатывается и хранится в сетях IoT.

Проблема обеспечения требуемого уровня информационной защиты в сетях подобного масштаба требует комплексного подхода. Очень важно в данных вопросах уделять достаточно внимания таким аспектам, как конечные информационные системы и безопасность их взаимодействия.

Таким образом, задача обеспечения безопасности данных в сетях IoT может быть разделена на две основные, более мелкие задачи, а именно обеспечение безопасности:

- конечных систем (рис. 2);
- их сетевого взаимодействия (рис. 3).

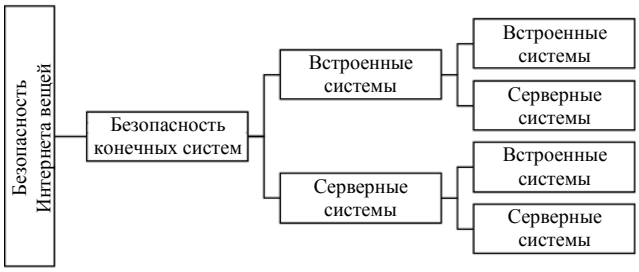


Рис. 2. Структура обеспечения ИБ в IoT конечных систем

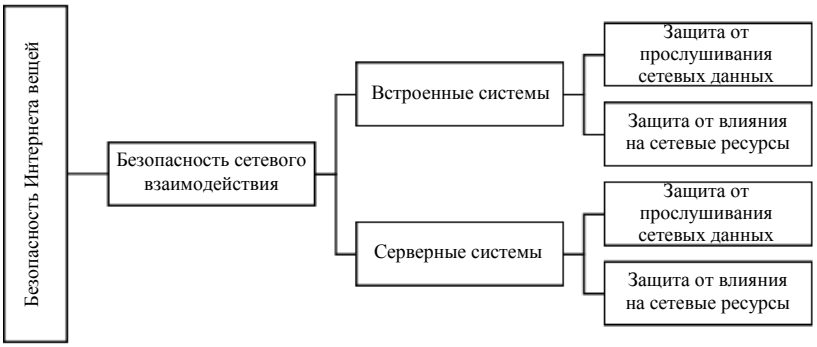


Рис. 3. Структура обеспечения ИБ в IoT сетевого взаимодействия

Наибольшую актуальность представляет структура обеспечения ИБ в IoT сетевого взаимодействия. Для обеспечения информационной безопасности Интернета вещей на данном уровне могут быть использованы квантово-криптографические методы шифрования информации [6].

Актуальность интеграции квантово-криптографических методов шифрования информации в сетях IoT

Основным алгоритмом шифрования информации, используемым в Китае, Сингапуре, России и США, является квантовая криптография. Так, российские компании "Инфотекс" и "Центр квантовых технологий МГУ" представили телефон с квантовой защитой связи ViPNet QSS Phone. Пара квантовых телефонов способна надежно сформировать общий секретный ключ, которым будет шифроваться общение собеседников. Квантовая криптография является методом защиты коммуникаций, основанным на принципах квантовой физики. Основная ее особенность относительно обычной криптографии — сосредоточение на физических методах, когда информация формируется и переносится посредством объектов квантовой механики. Процесс передачи и приема информации осуществляется посредством выполнения физических процессов. Примером является движение электронов в электрическом токе или фотонов в линиях волоконно-оптической связи (рис. 4).

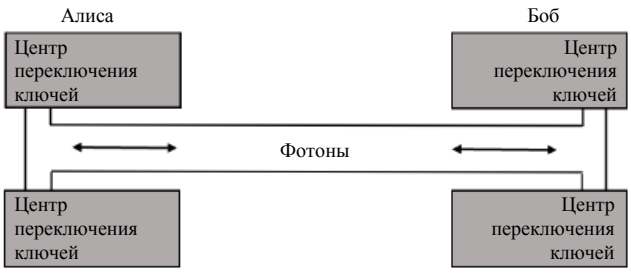


Рис. 4. Квантово-криптографическая схема (система состоит из квантового канала и специального оборудования на обоих концах схемы)

Как видно из рис. 4, ключевым принципом работы квантово-криптографических алгоритмов является неопределенность поведения квантовой системы. Основная идея этого принципа заключена в том, что отсутствует возможность одновременного выражения координаты и импульса частицы без параллельного искажения одного из них.

Посредством работы квантовых процессов широкомасштабно разрабатываются и внедряются различные системы связи и средства передачи информационных потоков, имеющие возможность стопроцентного обнаружения подслушивания и перехвата информации, одними из которых являются сети IoT. Данная способность достигается благодаря тому, что любая попытка измерения взаимосвязанных параметров квантовой системы вносит в нее нарушения, параллельно разрушая исходные данные.

Становление квантово-криптографических алгоритмов послужило началом разработки криптографического анализа, имеющего ряд преимуществ относительно обычной криптографии. Одним из самых известных и эффективных алгоритмов шифрования информационных потоков, способным конкурировать с квантово-криптографическими методами, является алгоритм шифрования RSA. Достоинством криптографического анализа относительно RSA является то, что методы криптографии могут быть основаны на проблеме дискретного логарифмирования. Именно поэтому разработка крупных квантово-криптоаналитических систем может стать негативным событием для RSA и других асимметричных систем. Для выполнения требуемых алгоритмов необходимо только создание квантового компьютера [7].

Актуальность использования и интеграции данных методов шифрования информации в сетях Интернета вещей особенно высока и заключается в том, что данный метод обеспечения информационной безопасности является уникальным в своем роде, и неподвластен расшифровке и декодированию третьими лицами.

Таким образом, квантово-криптографические методы шифрования информации являются инновационной технологией в системах информационной безопасности сетей IoT, способной повысить эффективность работы информационных систем в отношении информационной безопасности. Поэтому предприятия и компании, желающие повысить уровень информационной безопасности, должны обратить на них особое внимание.

Криптографические протоколы IoT-систем

Наиболее популярными криптографическими протоколами в системах IoT и Big Data являются следующие:

- набор межсетевых протоколов IPsec (IP Security) для аутентификации, проверки целостности и шифрования IP-пакетов, а также защищённого обмена ключами в Интернете. Часто применяется для организации VPN-соединений;
- TLS (Transport Layer Security) — протокол защиты транспортного уровня, обеспечивающий защищённую передачу данных между узлами в Интернете на основе асимметричного шифрования для аутентификации, симметричного шифрования для конфиденциальности и кодов аутентичности сообщений для сохранения их целостности. Данный протокол широко используют в веб-приложениях, электронной почте, мессенджерах и IP-телефонии (VoIP);
- Kerberos — сетевой протокол взаимной аутентификации клиента и сервера перед установлением связи между ними. Широко используют в системах Big Data и входит в состав некоторых дистрибутиов Apache Hadoop (HortonWorks, MapR).

Также очень часто в IoT-системах используют протокол 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks), который позволяет безопасно передавать пакеты IPv6 в небольших фреймах канального уровня поверх маломощных беспроводных персональных сетей [8].

Заключение

Проработан вопрос, касающийся актуальности интеграции квантово-криптографических методов шифрования информации в системах информационной безопасности сетей IoT. Рассмотрено общее представление о сетях Интернета вещей, изучены способы взаимодействия с IoT, актуальность вопроса информационной безопасности в сетях IoT, структура обеспечения ИБ в IoT конечных систем, структура обеспечения ИБ в IoT сетевого взаимодействия, актуальность интеграции квантово-криптографических методов шифрования информации в сетях IoT, криптографические протоколы IoT-систем.

Исходя из технических стандартов IoT представляет собой общественную мировую инфраструктуру, которая состоит из передовых решений в области объединения физических и информационных вещей с помощью существующих информационных технологий. Можно с уверенностью заявить, что IoT очень сильно влияет на жизнь современного общества, проникая практически во все сферы деятельности человека. Построение такой структуры должно осуществляться с учетом всех требований, предъявляемых к информационной безопасности.

В заключение необходимо отметить, что применение и внедрение квантово-криптографических методов шифрования информации в системах информационной безопасности сетей IoT способно обеспечить бесперебойную, рационализированную работу практически всех сфер жизнедеятельности человека при активном использовании информационных систем и различных электронно-вычислительных машин.

Литература

1. *Соколов М. Н., Смолянинова К. А., Якушева Н. А.* Проблемы безопасности Интернета вещей: обзор // Вопросы кибербезопасности. 2015. № 5. С. 32—35.
2. *Полегенько А. М.* Особенности защиты информации в Интернете вещей // International J. Open Information Technologies. 2018. V. 6. № 10. P. 41—45.
3. *Маслова М. А.* Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. Т. 4. № 1. С. 31—37.
4. *Корольков А. В.* О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы квантовой кибербезопасности. 2015. № 1(9). С. 6—13.
5. *Румянцев К. Е., Плёнкин А. П.* Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. 2014. №. 10. С. 11—15.
6. *Шемякина М. А.* Анализ использования квантовых технологий в криптографии // Междунар. журнал гуманитарных и естественных наук. 2019. № 5-4. С. 59—62.
7. *Актаева А. У., Илипбаева Л. Б.* Инновационные технологии в системе информационной безопасности: квантовые технологии // Современные информационные технологии и ИТ-образование. 2014. № 10. С. 320—326.
8. *Дрон К. К.* О перспективах совместного использования методов квантовой и классической криптографии // Вестник ХГУ им. Н. Ф. Катанова. 2018. № 24. С. 8—11.

Quantum cryptographic encryption methods as an actual and effective means of ensuring information security in IoT Networks

D. S. Karnuta
Moscow Aviation Institute (National Research University), Moscow, Russia

Considered are cryptographic encryption methods as a means of ensuring information security in the Internet of Things networks. An attempt is made to prove the hypothesis that quantum-cryptographic encryption methods have the ability to qualitatively increase the efficiency of the work and functioning of systems to ensure information security in IoT networks. Quantum-cryptographic encryption methods for solving problems in the field of information security have been studied in detail. As a result of the presented study, the relevance is fully disclosed and an assessment of the effectiveness of using cryptographic encryption methods in the problems of information security of the Internet of Things networks is given.

Keywords: Internet of Things, quantum cryptographic encryption, information security, networks, information technology.

Bibliography — 8 references. *Received April 29, 2021*

УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004
DOI: 10.52190/2073-2600_2021_2_8

Оценка актуальности и эффективности интеграции искусственных нейронных сетей в системы информационной безопасности

С. А. Дмитриев
Московский авиационный институт (национальный исследовательский университет), Москва, Россия

Рассмотрено одно из решений задачи повышения эффективности работы систем информационной безопасности, связанное с интеграцией в эти системы интеллектуальных средств и методов. Подтверждены актуальность и эффективность использования искусственных нейронных сетей в задачах информационной безопасности.

Ключевые слова: интеллектуальные средства, информационная безопасность, нейронные сети, технология, эффективность.

Информационные технологии (ИТ) являются неотъемлемой частью жизни человека. ИТ функционируют на базе использования множества средств и методов сбора, обработки и передачи данных в целях получения информации необходимого качества о состоянии объекта, процесса или явления.

Основная цель информационных технологий — усовершенствование и автоматизация производственных процессов на предприятии и процессов обеспечения личных потребностей человека. ИТ являются лидирующим направлением в профессиональной сфере человеческой деятельности. Повсеместно внедряются и разрабатываются совершенно новые, ранее не изученные технологии. На предприятиях происходит интенсивное распространение и совершенствование цифровых и информационных технологий. Данное направление определяет основные траектории развития экономики и общества. Это приводит к колоссальным изменениям, касающимся жизни людей [1].

Посредством информации и информационных технологий передаются конфиденциальные данные, производятся транзакции на предприятиях, осуществляются хранение и работа с засекреченной информацией и т. д. Данный список можно продолжать бесконечно, так как в век информационных технологий практически все процессы основываются на применении информационных технологий и информации. Исходя из этого формируется проблема, связанная с защитой информации и информационных ресурсов в целом. Информационная безопасность является одним из приоритетных направлений. Существует колоссальное количество способов и методов защиты информации [2].

Вопрос защиты информации достаточно хорошо изучен многими отечественными и зарубежными исследователями. Однако в данной области все еще существует колоссальное количество проблем, одной из которых является недостаточная сформированность методического аппарата, регулирующего вопросы технической защиты информации в качестве части информационной безопасности критически важной инфраструктуры.

Методы исследования

Цель настоящей работы заключается в изучении технологии нейронных сетей как инновационного средства развития сегмента информационной безопасности. Автором рассматриваются основные сведения, актуальность и эффективность, касающиеся темы исследования. Исследование проводится с применением статистических данных, а также эмпирических, теоретических и статистических методов исследования. Для более полного раскрытия темы и получения достоверных данных используются материалы отечественных и зарубежных источников.

Дмитриев Сергей Александрович, старший преподаватель.
E-mail: s-dmi@yandex.ru

Статья поступила в редакцию 29 апреля 2021 г.

Близким представленной в данной работе и смежным с ней темам посвящено множество научных статей, работ и монографий, каждая из которых изучает более досконально отдельные аспекты структуры и систем информационной безопасности. Автор использует, научные выкладки и результаты, полученные Соколовым М. Н., Смоляниной К. А., Полегонько А. М., Довгаль В. А. и другими исследователями. В каждой из указанных работ производятся чрезвычайно актуальные исследования по информационной безопасности, например вопросов информационной безопасности Интернета вещей, защиты информации в Интернете, актуальных технологий и методов защиты информационных ресурсов и т. д.

Актуальность вопроса обеспечения информационной безопасности и интеграции искусственного интеллекта

В мире непрерывно и с невероятно высокой скоростью увеличивается число информационных архивов, переводов денежных средств и коммуникаций в цифровую форму, в результате чего создан самостоятельный вид актива, называемый информацией. Как и иные ценности, информация подвержена нападениям со стороны хакерских и мошеннических атак. Поэтому существует ряд рисков, относящихся к области информационной безопасности (ИБ). Бездействие при возникающих проблемах может привести к потере конкурентоспособности организаций на различных уровнях. Помимо предприятий и организаций от рисков информационной безопасности страдают и обычные люди, которые пользуются гаджетами и иными средствами коммуникации [1].

На рис. 1 представлены основные факторы, из-за которых в современном мире актуализируется проблема, связанная с обеспечением информационной безопасности на предприятиях.

Одними из наиболее актуальных технологий, активно разрабатываемых и тестируемых в задачах информационной безопасности на современных предприятиях, являются интеллектуальные средства. Одной из основных технологий, относящейся к сфере ИТ и имеющей колоссальное влияние во многих процессах, является искусственный интеллект. Актуальность использования искусственного интеллекта (ИИ) как никогда высока. Именно посредством данных технологий решаются одни из самых трудновычислимых задач. Искусственный интеллект находит применение не только при решении математических и иных инженерных задач для принятия оптимальных решений, но и успешно применяется в сфере защиты информации [2].

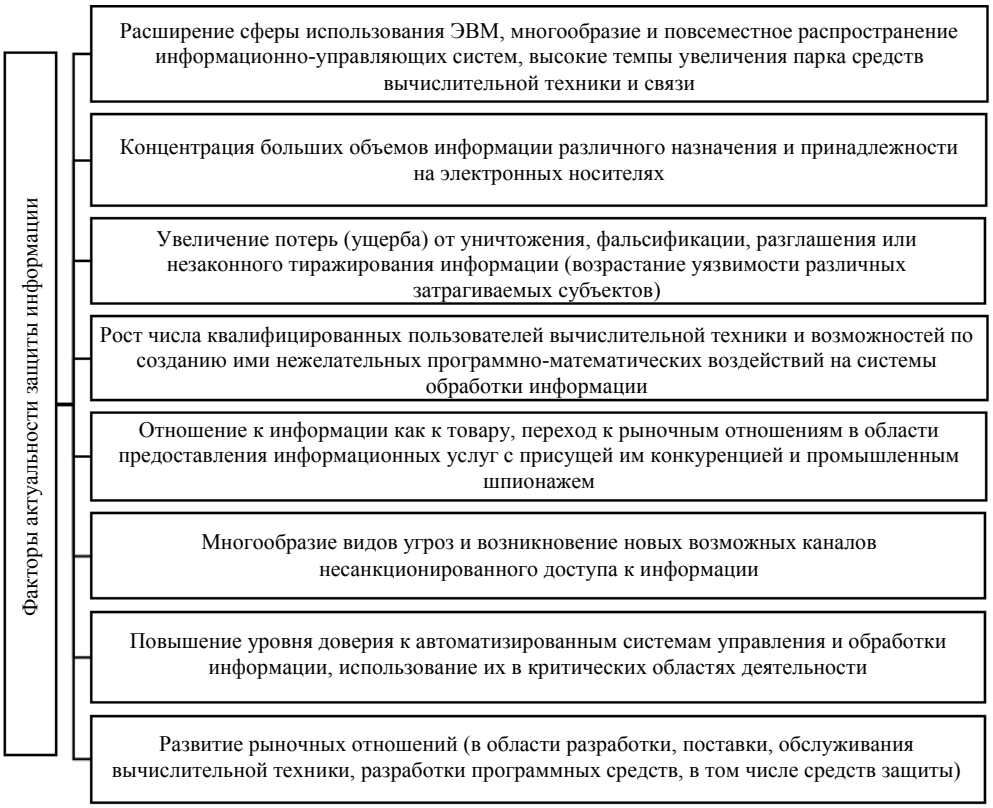


Рис. 1. Основные факторы, определяющие актуальность защиты информации

Ключевой технологией, на базе которой основывается искусственный интеллект, является возможность самообучения, а также использования накопленных данных в целях прогнозирования будущего. Основной отличительной особенностью ИИ относительно обычных цифровых решений является то, что при выполнении задач искусственный интеллект не основывается на логических схемах, заданных ранее программистами, а самостоятельно производит настройку комплексных механизмов для принятия решений, основываясь на тех данных и задачах, которые были изначально заданы программистами.

Представление об искусственных нейронных сетях и актуальности их использования в системах информационной безопасности

Одним из направлений развития искусственного интеллекта, активно использующимся при решении задач информационной безопасности, являются искусственные нейронные сети. Искусственные нейронные сети (ИНС), или нейросети, выступают в качестве математической модели, которая имеет программную и аппаратную реализацию. ИНС выстраиваются на принципиальной базе биологических сетей, а именно по принципу сетей нервных клеток живых существ. Данное понятие было разработано в результате изучения и попытки моделирования процессов, происходящих в мозге у биологического существа. Одной из первых попыток в данной области исследования стали нейронные сети У. Маккалока и У. Питса. В дальнейшем нейронные сети нашли свое применение практически во всех задачах современного мира, например задачах прогнозирования, распознавания образов, управления, защиты информации и других. На рис. 2 представлена схема простой нейронной сети [3].

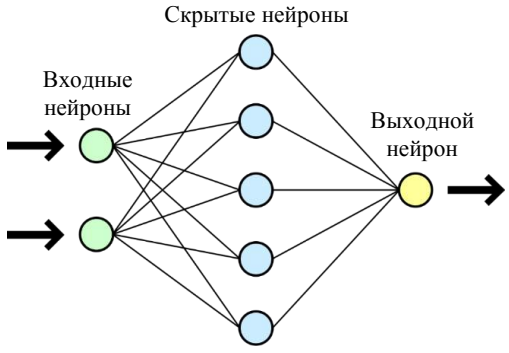


Рис. 2. Схема простой нейросети

В математической интерпретации искусственный нейрон представляется в виде нелинейной функции. В математической модели w характеризует связи, посредством которых сигналы от одних нейронов поступают как входные сигналы в другие нейроны. Каждый нейрон из ИНС имеет единственный выход, называемый синапсом. Каждый выход нейрона может быть связан с неограниченным числом выходов других нейронов (рис. 3).

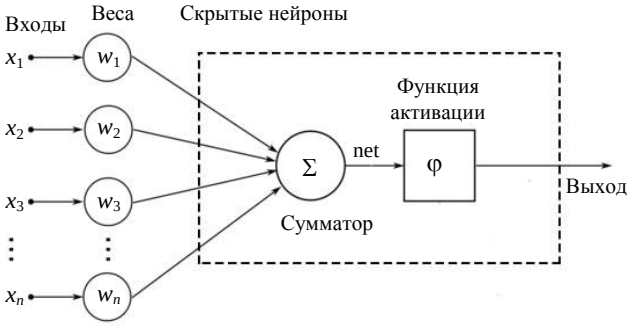


Рис. 3. Схема искусственного нейрона

Для наглядности запишем математическую модель искусственного нейрона [4]:

$$y = f\left[\sum_{i=1}^{n}\left(w_i\, x_i + b_i\right)\right],$$

где w_i — веса соответствующих входов;
x_i — сигналы на входах нейрона;
b_i — вход и вес нейрона смещения.

Оценка эффективности интеграции искусственных нейронных сетей в системы информационной безопасности

ИНС достаточно прочно входят в жизнь современного человека при решении различного рода задач, а также используются там, где примитивные алгоритмы являются неэффективным или вовсе невозможным инструментом. В ряде задач, решение которых основывается на использовании нейронных сетей, находятся распознавание текста, контекстная реклама на сайтах, фильтрация спама, мониторинг подозрительных операций в банковской системе, реставрация изображения и многие другие [4].

Технологии ИНС обладают сильным инструментом, позволяющим решать многие из самых сложных и трудновычислимых задач, включая область информационной безопасности предприятий. Наблюдается тенденция, связанная с распространением и повсеместным внедрением ИНС практически во все бытовые и профессиональные сферы жизнедеятельности человека. Данный фактор обусловлен высокой эффективностью и раци-

ональностью использования нейронных сетей в решении задач различного рода [5].

Определим основные направления интеграции ИНС в сегменте информационной безопасности на предприятиях (рис. 4).

Современные предприятия, которые внедряют технологии ИИ, в частности ИНС, в системы ИБ, получают колоссальные результаты, выражающиеся в повышении эффективности обнаружения атак на информационные ресурсы, а также сокращении времени реагирования и затрат на организацию обеспечения информационной безопасности. На рис. 5 представлено распределение продуктов информационной безопасности с применением технологий искусственного интеллекта по сценариям использования [5].

Изучив вопрос актуальности использования интеллектуальных систем, в частности искусственных нейронных сетей, в задачах по защите информации, необходимо более подробно остановиться на эффективности интеграции данных сетей в изучаемую область.

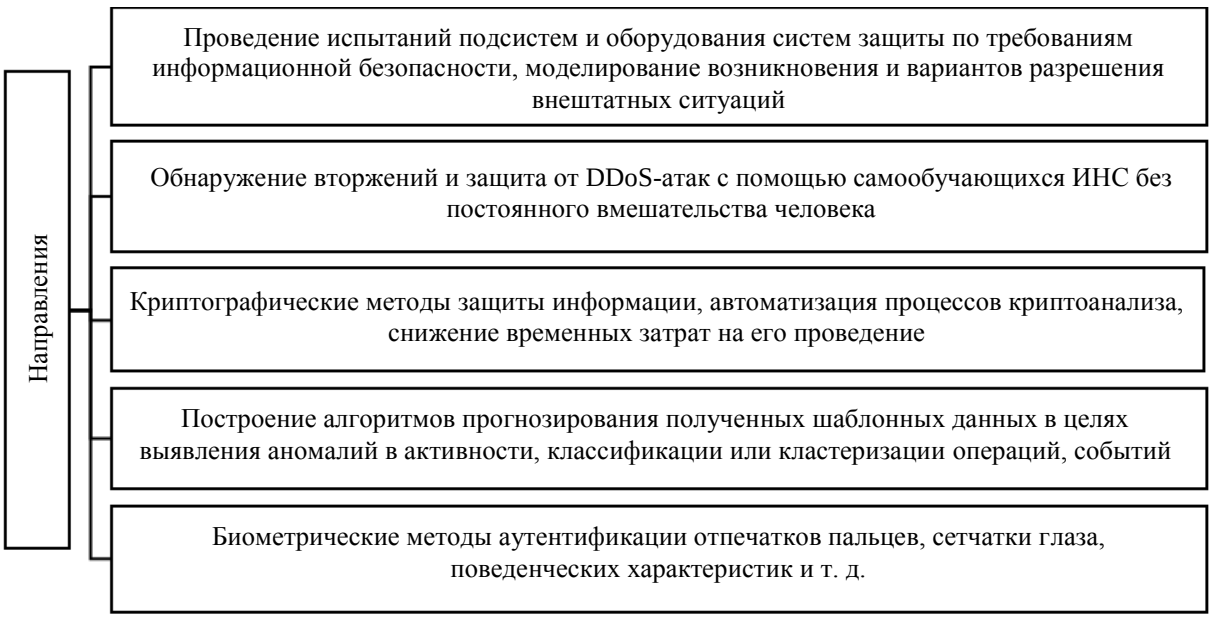


Рис. 4. Направления интеграции ИНС в сегменте информационной безопасности

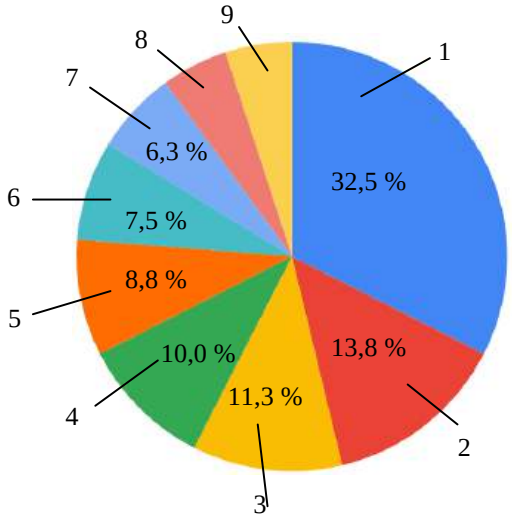


Рис. 5. Распределение продуктов с применением технологий ИИ по сценариям использования:
1 — обнаружение и реагирование на кибератаки; 2 — обнаружение мошенничества в бизнес-процессах; 3 — управление событиями безопасности; 4 — защита конечных точек; 5 — защита приложений и управление уязвимостями; 6 — управление доступом и аутентификация; 7 — анализ поведения пользователей и устройств; 8 — обнаружение вредоносных программ; 9 — антифишинг

Определим основные преимущества интеграции ИНС в системы информационной безопасности предприятий (рис. 6).

Необходимо отметить, что, по данным SANS, около 30 % экспертов по информационной безопасности убеждено в том, что технологии искусственного интеллекта способны увеличить эффективность детектирования неизвестных угроз [6].

Рассмотрим в процентном соотношении относительно стандартных методов метрики информационной безопасности, улучшаемые посредством интеграции искусственных нейронных сетей (рис. 7).

Большинство компаний, активно использующих ИНС в целях повышения эффективности работы систем защиты информации, подтверждает, что интеллектуальные технологии повышают эффективность расследования инцидентов, уменьшают время реакции на угрозы, повышают эффективность управления персоналом и т. д. Также многими представителями компаний подтверждается факт сокращения количества ложных срабатываний в результате интеграции нейронных сетей в системы информационной безопасности.

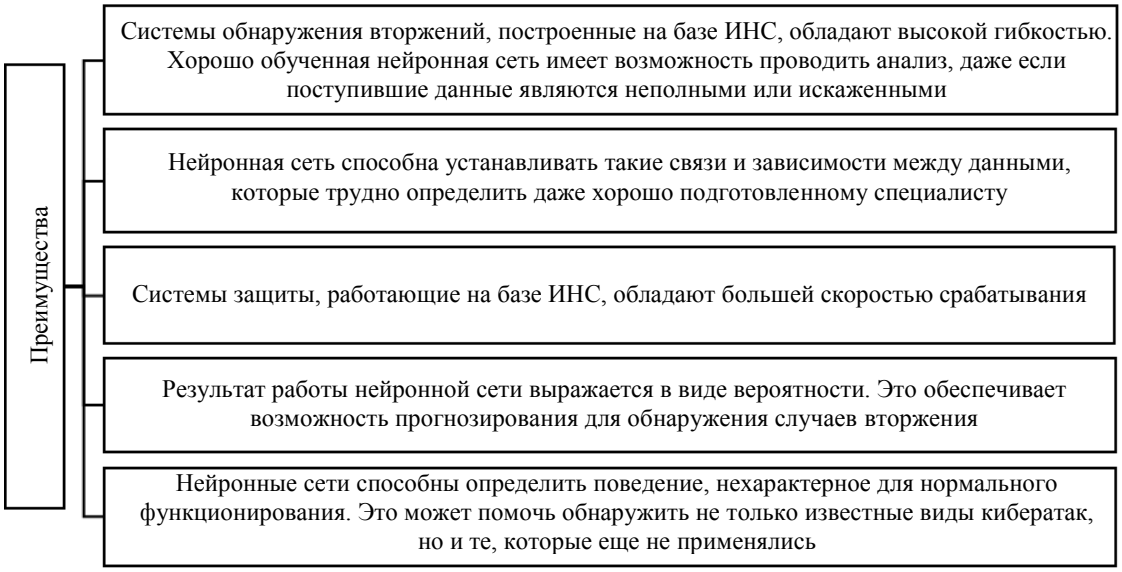


Рис. 6. Преимущества интеграции ИНС в сегменте информационной безопасности

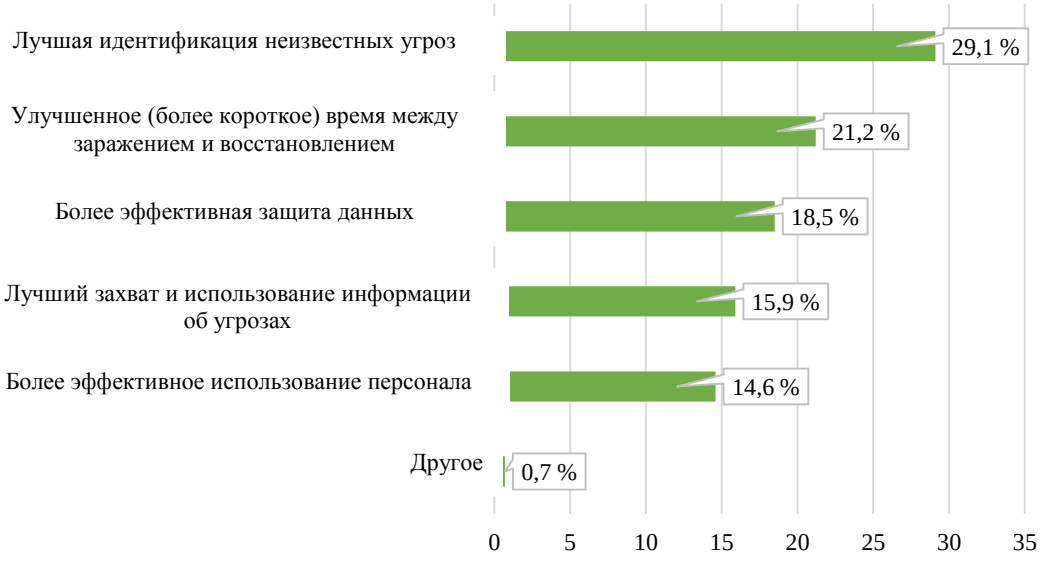


Рис. 7. Метрики информационной безопасности, улучшаемые посредством применения ИНС

Заключение

Из приведенных данных видно, что технологии ИНС вносят колоссальный вклад в борьбу с современными информационными угрозами. В подавляющем большинстве случаев интеллектуальные технологии сокращают время выявления проблем и последующего реагирования на инциденты, а также уменьшают расходы на управление персоналом. Эксплуатирующие в своих системах ИНС компании отмечают значительное повышение эффективности детектирования неизвестных угроз, а также повышение скорости анализа и обнаружения вредоносной активности на серверах.

Искусственный интеллект, в частности ИНС, является наукой и технологией создания интеллектуальных машин, подавляющее большинство которых представляет собой интеллектуальные компьютерные программы. Технологии ИИ в широком смысле подразумевают программное обеспечение, имеющее возможность выполнения задач посредством использования когнитивных способностей человека (например, распознавание речи, интерпретация визуальных образов, анализ логических операций, создание моделей будущего на основе накопленных данных и т. д.), что является наиболее эффективным инструментом в решении задач информационной безопасности на предприятиях.

Технологии ИНС являются одними из самых инновационных и прорывных достижений науки на сегодняшний день. ИНС повсеместно внедряются практически во всех сферах жизнедеятельности человека, начиная от бытовых и заканчивая профессиональными.

В данной работе подробно изучены вопросы, касающиеся интеграции искусственных нейронных сетей в системы информационной безопасности современных предприятий. В результате: определены основные сведения, касающиеся ИИ; факторы, которые определяют актуальность защиты информации; схема простой нейронной сети; схема искусственного нейрона; направления интеграции ИНС в сегменте информационной безопасности; преимущества интеграции ИНС в сегменте информационной безопасности и т. д.

Литература

1. *Афанасьева Д. В.* Применение искусственного интеллекта в обеспечении безопасности данных // Изв. ТулГУ. Технические науки. 2020. № 2. С. 151—154.
2. *Балановская А. В.* Анализ современного состояния угроз информационной безопасности предприятий // Информационная безопасность регионов. 2015. № 3(20). С. 9—15.
3. *Сырецкий Г. А.* Искусственный интеллект и производственная безопасность: настоящее и будущее // Интерэкспо Гео-Сибирь. 2016. Т. 5. № 1. С. 112—117.
4. *Тершуков Д. А.* Анализ современных угроз информационной безопасности // НБИ технологии. 2018. Т. 12. № 3. С. 6—12.
5. *Цветкова О. Л., Крепер А. И.* О применении теории искусственных нейронных сетей в решении задач обеспечения информационной безопасности // Символ науки. 2017. Т. 2. № 4. С. 105—107.
6. *Дыбина И. В., Славянов А. С.* Искусственный интеллект как инструмент повышения эффективности и устойчивости бизнеса // Экономика и бизнес: теория и практика. 2019. № 4-2. С. 67—70.

Evaluation of the relevance and effectiveness of the integration of artificial neural networks in information security systems

S. A. Dmitriev
Moscow Aviation Institute (National Research University), Moscow, Russia

One of the solutions to the problem of increasing the efficiency of information security systems, associated with the integration of intelligent tools and methods into these systems, is considered. The relevance and efficiency of using artificial neural networks in information security problems have been confirmed.

Keywords: intelligent tools, information security, neural networks, technology, efficiency.

Bibliography — 6 references. *Received April 29, 2021*

ДОВЕРЕННАЯ СРЕДА

УДК 004.052.42
DOI: 10.52190/2073-2600_2021_2_14

Реакционный метод противодействия атакам класса "отказ в обслуживании" с использованием прогнозирования характеристик корректирующих кодов

[1, 2] *Е. О. Карпухин*, канд. техн. наук; [1] *К. В. Мешавкин*
[1] Московский авиационный институт (национальный исследовательский университет), Москва, Россия
[2] Центр информационных технологий в проектировании РАН, г. Одинцово, Московская обл., Россия

Предложен реакционный метод защиты от атак класса "отказ в обслуживании", основанный на применении корректирующих кодов, которые способны восстанавливать утраченные вследствие возникновения перегрузок в сетях пакеты. Рассмотрены методы прогнозирования влияния атак класса "отказ в обслуживании" на передачу данных для выбора характеристик корректирующих кодов, которые нашли применение в имитационной модели системы массового обслуживания M/M/1/K. Представлена оценка точности формирования прогноза моделью с учетом изменения загруженности очереди в "узком" месте телекоммуникационной системы.

Ключевые слова: линейный сетевой код, информационное взаимодействие, противодействие перегрузкам, телекоммуникационные системы и сети.

Атаки класса "отказ в обслуживании" считают одними из наиболее распространенных и опасных в сетевом пространстве [1, 2]. Из-за большого числа различных технологий, программного обеспечения и оборудования существует множество различных видов DDoS-атак (распределенных атак класса "отказ в обслуживании", которые производятся не с одного, а с множества устройств), различающихся по субъекту воздействия, объекту воздействия и виду (процессу) воздействия [3].

С помощью DDoS-атак злоумышленник уменьшает емкость ресурсов атакуемой цели, таких, как пропускная способность или размер буфера (очереди), или доводит атакуемую систему до отказа за счет переполнения каналов данных, ведущих к ней (в случае пропускной способности), или перегрузки сервера (в случае размера буфера) с множества различных источников. В этом случае реальные пользователи сервисов атакуемой системы не могут получить доступ к ним. Кроме того, данные атаки могут вызвать отказы в оборудовании и потерю критических данных.

Защиту от DDoS-атак можно разделить на два основных класса: превентивную и реакционную [4]. Превентивная защита полагается на прогнозирование атаки и подготовку к ее смягчению еще до начала атаки, реакционная работает непосредственно во время и/или после атаки, защищая цель от истощения ресурсов.

Превентивные методы защиты являются крайне важным элементом в защите от сетевых атак. Однако они имеют высокую цену установки и поддержки. Кроме того, существует вероятность, что превентивная защита не сработает. В этих случаях реакционная защита является привлекательным вариантом и как дополнение к превентивной, и как самостоятельный метод защиты. Также реакционная защита использует трафик, который уже поступил в систему. Такая защита может быть отключена, когда на систему не производится атака, что делает ее крайне привлекательной с точки зрения цены установки и обслуживания. Недостатком реакционной системы защиты является то, что ей нужно время реагирования на атаку, что создает небольшую, но все же достаточно существенную задержку между началом атаки и началом работы реакционной защиты [5].

Карпухин Евгений Олегович, доцент, старший научный сотрудник.
E-mail: ret1987@yandex.ru
Мешавкин Константин Викторович, ассистент.
E-mail: meshavkin1996@gmail.com

Статья поступила в редакцию 26 апреля 2021 г.

В данной работе внимание сфокусировано на DDoS-атаках и воздействии помех умеренного уровня (планомерная нагрузка канала без угроз полного отключения системы) на систему с ограниченной пропускной способностью ("узкое" место), где использование кодирования имеет определенную эффективность (высокая вероятность потерь пакетов в системе приводит к резкому снижению эффективности, поэтому следует учитывать как нижнюю, так и верхнюю границы применимости кодирования для улучшения процесса передачи данных [6]) (рис. 1).

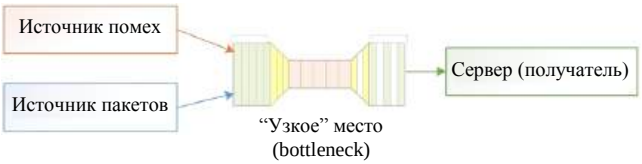


Рис. 1. Модель системы под действием рассматриваемого вида DDoS-атак

Методы прогнозирования перегрузок в сетях для выбора характеристик корректирующих кодов

Для выбора параметров кода, которые сделают применение кодирования эффективным, недостаточно полагаться только на текущие параметры системы, так как в этом случае кодирование будет "отставать" от реальных потерь. Иначе, к тому моменту, когда для данных будут добавлены избыточные пакеты в зависимости от характеристик сети (потерь пакетов, задержек и т. д.), потребуется другая корректирующая способность, а значит отправленные пакеты будут уже безвозвратно потеряны.

Если в системе возникнут потери и использование механизма перезапросов уже не будет столь эффективным, простейшим вариантом будет выбор таких параметров кода, при которых гарантировано отсутствие потерь в любой момент времени. Однако важно отметить, что хотя при соблюдении таких условий действительно получится добиться отсутствия потерь применением кодирования, реальный выигрыш данный метод будет давать только при высоких значениях потерь, а при малых потерях применение перезапросов зачастую оказывается эффективнее. Это связано с тем, что применение механизма квитирования хоть и замедляет передачу данных и увеличивает задержку за счет перезапросов при возникновении потерь, при очень малых (меньше 0,1 %) значениях потерь и небольшом (меньше 50 мс) времени передачи до получателя и обратно все запрошенные заново пакеты в итоге дойдут до приемной стороны [7]. При малых потерях большая избыточность значительно уменьшит интенсивность передачи данных, что может оказаться более существенным, чем уменьшение интенсивности передачи данных при использовании механизмов перезапроса. Кроме того, безосновательно предполагать, что потери на определенном промежутке времени не превысят заранее заданную величину в случае динамического процесса атаки, когда интенсивность атаки меняется в течение одного соединения/сеанса. В связи с этим предлагается использовать прогнозирование при подборе параметров кода. Оно позволит в зависимости от определенных условий в канале выбирать один из вариантов:

- Подбирать параметры кода, которые позволят минимизировать накладные расходы и достичь максимальной скорости кода, таким образом решая сразу две проблемы: большую и неэффективную избыточность при малых потерях и требование прогнозирования верхней границы потерь. При этом важно отметить, что можно прогнозировать как динамический процесс атак, так и статический для получения корректных параметров кода. Случай статического прогноза также является приоритетным, так как хотя сам поток статичен (интенсивность передачи данных не меняется), соединение часто длится непродолжительное время, а во время каждого соединения загруженность потока может изменяться. В этом случае имеет смысл производить анализ первичных потерь в канале и в соответствии с этим выбирать определенные параметры кода на весь период сеанса.
- Делать выбор между механизмом перезапроса и кодированием в зависимости от уровня потерь. При достаточно малых величинах потерь кодирование окажется менее эффективным даже с учетом того, что затраты на кодирование и декодирование малы. В таком случае имеет смысл отключать кодирование в принципе и использовать механизм квитирования. Это будет являться одним из вариантов внедрения гибридной системы с перезапросами и механизмом помехоустойчивого кодирования.

Таким образом, использование прогнозирования параметров кода является перспективной задачей. Поэтому важно рассмотреть цель, параметры, а также методы прогнозирования.

Выбор цели прогнозирования. Под целью прогнозирования будем понимать то, какие процессы прогнозируются в разработанном методе противодействия атакам класса "отказ в обслуживании". Можно производить краткосрочное реакционное прогнозирование, когда в зависимости от приходящих в систему пакетов производится прогнозирование состояния следующих пакетов или других параметров, таких, как средняя вероятность поте-

ри пакета в определенном промежутке, интенсивность передачи данных или загруженность очереди. Под краткосрочным прогнозированием понимается малое число значений, между которыми есть статистическая зависимость. Также имеется возможность производить долгосрочное прогнозирование, когда проводится превентивный анализ различных параметров и на их основе делается прогноз на определенный срок. Например, можно исследовать нагрузку на систему в течение недели и для каждого определенного дня или часа выдавать прогноз о возможной загруженности конечного устройства. Кроме того, возможно поквартальное прогнозирование, как это было сделано в работе [8].

Авторы предлагают использовать реакционное краткосрочное прогнозирование параметров канала на основе информации о потерянных или успешно принятых пакетах в связи с тем, что такой вариант позволит мгновенно выбрать параметры кода и в дальнейшем применить кодирование для предотвращения потерь вне зависимости от характера или вида атаки.

Методы прогнозирования атак класса "отказ в обслуживании". Так как существует множество методов прогнозирования атак класса "отказ в обслуживании", требуется рассмотреть различные методы и выбрать наиболее подходящий. Следует отметить, что существует две основные категории методов прогнозирования: качественные и количественные. Качественные методы основаны на мнении экспертов и являются по своей сути субъективными. Обычно они используются при отсутствии накопленных данных о модели [9]. Качественные методы больше подходят для средне- и долгосрочных прогнозов, а не для прогнозирования характеристик трафика, подверженного сильной флуктуации в краткосрочном интервале. В связи с этим в дальнейшем в работе будут рассмотрены именно количественные методы.

К одному из самых простых методов прогнозирования следующих в ряде величин относят линейную зависимость, когда предполагается, что следующее значение зависит от предыдущего. В условиях работы с системами M/M/1/K это может быть прогнозирование того, будет ли потерян следующий пакет в очереди или он будет успешно доставлен. В случае, если отправленный источником пакет успешно дошел до конечного устройства с очередью, предполагается, что следующий пакет также будет успешно доставлен. Если же последний пакет потерялся, то предполагается, что следующий пакет будет потерян.

Чтобы выбрать корректные параметры для кода информации только о последнем пакете недостаточно. Поэтому производится накопление информации об определенном (заданном заранее) количестве последних пакетов и по ней либо определяется средняя вероятность потерь на этом промежутке, либо производится попытка прогнозирования показателя ρ (загруженности очереди), по которым уже можно выбрать параметры кода. Конкретные параметры кода зависят от выбранного варианта кодирования.

Метод скользящих средних является эмпирическим методом для прогнозирования и сглаживания временных рядов. При его использовании с большим значением глубины прогнозирования реакция на изменение значений будет недостаточной для того, чтобы кривая ряда быстро изменила свое направление, а при малом значении глубины прогнозирования погрешность прогнозирования будет высока. Однако для прогнозирования параметра, который не требует быстрой реакции на его изменение, данный метод подходит хорошо и может быть использован как метод, дополняющий или направляющий другой метод прогнозирования.

Принцип полиномиального регрессионного анализа по заданным точкам заключается в подборе такой функции, которая как можно точнее аппроксимирует множество этих точек. В рамках прогнозирования параметров кода это означает подбор ряда точек, обобщенных по одному определенному параметру системы, и построение соответствующей регрессионной функции, по которой затем можно спрогнозировать следующий параметр. При этом для успешного прогнозирования требуется не только выбрать подходящий параметр системы, но и подобрать корректную степень полинома. В противном случае у функции прогноза могут возникнуть излишние колебания, что приведет к крайне неточным результатам.

Результаты полиномиального регрессионного анализа зачастую теряют точность с увеличением удаленности точки прогноза от последнего известного значения, однако эти результаты позволяют достаточно точно определить тенденцию направления ряда точек. При этом требуется наличие знания о предыдущих значениях в системе. Для предложенной модели такой вариант прогнозирования является валидным, так как имеется возможность запоминать информацию о любых параметрах системы, которые известны прогнозирующему устройству. Кроме того, предлагается производить именно краткосрочное реакционное прогнозирование, когда требуется определять тенденцию кривой определенного параметра.

Развитие информационных технологий привело к возникновению интереса к прогнозированию

различными интеллектуальными методами, в том числе с применением нейронных сетей. Прогнозирование DDoS-атак нейросетевыми методами исследовано в работах [10—12].

Данный метод предпочтителен в системах, где трафик атакующего является статическим или имеет предсказуемый характер. В этом случае можно произвести обучение заранее, а затем использовать уже настроенную модель только для самого прогнозирования без применения обучения. В противном случае потребуется применение обучения во время передачи данных на основе трафика, который в данный момент поступает в систему. При этом требуется, чтобы система обработки пакетов имела запас вычислительных мощностей, при котором применение обучения нейронной сети не придаст излишней нагрузки системе, а сеанс являлся бы длительным. Если сеанс будет коротким, то применение нейронных сетей может только навредить, так как в начале обучения нейронные сети имеют крайне высокий показатель ошибочных результатов.

По результатам представленного анализа предлагается использовать полиномиальный регрессионный анализ для прогнозирования параметров системы, так как он с высокой точностью позволяет прогнозировать тенденции на коротком периоде времени.

Выбор показателей прогнозирования. Важно использовать те параметры, которые позволят подобрать корректные длины информационной и кодовой последовательностей кода. Другими словами, эти параметры должны быть коррелированы с параметрами кода.

Предлагается использовать один из двух показателей: ρ (загруженность очереди) или среднюю вероятность потерь пакетов на определенном промежутке. Важно отметить, что оба параметра связаны, так как повышение загруженности очереди в итоге приводит к потерям при ее переполнении. При этом более сильная нагрузка на очередь коррелирует с повышением числа потерь в сети. Разница заключается в сложности прогнозирования. Точный прогноз загруженности очереди может заранее дать возможность подобрать корректные параметры кода и, как следствие, избежать лишних потерь. Однако прогнозирование загруженности очереди является более сложной задачей в связи с невозможностью непосредственно узнать показатели загруженности очереди в "узком" месте.

Прогнозирование средней вероятности является наиболее очевидным вариантом, так как выбор параметров кода напрямую зависит в первую очередь именно от количества потерянных пакетов на определенном промежутке.

Для этого требуется запоминать некоторое количество последних пакетов в массив для вычисления средней вероятности потерь на данном промежутке. Длину такого массива пакетов называют глубиной прогнозирования. Ее выбирают исходя из размера окна очереди. Кроме того, для прогнозирования требуется запоминать последние значения параметра, поэтому средняя вероятность потерь также сохраняется в массив. После этого можно использовать данный массив для получения предполагаемого значения вероятности потерь, которая должна быть определена только на следующем промежутке. Описанный процесс показан на рис. 2.

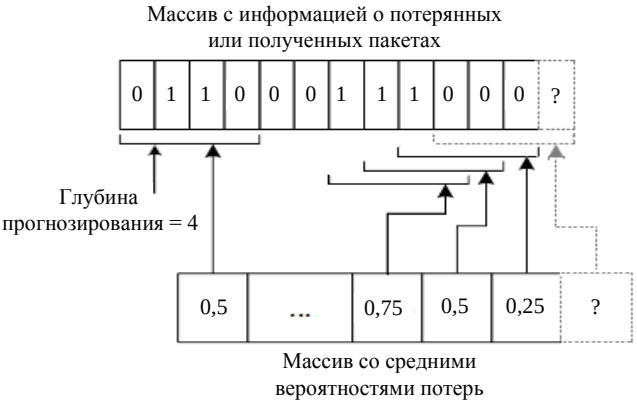


Рис. 2. Массивы информации о потере или получении пакета и средней вероятности потерь

Получение прогнозируемого параметра предлагается производить с помощью полиномиального регрессионного метода: выбирается фиксированная величина степени полинома, а затем для каждого набора данных с определенной глубиной прогнозирования составляется полином, с помощью которого и прогнозируется следующий в ряде параметр.

Параметр загруженности очереди ρ связан с интенсивностью поступления данных в очередь λ формулой $\rho = \frac{\lambda}{\mu}$. При этом μ (интенсивность обслуживания пакетов) в рамках данной работы является фиксированной величиной, для упрощения модели выбранной равной 1. Следовательно, приведенное соотношение можно упростить до $\rho \approx \lambda$. В связи с этим если предположить, что возможно с достаточной точностью спрогнозировать загруженность очереди, то это также дает знание и об интенсивности поступления пакетов в очередь, что в случае разработанной модели является основным входным параметром.

Это позволяет заранее провести анализ потерь на различных фиксированных значениях интен-

сивности передачи данных, собрав статистику по потерянным пакетам, а затем подобрав соответствующие каждому значению интенсивности кодовые параметры.

Для прогнозирования загруженности очереди информации о потере пакетов недостаточно. В связи с этим предлагается использовать средний показатель задержки между двумя пакетами. При этом прогнозирование будет производиться с использованием большей глубины прогнозирования, чем в предыдущем пункте, так как изменение интенсивности входящего потока происходит не так часто и не так критично, как переполнение очереди и, соответственно, потери пакетов. Предполагается использовать данный прогноз как дополняющий предыдущий для того, чтобы подготовить нужные параметры кода к возможному возникновению потерь.

Структура метода противодействия последствиям атак класса "отказ в обслуживании" с использованием прогнозирования характеристик корректирующих кодов

Вычисление параметров кода по спрогнозированной средней вероятности потерь проводится по формуле

$$t = \frac{n-k}{2},$$

где t — корректирующая способность кода;
k — число информационных пакетов;
n — длина кодовой последовательности.

Параметр t показывает количество пакетов, которое требуется восстановить. Его можно получить из средней вероятности потерь на заданном промежутке, так как этот показатель и прогнозируется. Параметр n выбирают в зависимости от различных условий, в том числе от максимальной длины очереди. После этого можно получить k, таким образом спрогнозировав параметры кода. В случае, если получается нецелое число, можно либо изменить n, либо округлить в меньшую сторону k (при этом скорость кода понизится).

Для разных величин интенсивности поступления данных в очередь λ можно получить корректные параметры кода для каждой из величин λ. Для этого использована модель, разработанная в [13]. Поиск оптимальных длин информационной (K) и кодовой (N) последовательностей сетевого кода при моделировании системы массового обслуживания M/M/1/K производится по следующим критериям: максимизация скорости кода и минимизация длины кодовой последовательности при условии вероятности потери пакета, равной нулю.

На рис. 3 приведена структурная схема предложенного реакционного метода противодействия атакам класса "отказ в обслуживании". В основе метода прогнозирования стоит модель массового обслуживания M/M/1/K, выбор которой обусловлен наиболее подходящими для работы параметрами модели: для вычисления времени обработки пакета и для генерации пакетов используется экспоненциальное распределение, применяется одно устройство массового обслуживания для обработки пакетов и имеется возможность использовать вариативную длину очереди. Также к модели добавляется алгоритм управления перегрузками очереди RED для имитации реальных систем обработки пакетов. Данная система позволит моделировать процесс передачи пакетов между источником и получателем, что необходимо для исследования эффективности предложенного метода.

Главной составляющей частью метода является оценка корректирующих способностей кода (t_1, t_2) по спрогнозированным показателям модели СМО, выбор параметров n, k кода с учетом наибольшей спрогнозированной корректирующей способности и использование их как результата прогнозирования.

Для использования описанного метода требуется провести прогнозирование параметров кода. Параметры кода выбирают на основе двух показателей: средней вероятности потери пакета на определенном промежутке и загруженности очереди ρ. Прогнозирование этих показателей производят по задержке пакетов и информации о том, потерян пакет или нет.

Рис. 3. Структура предложенного метода противодействия последствиям атак класса "отказ в обслуживании"

Следующим этапом является выбор параметров кода по спрогнозированным показателям. Для выбора параметров кода по загруженности очереди сначала получены данные для разных значений ρ (со статичным входным трафиком) [13], а затем по полученным результатам построена матрица, по которой можно выбирать параметры кода для различных значений загруженности очереди. Из полученных двух значений параметров кода в определенный момент времени выбирается худший случай, используемый как результат прогнозирования, т. е. производится выбор кода, обладающего наибольшей корректирующей способностью.

Оценка эффективности предложенного метода противодействия атакам класса "отказ в обслуживании"

После завершения сборки имитационной модели с реализованным методом противодействия атакам можно приступить к проверке работоспособности предложенного прототипа. Для этого требуется поставить условия, при которых результаты прогнозирования разработанного метода будут считаться успешными.

Для этого планируется рассматривать насколько правильно были выбраны параметры кода при прогнозировании по сравнению с оптимальными параметрами кода. Превышение спрогнозированного параметра избыточности допустимо, так как в данном случае будет лишь понижена скорость кода, а значения ниже оптимальных крайне нежелательны, поскольку в таком случае пакет не будет подлежать восстановлению кодированием и потребуется делать его перезапрос. Кроме того, нужно оценить, дает ли преимущество такой метод в целом, в связи с чем требуется сравнить количество запрошенных заново пакетов данным методом и при отсутствии кодирования в принципе.

Важно отметить, что для тестирования в условиях, максимально приближенных к реальным, трафик атакующего является не статическим, а импульсным, меняющимся во времени. Это явно видно на графиках прогноза загруженности очереди.

Были взяты показатели, при которых не возникало перегрузок в очереди устройства массового обслуживания ("узком" месте сети, на которое направлена атака), когда невозможно восстановить все пакеты. Перед получением прогноза параметров кода были получены графики прогноза загруженности очереди ρ (рис. 4) и средней вероятности потери пакета на более коротком промежутке (рис. 5).

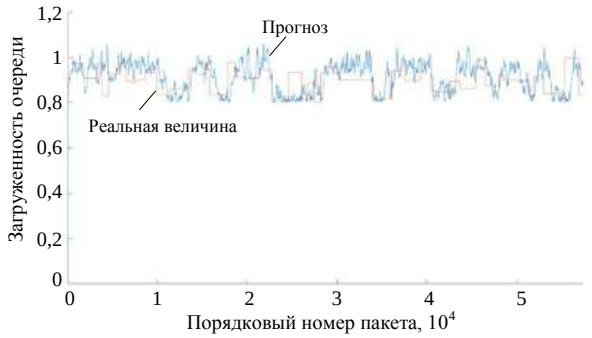


Рис. 4. Прогноз загруженности очереди для невысокой нагрузки

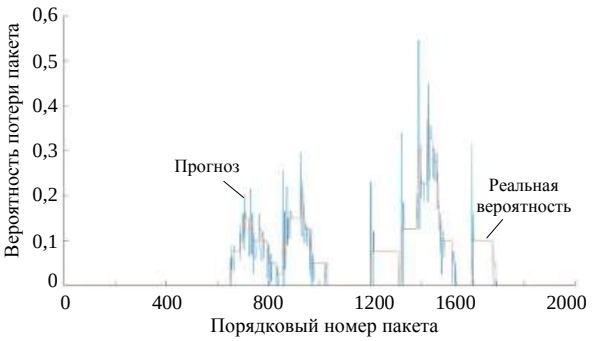


Рис. 5. Прогноз средней вероятности потери пакета для невысокой нагрузки на коротком промежутке

Затем были получены графики прогнозов параметров кода по двум показателям и общий график худшего случая на более коротких промежутках (рис. 6 и 7).

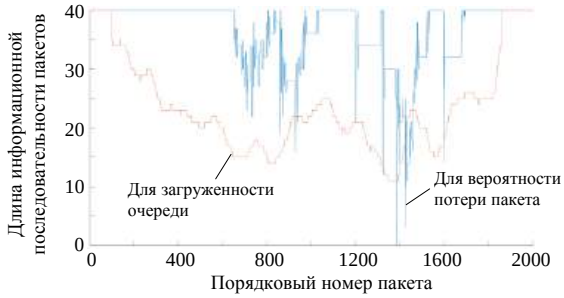


Рис. 6. Прогноз параметров кода по двум показателям для невысокой нагрузки на коротком промежутке

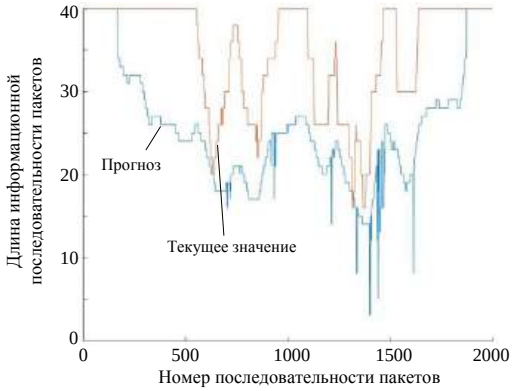


Рис. 7. Итоговый прогноз параметров кода для невысокой нагрузки на коротком промежутке

Также был получен график сравнения количества потерянных пакетов, которые требуют перезапроса, с использованием описанного метода и без применения кодирования (рис. 8).

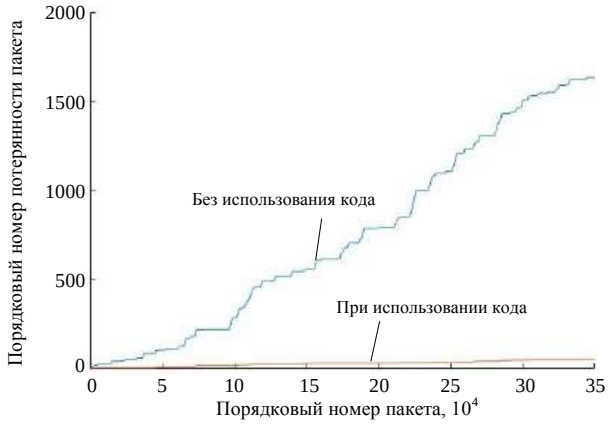


Рис. 8. Сравнение количества потерянных пакетов без использования кода и с использованием алгоритма для невысокой нагрузки

Из графиков видно, что прогнозы имеют достаточно высокую точность. При этом итоговый прогноз параметров кода имеет среднюю точность 98,17 %. Использование алгоритма позволило сократить количество перезапрашиваемых пакетов на 96,99 %. В таблице приведены значения по последним двум показателям за несколько экспериментов.

Значения по контрольным показателям за несколько экспериментов

№ экспер.	Точность прогноза параметров кода, %	Сокращение количества перезапрашиваемых пакетов, %
1	98,36	97,12
2	97,74	96,82
3	98,28	96,96
4	98,01	97,34
5	98,44	96,71

Заключение

Выяснено, что эффективность разработанного метода защиты на основе прогнозирования достаточно высока (более 95 %). При этом она снижается с увеличением интенсивности атак класса "отказ в обслуживании", т. е. с возникновением перегрузок на "узком" месте. Это связано с тем, что из-за экспоненциального характера генерации пакетов скорость передачи пакетов периодически резко повышается при одной и той же входной интенсивности. В результате прогнозы параметров кода и по загруженности очереди, и по средней вероятности потери пакетов не успевают реагировать на резкие импульсные изменения в интенсивности передачи пакетов и впоследствии возникающие потери.

По полученным в эксперименте графикам можно сделать выводы о границах применимости разработанного метода. С текущими настройками прогнозирования даже с учетом кодирования система не справится с восстановлением пакетов, если на коротком промежутке (порядка 40 пакетов) потерь будет более 50 %, а средняя нагрузка на "узкое" место превысит 1,1. Важно отметить, что хотя в этом случае алгоритм будет использовать механизм перезапросов, все еще будет возможно восстановить пакеты, однако тогда задержки для получения пакета сильно увеличатся. Нижней границей при этом является значение нагрузки на очередь менее 0,8, когда возникают редкие единичные потери, легко восстанавливаемые перезапросами без необходимости внесения дополнительной избыточности кодированием.

Исследование выполнено в рамках проведения научных исследований по теме № 0071-2019-0001.

Литература

1. *Сачков И. К.* Ddos атаки: технологии, тенденции, реагирование и оформление доказательств // Защита информации. Инсайд. 2010. № 6(36). С. 59—63.

2. *Report C.* 2018 Annual Cybersecurity Report: The evolution of malware and rise of artificial intelligence 2018 [Электронный ресурс]. URL: https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

3. *Сердечный А. Л., Андреев Д. А.* DDoS-атаки: классификация, статистическая модель // Информация и безопасность. 2010. Т. 13. № 2. С. 289—290.

4. *Dongwoo Kwon, Hyeonwoo Kim, Donghyeok An, Hongtaek Ju.* DDoS attack volume forecasting using a statistical approach: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 8—12 May 2017.

5. *Sens R.* Proactive vs. Reactive: Which is better for DDoS defence? [Электронный ресурс]. URL: https://gdpr.report/news/2018/01/29/proactive-vs-reactive-better-ddos-defence/

6. *Карпухин Е. О., Бритвин Н. В., Мешавкин К. В.* Исследование эффективности применения перспективных корректирующих кодов в гибридной ARQ/FEC системе на прикладном уровне // Новые информационные технологии в автоматизированных системах. 2017. № 20. С. 181—185.

7. *Карпухин Е. О., Мешавкин К. В.* Варианты использования корректирующих кодов в гибридной системе ARQ/FEC // Электромагнитные волны и электронные системы. 2017. Т. 22. № 8. С. 43—50.

8. *Бармина С. С., Таджибаева Ф. М.* Прогнозирование DDoS-атак типа SYN на Web-ресурсы // National Interests: Priorities and Security. 2018. Т. 14. № 11. С. 2162—2174.

9. *Шамаев И.* Обзор методов прогнозирования [Электронный ресурс]. URL: http://ivan-shamaev.ru/overview-forecast-methods/ (дата обращения: 25.02.2020).

10. *Тарасов Я. В.* Исследование применения нейронных сетей для обнаружения низкоинтенсивных DDoS-атак прикладного уровня // Вопросы кибербезопасности. 2017. Т. 24. № 5. С. 23—29.

11. *Частикова В. А., Власов К. А., Картамышев Д. А.* Обнаружение DDoS-атак на основе нейронных сетей с применением метода роя частиц в качестве алгоритма обучения // Фундаментальные исследования. 2014. Т. 8. № 4. С. 829—832.

12. *Слеповичев И. И., Ирматов П. В., Комарова М. С., Бежин А. А.* Обнаружение DDoS-атак нечеткой нейронной сетью // Изв. Саратовского ун-та. 2009. Т. 9. № 3. С. 84—89.

13. *Karpukhin E. O., Meshavkin K. V., Britvin N. V.* Simulation modeling of congestion in telecommunication systems to determine the optimal parameters of linear network code // Revista Inclusiones. 2020. V. 7. numEspecial. P. 105—121.

A reactive method for countering denial-of-service attacks using the forecast of the characteristics of error-correcting codes

[1, 2] *E. O. Karpukhin*, [1] *K. V. Meshavkin*

[1, 2] Moscow Aviation Institute (National Research University), Moscow, Russia

[2] Design Information Technologies Center of the RAS, Odintsovo, Moscow region, Russia

A reactive method of protection against denial-of-service attacks is proposed, based on the use of error-correcting codes that can restore packets lost due to the network congestion. Methods for forecasting the consequences of denial-of-service attacks on data transmission for selecting for the characteristics of error-correcting codes that have been used in the simulation model of the M/M/1/K queuing system are considered. The estimation of the accuracy of forming a forecast by the model is presented, taking into account changes in the queue load in bottleneck of the telecommunications system.

Keywords: linear network code, data-driven interaction, congestion avoidance, telecommunication systems and networks.

Bibliography — 13 references. *Received April 26, 2021*

ЭЛЕКТРОННАЯ ПОДПИСЬ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 003.26
DOI: 10.52190/2073-2600_2021_2_22

Протоколы коллективной и слепой подписи на конечных группах с многомерной цикличностью

Н. А. Молдовян, д-р техн. наук; *А. А. Костина*; *А. А. Курышева*
Санкт-Петербургский федеральный исследовательский центр РАН, Санкт-Петербург, Россия

Рассмотрено построение протоколов слепой, коллективной и слепой коллективной цифровой подписи на конечных группах, обладающих многомерной цикличностью. В качестве алгебраического носителя используются четырехмерные конечные коммутативные ассоциативные алгебры, мультипликативная группа которых обладает двухмерной или четырехмерной цикличностью в зависимости от выбора структурного коэффициента, используемого для задания операции векторного умножения.

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

Широко используемые протоколы электронной цифровой подписи (ЭЦП) основаны на вычислительной сложности задачи факторизации (ЗФ) [1] и задачи дискретного логарифмирования (ЗДЛ) [2, 3]. Однако ожидаемый в ближайшем будущем прорыв в технологии квантовых вычислений делает крайне актуальной разработку криптосхем, устойчивых к атакам с использованием квантовых компьютеров. Постквантовые протоколы ЭЦП должны основываться на вычислительно сложных задачах, отличных от ЗФ и ЗДЛ, поскольку для квантового компьютера известны полиномиальные алгоритмы решения каждой из этих задач [4—6].

В области постквантовой криптографии значительное внимание криптографическое сообщество уделяет разработке криптосхем на алгебрах [7, 8], булевых функциях [9], решетках [10] и линейных кодах [11, 12]. В рамках всемирного конкурса по разработке кандидатов на постквантовые криптографические стандарты в качестве финалистов выбраны следующие схемы ЭЦП [13]: Crystals-Dilithium, Falcon и Rainbow. Существенным недостатком этих схем является большой размер открытого ключа, закрытого ключа и подписи. Поэтому представляет интерес поиск новых, более практичных схем электронной подписи.

Одним из новых подходов к разработке практических постквантовых схем ЭЦП является использование скрытой ЗДЛ, определяемой обычно в некоммутативных конечных ассоциативных алгебрах (КАА). Различные формы СЗДЛ предложены для разработки схем электронной подписи на основе некоммутативных КАА [14—16]. Интерес к этому подходу связан с тем, что он позволяет построить схемы ЭЦП с достаточно малыми размерами открытого ключа и подписи. Для практики представляют интерес не только протоколы обычной индивидуальной ЭЦП, но также и протоколы коллективной и слепой подписи. Недавно [17] на коммутативных КАА была предложена схема слепой подписи.

Авторами предлагается новая формула для вычисления открытого ключа и построения протоколов коллективной, слепой и слепой коллективной подписи с использованием в качестве алгебраического носителя коммутативных КАА, в которых мультипликативная группа обладает многомерной цикличностью.

Предварительные сведения

Понятие слепой подписи, проблема обеспечения неотслеживаемости (анонимности) пользователей и базовый механизм построения протоколов слепой ЭЦП описаны достаточно подробно в работах [18, 19]. Понятие коллективной подписи как значения фиксированного размера, заменяющего набор произвольного числа индивидуальных под-

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

Статья поступила в редакцию 8 апреля 2021 г.

писей, и частные варианты построения протоколов коллективной ЭЦП представлены в работах [20, 21].

Конечные алгебры задают следующим образом. Пусть конечное m-мерное векторное пространство определено над конечным простым полем $GF(p)$ или конечным расширением двоичного поля $GF(2^z)$, где z — степень расширения поля $GF(2)$. Если дополнительно к операциям сложения и скалярного умножения векторов задана операция векторного умножения векторов, являющаяся дистрибутивной слева и справа относительно операции сложения, то полученную алгебраическую структуру называют конечной m-мерной алгеброй. Некоторый элемент алгебры **A** (m-мерный вектор) можно представить в следующих двух видах: $\mathbf{A} = (a_0, a_1, \ldots, a_{m-1})$, где a_i — координаты вектора, т. е. $a_i \in GF(p)$ или $a_i \in GF(2^z)$; $\mathbf{A} = \sum_{i=0}^{m-1} a_i \mathbf{e}_i$, где $\mathbf{e}_i$ — базисные векторы; $a_i \mathbf{e}_i$ — компоненты вектора **A**.

Операцию векторного умножения векторов **A** и $\mathbf{B} = \sum_{j=0}^{m-1} b_j \mathbf{e}_j$ удобно задать по правилу перемножения каждой компоненты вектора **A** с каждой компонентой вектора **B** по следующей формуле:

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

где всевозможные произведения пар базисных векторов $\mathbf{e}_i \mathbf{e}_j$ заменяются на соответствующие однокомпонентные векторы вида $\lambda\, \mathbf{e}_k$ (λ — структурная константа), указанные в ячейках на пересечении i-й строки и j-го столбца в так называемой таблице умножения базисных векторов (ТУБВ). Если $\lambda = 1$, то в ТУБВ указывается только базисный вектор $\mathbf{e}_k$. Если заданная операция векторного умножения обладает свойством ассоциативности (коммутативности), то алгебра называется ассоциативной (коммутативной). В коммутативной алгебре равенство $\mathbf{AB} = \mathbf{BA}$ выполняется для произвольной пары векторов **A** и **B**.

Для задания ассоциативной алгебры разрабатывается ТУБВ, которая определяет операцию векторного умножения (далее просто операцию умножения), обладающую свойством ассоциативности, т. е. такую операцию умножения, для которой для всевозможных троек векторов **A**, **B** и **C** имеет место равенство

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

С учетом формул (1) и (2) легко показать, что ТУБВ, которая задает выполнимость равенства

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

для всевозможных троек базисных векторов, определяет ассоциативное векторное умножение.

Для раскрытия термина «многомерная цикличность» используют понятие базиса группы. Это минимальный по численности набор элементов группы, всевозможные произведения степеней которых порождают все значения в группе. Конечной группой с μ-мерной цикличностью называется группа, в которой базис включает μ элементов одинакового порядка. Примером группы с двухмерной цикличностью является мультипликативная группа Γ двухмерной КАА с операцией умножения, заданной по табл. 1 [22], при значении λ, являющемся квадратичным вычетом в $GF(p)$. Порядок группы Γ равен $\Omega = (p-1)^2$. Примеры групп с μ-мерной цикличностью для значений $\mu > 2$ рассмотрены в работах [22, 23].

Таблица 1

Задание двухмерной КАА над полем $GF(p)$ ($\lambda \neq 0$)

•	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_0$	$\mathbf{e}_0$	$\mathbf{e}_1$
$\mathbf{e}_1$	$\mathbf{e}_1$	$\lambda\mathbf{e}_0$

Алгебраический носитель

В качестве алгебраического носителя в предлагаемых протоколах коллективной и слепой ЭЦП используется четырехмерная алгебра, заданная по табл. 2 над полем $GF(p)$ при значении характеристики поля, равном простому числу $p = 2q + 1$, где q — 256-битное простое число (генерируется путем перебора простых q до тех пор, пока не будет получено простое значение $2q + 1$).

Таблица 2

Задание 4-мерной коммутативной КАА, обладающей четырехмерной цикличностью ($\lambda = 4$)

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

Утверждение 1. Векторное умножение, определенное по табл. 2, является ассоциативным.

Доказательство выполняется проверкой справедливости формулы (3) для всевозможных троек базисных векторов.

Утверждение 2. Четырехмерная КАА, заданная табл. 2, содержит глобальную двухстороннюю единицу в виде вектора **E** = (0, 0, 1, 0).

Доказательство. Используя формулу (1), получаем $\mathbf{AE} = \sum_{i=0}^{3} a_i (\mathbf{e}_i \mathbf{e}_2) = \sum_{i=0}^{3} a_i \mathbf{e}_i = \mathbf{A}$ и $\mathbf{EA} = \sum_{j=0}^{3} a_j (\mathbf{e}_2 \mathbf{e}_j) = \sum_{j=0}^{3} a_j \mathbf{e}_j = \mathbf{A}$. Утверждение 2 доказано.

Вектор **A** называют обратимым, если векторное уравнение **AX** = **E** имеет единственное решение, которое обозначают как $\mathbf{A}^{-1}$ и называют обратным значением вектора **A**. Очевидно выполняются соотношения $\mathbf{AA}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{E}$. Для нахождения условий обратимости и необратимости векторов в рассматриваемой КАА следует рассмотреть векторное уравнение **AX** = **E**, которое сводится к решению следующей системы из четырех линейных уравнений с четырьмя неизвестными координатами вектора **X** = (x_0, x_1, x_2, x_3):

$$\begin{cases} a_2 x_0 + a_3 x_1 + a_0 x_2 + a_1 x_3 = 0; \\ \lambda a_3 x_0 + a_2 x_1 + a_1 x_2 + \lambda a_0 x_3 = 0; \\ \lambda a_0 x_0 + a_1 x_1 + a_2 x_2 + \lambda a_3 x_3 = 1; \\ a_1 x_0 + a_0 x_1 + a_3 x_2 + a_2 x_3 = 0. \end{cases} \quad (4)$$

Главный определитель Δ системы (4) равен

$$\Delta = \begin{vmatrix} a_2 & a_3 & a_0 & a_1 \\ \lambda a_3 & a_2 & a_1 & \lambda a_0 \\ \lambda a_0 & a_1 & a_2 & \lambda a_3 \\ a_1 & a_0 & a_3 & a_2 \end{vmatrix} = a_2 \begin{vmatrix} a_2 & a_1 & \lambda a_0 \\ a_1 & a_2 & \lambda a_3 \\ a_0 & a_3 & a_2 \end{vmatrix} -$$

$$- a_3 \begin{vmatrix} \lambda a_3 & a_1 & \lambda a_0 \\ \lambda a_0 & a_2 & \lambda a_3 \\ a_1 & a_3 & a_2 \end{vmatrix} + a_0 \begin{vmatrix} \lambda a_3 & a_2 & \lambda a_0 \\ \lambda a_0 & a_1 & \lambda a_3 \\ a_1 & a_0 & a_2 \end{vmatrix} -$$

$$- a_1 \begin{vmatrix} \lambda a_3 & a_2 & a_1 \\ \lambda a_0 & a_1 & a_2 \\ a_1 & a_0 & a_3 \end{vmatrix} =$$

$$= a_2 \left[a_2 \left(a_2^2 - \lambda a_3^2 \right) - a_1 \left(a_1 a_2 - \lambda a_0 a_3 \right) + \lambda a_0 \left(a_1 a_3 - a_0 a_2 \right) \right] -$$

$$- a_3 \left[\lambda a_3 \left(a_2^2 - \lambda a_3^2 \right) - a_1 \left(\lambda a_0 a_2 - \lambda a_1 a_3 \right) + \lambda a_0 \left(\lambda a_0 a_3 - a_1 a_2 \right) \right] +$$

$$+ a_0 \left[\lambda a_3 \left(a_1 a_2 - \lambda a_0 a_3 \right) - a_2 \left(\lambda a_0 a_2 - \lambda a_1 a_3 \right) + \lambda a_0 \left(\lambda a_0^2 - a_1^2 \right) \right] -$$

$$- a_1 \left[\lambda a_3 \left(a_1 a_3 - a_0 a_2 \right) - a_2 \left(\lambda a_0 a_3 - a_1 a_2 \right) + a_1 \left(\lambda a_0^2 - a_1^2 \right) \right] = \ldots =$$

$$= \lambda^2 \left(a_0^2 + a_3^2 \right)^2 - 4\lambda a_0^2 a_3^2 + \left(a_1^2 + a_2^2 \right)^2 - 4\lambda a_0^2 a_3^2 -$$

$$- 2\lambda \left(a_0^2 + a_3^2 \right) \left(a_1^2 + a_2^2 \right) + 8\lambda a_0 a_1 a_2 a_3 = \ldots =$$

$$= \left(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 \right)^2 - 4 \left(\lambda a_0 a_3 - a_1 a_2 \right)^2.$$

Система уравнений (4) имеет единственное решение, если $\Delta \neq 0$, и не имеет решений, если $\Delta = 0$. В результате имеем условие обратимости

$$\left(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 \right)^2 - 4 \left(\lambda a_0 a_3 - a_1 a_2 \right)^2 \neq 0 \quad (5)$$

и условие необратимости:

$$\left(\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 \right)^2 = 4 \left(\lambda a_0 a_3 - a_1 a_2 \right)^2. \quad (6)$$

Множество всех обратимых векторов образует мультипликативную группу алгебры.

Утверждение 3. Если структурная константа λ является квадратичным невычетом в поле *GF*(*p*), то четырехмерная КАА, заданная по табл. 2, содержит $\eta = 2p^2 - 1$ необратимых векторов, а ее мультипликативная группа имеет порядок, равный значению $\Omega = (p^2 - 1)^2$.

Доказательство. Условие необратимости (6) задает следующие два случая:

$$\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = 2\lambda a_0 a_3 - 2 a_1 a_2 \Rightarrow$$

$$\Rightarrow \lambda \left(a_0 - a_3 \right)^2 = \left(a_1 - a_2 \right)^2;$$

$$\lambda a_0^2 - a_1^2 - a_2^2 + \lambda a_3^2 = -2\lambda a_0 a_3 + 2 a_1 a_2 \Rightarrow$$

$$\Rightarrow \lambda \left(a_0 + a_3 \right)^2 = \left(a_1 + a_2 \right)^2.$$

Поскольку λ является квадратичным невычетом, в первом случае равенство выполняется только при условии $\left(a_0 - a_3 \right)^2 = \left(a_1 - a_2 \right)^2 = 0$. Это дает p^2 различных наборов координат a_0, a_1, a_2 и a_3, включая вектор (0, 0, 0, 0). Во втором случае равенство выполняется только при условии $\left(a_0 + a_3 \right)^2 = \left(a_1 + a_2 \right)^2 = 0$. Это дает другие p^2 различных наборов координат a_0, a_1, a_2 и a_3, включая вектор (0, 0, 0, 0). Поэтому имеем $\eta = 2p^2 - 1$ и $\Omega = p^4 - \eta = (p^2 - 1)^2$. Утверждение 3 доказано.

Утверждение 4. Если структурная константа λ является квадратичным вычетом в поле *GF*(*p*), то четырехмерная КАА, заданная по табл. 2, содержит $\eta = 4p^3 - 6p^2 + 4p - 1$ необратимых векторов, а ее мультипликативная группа имеет порядок, равный значению $\Omega = (p - 1)^4$.

Доказательство. Поскольку λ является квадратичным невычетом условие необратимости (6) задает следующие два случая:

$$\left(a_0 \sqrt{\lambda} - a_3 \sqrt{\lambda} \right)^2 = \left(a_1 - a_2 \right)^2 \Rightarrow a_0 \sqrt{\lambda} - a_3 \sqrt{\lambda} =$$

$$= \pm \left(a_1 - a_2 \right);$$

$$\left(a_0 \sqrt{\lambda} + a_3 \sqrt{\lambda} \right)^2 = \left(a_1 + a_2 \right)^2 \Rightarrow a_0 \sqrt{\lambda} + a_3 \sqrt{\lambda} =$$

$$= \pm \left(a_1 + a_2 \right).$$

Каждое их двух последних условий распадается на два новых условия. В результате получаем 4 условия, одному из которых удовлетворяет произвольный необратимый вектор (a_0, a_1, a_2, a_3). Эти условия представлены в левом столбце табл. 3. В правом столбце представлено число необратимых векторов, задаваемое каждым из четырех указанных слева условий.

Таблица 3

Число необратимых векторов, соответствующих четырем частным условиям необратимости для случая, когда λ является квадратичным вычетом

Частные условия	Число различных наборов координат (a_0, a_1, a_2, a_3)
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = a_1 - a_2 = 0$	p^2, включая (0,0,0,0)
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = a_1 + a_2 = 0$	p^2, включая (0,0,0,0)
$a_0\sqrt{\lambda} - a_3\sqrt{\lambda} = \pm(a_1 - a_2) \neq 0$	$2p(p-1)^2$
$a_0\sqrt{\lambda} + a_3\sqrt{\lambda} = \pm(a_1 + a_2) \neq 0$	$2p(p-1)^2$

Суммируя значения в правом столбце и учитывая, что нулевой вектор входит в два подмножества необратимых векторов, получаем полное число необратимых векторов:

$$\eta = p^2 + p^2 + 2p(p-1)^2 + 2p(p-1)^2 = \\ = 4p^3 - 6p^2 + 4p - 1.$$

Для порядка мультипликативной группы алгебры получаем следующую формулу: $\Omega = p^4 - \eta = (p-1)^4$. Утверждение 4 доказано.

Из табл. 2 следует, что рассматриваемая четырехмерная КАА содержит следующие подалгебры с единицей $\mathbf{E} = (0, 0, 1, 0)$, мультипликативные группы которых обладают двухмерной цикличностью: множество всех векторов вида $(a_0, 0, a_2, 0)$; множество всех векторов вида $(0, a_1, a_2, 0)$; множество всех векторов вида $(0, 0, a_2, a_3)$. Также легко показать, что в случае, когда структурная константа λ является квадратичным вычетом, каждая из этих трех подалгебр обладает двухмерной цикличностью, что предопределяет четырехмерную цикличность рассматриваемой четырехмерной алгебры.

Таким образом, как и в случае четырехмерной коммутативной КАА, представленной в [17], множество всех обратимых векторов КНАА, заданной по табл. 2, образует группу порядка $(p-1)^4$, обладающую четырехмерной цикличностью, т. е. она включает некоторый базис $\langle \mathbf{B}_1, \mathbf{B}_2, \mathbf{B}_3, \mathbf{B}_4 \rangle$ из четырех векторов порядка $p - 1 = 2q$.

Базовая схема подписи

Рассмотрим векторы $\mathbf{Q}_1 = \mathbf{B}_1^2$, $\mathbf{Q}_2 = \mathbf{B}_2^2$, $\mathbf{Q}_3 = \mathbf{B}_3^2$ и $\mathbf{Q}_4 = \mathbf{B}_4^2$, порядок которых равен простому числу q. Эти четыре вектора образуют базис $\langle \mathbf{Q}_1, \mathbf{Q}_2, \mathbf{Q}_3, \mathbf{Q}_4 \rangle$, задающий примарную группу порядка q^4, обладающую четырехмерной цикличностью. Пары этих векторов образуют базисы различных примарных подгрупп порядка q^2, обладающих двухмерной цикличностью. Тройки этих векторов образуют базисы различных примарных подгрупп порядка q^3, обладающих двухмерной цикличностью.

Пусть даны два равновероятных случайных вектора $\mathbf{Q}$ и $\mathbf{G}$ порядка q. Вычисление открытого ключа $\mathbf{Y}$ зададим по формуле

$$\mathbf{Y} = \mathbf{Q}^x \mathbf{G}^u \chi, \qquad (7)$$

где $x < q$, $u < q$ и $\chi < p$ — случайные натуральные числа, являющиеся секретными (образуют личный секретный ключ владельца открытого ключа $\mathbf{Y}$).

Процедуру формирования цифровой подписи к некоторому документу M зададим в виде следующего алгоритма.

1. Сгенерировать разовый секретный ключ в виде тройки натуральных чисел $k < q$, $t < q$ и $\rho < p$ и вычислить разовый открытый ключ в виде вектора $\mathbf{R} = \mathbf{Q}^k \mathbf{G}^t \rho$.

2. Используя некоторую специфицированную хэш-функцию $f_h(...)$, вычислить ее значение e от документа, к которому присоединено значение $\mathbf{R}$: $e = f_h(M, \mathbf{R})$.

3. Вычислить значение $s = k - ex \bmod q$.

4. Вычислить значение $d = t - eu \bmod q$.

5. Вычислить значение $\sigma = \rho\chi^{-e} \bmod p$.

Подписью является четверка натуральных чисел (e, s, d, σ).

Процедура проверки подлинности ЭЦП к документу M включает следующие шаги.

1. Вычислить вектор $\mathbf{R}' = \mathbf{Y}^e \mathbf{Q}^s \mathbf{G}^d \sigma$.

2. Вычислить значение хэш-функции e' от документа, к которому присоединено значение $\mathbf{R}'$: $e = f_h(M, \mathbf{R}')$.

3. Если $e' = e$, то подпись признается подлинной, в противном случае — ложной.

Доказательство корректности описанной схемы ЭЦП (показываем, что правильно вычисленная подпись проходит проверочную процедуру как подлинная ЭЦП) выполняется следующим образом:

$$\mathbf{R}' = \mathbf{Y}^e \mathbf{Q}^s \mathbf{G}^d \sigma = \mathbf{Q}^{ex} \mathbf{G}^{eu} \chi^e \mathbf{Q}^{k-ex} \mathbf{G}^{t-eu} \rho\chi^{-e} = \\ = \mathbf{Q}^k \mathbf{G}^t \rho = \mathbf{R} \Rightarrow e' = e.$$

Протокол коллективной подписи

Пусть каждый из некоторых m пользователей желает подписать электронный документ M. Для этого они могут использовать следующий протокол коллективной ЭЦП, формирующий коллективную подпись фиксированного размера для произвольного числа подписантов.

1. Каждый i-й подписант ($i = 1, 2, \ldots, m$) генерирует разовый секретный ключ в виде тройки натуральных чисел $k_i < q$, $t_i < q$ и $\rho_i < p$ и вычисляет разовый открытый ключ в виде вектора $\mathbf{R}_i = \mathbf{Q}^{k_i}\mathbf{G}^{t_i}\rho_i$. Затем он рассылает значение $\mathbf{R}_i$ всем остальным подписантам.

2. Все участники протокола вычисляют коллективный разовый открытый ключ в виде вектора

$$\mathbf{R} = \prod_{i=1}^{m}\mathbf{R}_i = \mathbf{Q}^{\sum_i k_i}\mathbf{G}^{\sum_i t_i}\left(\prod_{i=1}^{m}\rho_i \bmod p\right)$$

и первый элемент коллективной ЭЦП в виде значения $e = f_h(M, \mathbf{R})$.

3. Каждый i-й подписант ($i = 1, 2, \ldots, m$), используя свой секретный ключ (x_i, u_i, ρ_i), вычисляет значения

$$s_i = k_i - ex_i \bmod q;$$
$$d_i = t_i - eu_i \bmod q;$$
$$\sigma_i = \rho_i\chi_i^{-e} \bmod p$$

и рассылает их остальным участникам протокола.

4. Каждый подписант вычисляет элементы s, d и σ коллективной ЭЦП:

$$s = \sum_{i=1}^{m}s_i \bmod q;\ \ d = \sum_{i=1}^{m}d_i \bmod q;\ \ \sigma = \prod_{i=1}^{m}\sigma_i \bmod p.$$

Процедура проверки подлинности коллективной ЭЦП (e, s, d, σ) к документу M включает по сравнению с проверочной процедурой базовой схемы один дополнительный шаг, заключающийся в формировании коллективного открытого ключа, и имеет следующий вид.

1. Используя открытые ключи подписантов, вычислить коллективный открытый ключ в виде вектора

$$\mathbf{Y} = \prod_{i=1}^{m}\mathbf{Y}_i = \mathbf{Q}^{\sum_i x_i}\mathbf{G}^{\sum_i u_i}\left(\prod_{i=1}^{m}\chi_i \bmod p\right),$$

где $\mathbf{Y}_i = \mathbf{Q}^{x_i}\mathbf{G}^{u_i}\rho_i$ — открытый ключ i-го подписанта ($i = 1, 2, \ldots, m$).

2. Вычислить вектор $\mathbf{R}' = \mathbf{Y}^e\mathbf{Q}^s\mathbf{G}^d\sigma$.

3. Вычислить значение хэш-функции e' от документа, к которому присоединено значение $\mathbf{R}'$: $e = f_h(M, \mathbf{R}')$.

4. Подпись признается подлинной, если выполняется равенство $e' = e$.

Доказательство корректности протокола коллективной ЭЦП:

$$\mathbf{R}' = \mathbf{Y}^e\mathbf{Q}^s\mathbf{G}^d\sigma = \left(\prod_{i=1}^{m}\mathbf{Y}_i\right)^e\mathbf{Q}^{\sum_i(k_i - ex_i)}\mathbf{G}^{\sum_i(t_i - eu_i)} \times$$
$$\times\left(\prod_{i=1}^{m}\sigma_i \bmod p\right) = \mathbf{Q}^{e\sum_i x_i}\mathbf{G}^{e\sum_i u_i}\left(\prod_{i=1}^{m}\chi_i^e \bmod p\right) \times$$
$$\times\mathbf{Q}^{\sum_i k_i}\mathbf{Q}^{e\sum_i x_i}\mathbf{G}^{\sum_i t_i}\mathbf{G}^{e\sum_i u_i}\left(\prod_{i=1}^{m}\sigma_i \bmod p\right) =$$
$$= \left(\prod_{i=1}^{m}\chi_i^e \bmod p\right)\mathbf{Q}^{\sum_i k_i}\mathbf{G}^{\sum_i t_i}\left(\prod_{i=1}^{m}\rho_i\chi_i^{-e} \bmod p\right) =$$
$$= \mathbf{Q}^{\sum_i k_i}\mathbf{G}^{\sum_i t_i}\left(\prod_{i=1}^{m}\rho_i \bmod p\right) = \mathbf{R} \Rightarrow e' = e.$$

Протокол слепой подписи

В протоколе слепой подписи некоторый пользователь (именуемый далее клиентом) готовит некоторый электронный документ M и получает подлинную подпись некоторого подписанта таким образом, что подписант не имеет возможности получения доступа к содержанию документа и формирует слепую подпись, в которую клиентом внесены случайные ослепляющие множители. Последние клиент удаляет и получает подлинную подпись подписанта к документу M.

Предлагаемый протокол слепой подписи описывается следующим образом.

1. Подписант генерирует разовый секретный ключ в виде тройки чисел $k < q$, $t < q$ и $\rho < p$, вычисляет разовый открытый ключ $\bar{\mathbf{R}} = \mathbf{Q}^k\mathbf{G}^t\rho$ и передает его клиенту.

2. Клиент генерирует равновероятные ослепляющие значения в виде натуральных чисел $\varepsilon < q$, $\tau < q$, $\gamma < q$ и $\mu < p$ и вычисляет вектор $\mathbf{R} = \bar{\mathbf{R}}\mathbf{Y}^{\varepsilon}\mathbf{Q}^{\tau}\mathbf{G}^{\gamma}\mu$ и первый элемент e подлинной подписи: $e = f_h(M, \mathbf{R})$. Затем клиент вычисляет первый элемент слепой ЭЦП $\bar{e} = e - \varepsilon \bmod q$ и передает его подписанту.

3. Подписант вычисляет второй, третий и четвертый элементы слепой подписи (которые потом передает клиенту):

$$\bar{s} = k - \bar{e}x \bmod q;\ \ \bar{d} = t - \bar{e}u \bmod q;\ \ \bar{\sigma} = \rho\chi^{-\bar{e}} \bmod p.$$

4. Получив второй, третий и четвертый элементы слепой подписи, клиент вычисляет соответствующие значения подлинной подписи:

$$s = \bar{s} + \tau \bmod q;\ d = \bar{d} + \gamma \bmod q;\ \sigma = \bar{\sigma}\mu \bmod p.$$

Для проверки подлинности ЭЦП используют проверочную процедуру базовой схемы ЭЦП.

Доказательство корректности протокола слепой ЭЦП выполняется как демонстрация того, что сформированная в ходе протокола подлинная подпись действительно положительно проходит проверочную процедуру. Действительно, учитывая равенство $\bar{\mathbf{R}} = \mathbf{Y}^{\bar{e}}\mathbf{Q}^{\bar{s}}\mathbf{G}^{\bar{d}}\bar{\sigma}$, имеем

$$\mathbf{R}' = \mathbf{Y}^{e}\mathbf{Q}^{s}\mathbf{G}^{d}\sigma = \mathbf{Y}^{\bar{e}+\varepsilon}\mathbf{Q}^{\bar{s}+\tau}\mathbf{G}^{\bar{d}+\gamma}\bar{\sigma}\mu =$$
$$= \mathbf{Y}^{\bar{e}}\mathbf{Q}^{\bar{s}}\mathbf{G}^{\bar{d}}\bar{\sigma}\mathbf{Y}^{\varepsilon}\mathbf{Q}^{\tau}\mathbf{G}^{\gamma}\mu = \bar{\mathbf{R}}\mathbf{Y}^{\varepsilon}\mathbf{Q}^{\tau}\mathbf{G}^{\gamma}\mu =$$
$$= \mathbf{R} \Rightarrow e' = e.$$

Протокол слепой коллективной подписи

Механизм ослепляющих множителей легко встраивается в протокол коллективной подписи. Это приводит к построению протокола слепой коллективной подписи. Практическая потребность в протоколах такого типа может возникнуть, например, в системах электронной наличности (электронных денег), в которых в процедуре генерации электронных банкнот участвует несколько банков. Другим примером является система тайного электронного голосования, в которой для повышения уровня безопасности электронный бюллетень для голосования подписывается несколькими подписантами. В каждом из этих примеров требуется подписывать и хранить очень большое количество электронных сообщений, что делает актуальной задачу сохранения размера подписи, задаваемой базовой схемой ЭЦП, для произвольного числа подписантов. Для протоколов коллективной и слепой коллективной подписи актуальным является вопрос о корректности регистрируемых в удостоверяющем центре открытых ключей.

В случае практического применения обычных индивидуальных цифровых подписей по умолчанию предполагается, что все владельцы открытых ключей генерируют эти ключи корректно. Под корректностью генерации открытых ключей здесь понимается то, что открытые ключи, которые регистрируются и распространяются удостоверяющим центом, являются сформированными в строгом соответствии с процедурой, специфицированной используемой схемой ЭЦП. Действительно, если пользователи не будут так поступать, то они будут владеть бесполезными открытыми ключами: пользователи не смогут формировать цифровые подписи к каким бы то ни было электронным сообщениям, которые могли бы быть проверены с помощью таких неправильных открытых ключей.

Пользователи также не смогут использовать неправильные открытые ключи для выполнения атаки на схему ЭЦП. Таким образом, для пользователей нет никакого смысла регистрировать неправильные открытые ключи. Поэтому неявно предполагается, что они этого делать и не будут. Тем не менее часто удостоверяющие центры устанавливают такой регламент регистрации, при котором от пользователей требуется подписать свою заявку на регистрацию своего открытого ключа цифровой подписью, проверяемой регистрируемым открытым ключом. Эти случаи соответствуют применению процедуры проверки корректности открытых ключей. Очевидно, что подписать свою заявку на регистрацию открытого ключа пользователь сможет только в случае, когда регистрируемый открытый ключ сформирован в строгом соответствии с процедурами генерации открытых ключей, специфицируемой используемой схемой ЭЦП.

В отличие от отсутствия строгой необходимости выполнения процедур проверки корректности открытых ключей в протоколах обычной индивидуальной ЭЦП, в протоколах коллективной и слепой коллективной ЭЦП данное требование является принципиальным. Дело в том, что нарушители могут выступить в роли пользователей и зарегистрировать специальным способом сгенерированные открытые ключи, которые ими не могут быть использованы для генерации своих цифровых подписей, но могут быть использованы для подделки коллективной ЭЦП, соответствующей некоторому фиксированному подмножеству пользователей. Для этого нарушитель вычисляет неправильный открытый ключ, настроенный строго на заданное подмножество открытых ключей, зарегистрированных в некотором удостоверяющем центре. Затем он регистрирует его в удостоверяющем центре. Если такая регистрация нарушителю удается, то он может от имени коллектива подписывающих, на который был настроен его зарегистрированный открытый ключ (сам нарушитель тоже входит в данный коллектив), формировать правильные коллективные ЭЦП.

Нарушитель не может формировать ни индивидуальные ЭЦП членов коллектива подписывающих, ни коллективные ЭЦП, соответствующие каким-либо подмножествам членов этого коллектива. Однако он может успешно подделывать

единственный вариант коллективной ЭЦП, что является существенным нарушением безопасности протокола коллективной ЭЦП. Поэтому в случае практического использования протоколов коллективной ЭЦП для придания юридической силы электронным сообщениям и документам следует в явном виде задать требование выполнения процедуры проверки корректности формирования каждого регистрируемого открытого ключа.

Заключение

Предложена новая схема ЭЦП, основанная на вычислительной трудности представления открытого ключа в виде произведения степеней элементов, входящих в базис группы с многомерной цикличностью. На ее основе предложены протоколы слепой, коллективной и слепой коллективной подписи. В качестве алгебраического носителя использована КАА, мультипликативная группа которой обладает четырехмерной цикличностью.

Для дальнейшего исследования важным представляется изучение вычислительной сложности использованной трудной задачи, включая рассмотрение случая применения квантового вычислителя. Этот вопрос связан с поиском гомоморфизмов использованной четырехмерной КАА в поле $GF(p)$, аналогичных найденным в [24] для случая двухмерной КАА, и требует отдельного изучения.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 21-57-54001-Вьет_а) и бюджетной темы № 0060-2019-0010.

Литература

1. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithms / /IEEE Transactions on Information Theory. 1985. V. IT-31. № 4. P. 469—472.

2. *Rivest R. L., Shamir A., Adleman L. M.* A Method for Obtaining Digital Signatures and Public Key Cryptosystems // Communications of the ACM. 1978. V. 21. № 2. P. 120—126.

3. *Chiou S. Y.* Novel Digital Signature Schemes based on Factoring and Discrete Logarithms // International J. Security and Its Applications. 2016. V. 10. № 3. P. 295—310.

4. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.

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

6. *Jozsa R.* Quantum algorithms and the Fourier transform // Proc. Roy. Soc. London, Ser A. 1988. V. 454. P. 323—337.

7. *Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.* Cryptographic Algorithms on Groups and Algebras // J. Math. Sci. 2017. V. 223. № 5. P. 629—641.

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

9. *Agibalov G. P.* ElGamal cryptosystems on Boolean functions // Прикладная дискретная математика. 2018. № 42. С. 57—65. DOI: 10.17223/20710410/42/4

10. *Hoffstein J., Pipher J., Schanck J. M., Silverman J. H., Whyte W., Zhang Zh.* Choosing parameters for NTRU Encrypt. Cryptographers' Track at the RSA Conference — CTA-RSA 2017. — Springer LNCS, 2017. V. 10159. P. 3—18.

11. *Alamelou Q., Blazy O., Cauchie S., Gaborit Ph.* A code-based group signature scheme // Designs, Codes and Cryptography. 2017. V. 82. № 1–2. P. 469—493.

12. *Kosolapov Y. V., Turchenko O. Y.* On the construction of a semantically secure modification of the McEliece cryptosystem functions // Прикладная дискретная математика. 2019. № 45. P. 33—43. DOI 10.17223/20710410/45/4

13. *Post-Quantum Cryptography. Round3 Submissions*. [Электронный ресурс]. Режим доступа: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions (дата обращения: 10.04.2021).

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

15. *Молдовян А. А., Молдовян Д. Н.* Постквантовая схема ЭЦП на основе скрытой задачи дискретного логарифмирования в четырехмерной конечной алгебре // Вопросы защиты информации. 2019. № 2. С. 18—22.

16. *Minh Nguyen Hieu, Moldovyan A. A., Moldovyan N. A., Canh Hoang Ngoc*. A New Method for Designing Post-Quantum Signature Schemes // J. Communications. 2020. V. 15. № 10. P. 747—754. DOI: 10.12720/jcm.15.10.747-754

17. *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

18. *Chaum D.* Security without identification: Transaction systems to make big brother obsolete// Communications of the AMS. 1985. V. 28. № 10. P. 1030—1044.

19. *Camenisch J. L., Piveteau J.-M., Stadler M. A.* Blind Signatures Based on the Discrete Logarithm Problem: Advances in Crypology — EUROCRYPT '94. — Springer LNCS, 1995. V. 950. P. 428—432.

20. *Moldovyan N. A.* Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Int. J. Network Security. 2011. V. 13. № 1. P. 22—30.

21. *Moldovyan A. A., Moldovyan N. A.* Blind Collective Signature Protocol Based on Discrete Logarithm Problem // Int. J. Network Security. 2010. V. 11. № 2. P. 106—113.

22. *Moldovyan N. A., Moldovyanu P. A.* New primitives for digital signature algorithms // Quasigroups and Related Systems. 2009. V. 17. № 2. P. 271—282.

23. *Moldovyan N. A.* Fast Signatures Based on Non-Cyclic Finite Groups // Quasigroups and Related Systems. 2010. V. 18. № 1. P. 83—94.

24. *Гурьянов Д. Ю., Молдовян Д. Н., Цехановский В. В.* Конечные группы двухмерных векторов: варианты задания и синтез алгоритмов цифровой подписи // Вопросы защиты информации. 2010. № 1. С. 7—13.

Collective and blind signature protocols on finite groups with multidimensional cyclicity

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

Construction of the blind, collective, and blind collective digital signature protocols on finite groups with multi-dimensional cyclicity is considered. The applied algebraic carrier represents a four-dimensional finite commutative associative algebra, the multiplicative group of which has two-dimensional or four-dimensional cyclicity depending on the choice of the structural coefficient used to specify the vector multiplication operation.

Keywords: information security, digital signature, collective signature, blind signature, finite associative algebra, commutative algebra, multi-dimensional cyclicity.

Bibliography — 24 references. *Received April 8, 2021*

УДК 003.26
DOI: 10.52190/2073-2600_2021_2_30

Схемы цифровой подписи с удвоенным проверочным уравнением

А. А. Молдовян, д-р техн. наук; *Н. А. Молдовян*, д-р техн. наук;
Д. Н. Молдовян, канд. техн. наук; *Р. Ш. Фахрутдинов*, канд. техн. наук
Санкт-Петербургский федеральный исследовательский центр РАН, Санкт-Петербург, Россия

Удвоение проверочного уравнения использовано для построения схем электронной цифровой подписи, основанных на вычислительной трудности скрытой задачи дискретного логарифмирования. Этот конструктивный прием позволяет использовать один из элементов подписи в качестве множителя в проверочном уравнении. Благодаря последнему обеспечивается возможность использования скрытой группы, обладающей двухмерной цикличностью, и выполнение усиленного критерия постквантовой стойкости. Два новых алгоритма цифровой подписи предложены в качестве практичных постквантовых криптосхем.

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

Предварительные данные

Одним из направлений разработки постквантовых схем с открытым ключом, в том числе алгоритмов электронной цифровой подписи (ЭЦП), является использование вычислительной трудности скрытой задачи дискретного логарифмирования (СЗДЛ), задаваемой в достаточно разнообразных формах [1—3].

Общепринятая формулировка задачи дискретного логарифмирования (ЗДЛ) состоит в нахождении целочисленного значения x, удовлетворяющего уравнению $Y = G^x$, где G — генератор циклической группы достаточно большого простого порядка q; Y — заданный элемент указанной группы. Обычно в двухключевых криптосхемах Y является открытым ключом, а x ($x < q$) — личным секретным ключом владельца открытого ключа ($x < q$). Для классического компьютера неизвестны алгоритмы с полиномиальной временной сложностью решения ЗДЛ в подгруппах мультипликативной группы простого конечного поля $GF(p)$ и в других конечных циклических группах. Поэтому до появления на практике квантовых компьютеров алгоритмы и протоколы, основанные на вычислительной сложности ЗДЛ, являются безопасными. Однако к атакам с использованием квантового компьютера они не являются стойкими, так как для последнего известен полиномиальный алгоритм решения ЗДЛ в конечной циклической группе [4], включающий задание периодической функции $f(i, j) = Y^i G^j$ от двух целочисленных переменных, i и j, имеющей период, длина которого определяется значением x:

$$Y^i G^j = Y^{i-1} G^{j+x} \Rightarrow f(i, j) = f(i - 1, j + x).$$

Квантовый компьютер чрезвычайно эффективно выполняет дискретное преобразование Фурье [5, 6], откуда вычисляются длины имеющихся периодов функции $f(i, j)$, в том числе и значение $(-1, x)$.

Скрытая ЗДЛ возникает в случае, когда двухключевая схема строится таким образом, что значения Y и G используются для вычисления элементов открытого ключа, однако по крайней мере одно из них является скрытым, т. е. соответствующий элемент открытого ключа представляет собой образ одного из значений Y и G, полученный путем выполнения над последним маскирующей операции, обладающей свойством взаимной коммутативности с операцией экспоненцирования. В схеме открытого распределения ключей маскируется один из указанных элементов [1], а в схемах ЭЦП — оба. Удобным алгебраическим носителем схем ЭЦП, основанных на СЗДЛ, являются конечные некоммутативные ассоциативные алгебры (КНАА) размерности $m = 4, 6, 8$. При перечисленных значениях размерности имеется достаточно большой выбор алгебр с разнообразными свойствами и сохраняется возможность обеспечения приемлемой производительности процедур генерации и проверки подлинности ЭЦП.

Молдовян Александр Андреевич, профессор.
E-mail: maa1305@yandex.ru
Молдовян Николай Андреевич, профессор.
E-mail: nmold@mail.ru
Молдовян Дмитрий Николаевич, преподаватель.
E-mail: mdn.spectr@mail.ru
Фахрутдинов Роман Шафкатович, заведующий лабораторией "Кибербезопасность и постквантовые криптосистемы".
E-mail: fahr@cobra.ru

Статья поступила в редакцию 23 апреля 2021 г.

При построении схем ЭЦП, основанных на СЗДЛ, используют некоторые критерии, которые ориентированы на предотвращение возможности непосредственного применения квантового компьютера для вычисления значения x. Один из критериев состоит в требовании того, чтобы построение периодических функций по открытым параметрам криптосхемы, содержащим период, зависящий от x, приводило к получению функций, значения которых лежат в различных циклических группах.

В ряде схем ЭЦП открытый ключ представляет собой следующие три вектора КНАА с глобальной двухсторонней единицей: $\mathbf{Y} = \mathbf{A}\mathbf{N}^{x}\mathbf{A}^{-1}$, $\mathbf{Z} = \mathbf{B}\mathbf{N}\mathbf{B}^{-1}$ и $\mathbf{T} = \mathbf{A}\mathbf{E}_{\mathbf{N}}\mathbf{B}^{-1}$, где $\mathbf{A}$ и $\mathbf{B}$ — секретные векторы, используемые как параметры маскирующей операции автоморфного отображения; $\mathbf{E}_{\mathbf{N}}$ — локальная двухсторонняя единица необратимого вектора $\mathbf{N}$, задающего скрытую циклическую группу; $\mathbf{T}$ — согласующий параметр, присутствующий в уравнении проверки подписи. По открытому ключу может быть задана периодическая функция $\mathbf{F}(i, j) = \mathbf{Y}^{i}\mathbf{T}\mathbf{Z}^{j}$, включающая период длины $(-1, x)$. Однако она принимает значения, лежащие в различных циклических группах, являющихся подмножествами элементов КНАА, используемой в качестве алгебраического носителя. Поэтому известный квантовый алгоритм [4] нахождения длины периода не может быть применен.

Другой, более общий критерий задает требование вычислительной неосуществимости построения периодической функции, включающей период, зависящий от x. Второй критерий является более общим и ориентирован на обеспечение стойкости к потенциально возможным новым квантовым атакам с использованием алгоритмов нахождения периода функций, принимающих значения как в конечной циклической группе, так и вне ее. Общий критерий постквантовой стойкости может быть сформулирован следующим образом: *на основе использования открытых параметров схемы ЭЦП должно быть вычислительно невозможным задание периодической функции, содержащей период, зависящий от значения дискретного логарифма*. В [7, 8] для построения схем ЭЦМ, удовлетворяющих этому критерию, в качестве скрытой группы использована коммутативная группа, обладающая двухмерной цикличностью, т. е. коммутативная группа, порождаемая всевозможными степенями двух элементов, $\mathbf{G}$ и $\mathbf{Q}$, обладающих одним и тем же значением простого порядка q и принадлежащих различным циклическим подгруппам.

Для удовлетворения общего критерия постквантовой стойкости открытый ключ представляют в виде следующей тройки векторов: $\mathbf{Y} = \mathbf{A}\mathbf{G}^{x}\mathbf{A}^{-1}$, $\mathbf{Z} = \mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{B}^{-1}$ и $\mathbf{T} = \mathbf{A}\mathbf{B}^{-1}$, где $\mathbf{G}$ — генератор скрытой циклической группы; $\mathbf{A}$ и $\mathbf{B}$ — секретные параметры маскирующей операции автоморфного отображения; $\mathbf{T}$ — согласующий параметр. Легко показать, что периодические функции, задаваемые на основе элементов открытого ключа, могут содержать только периоды, длина которых определяется значением порядка элементов $\mathbf{G}$ и $\mathbf{Q}$, составляющих базис скрытой коммутативной группы с двухмерной цикличностью, т. е. значением простого числа q.

Однако вектор $\mathbf{Q}$ вносит свой вклад при вычислении правой части проверочного уравнения, который учитывается введением дополнительного элемента подписи, представляющего собой вектор $\mathbf{S}$, входящий в правую часть проверочного уравнения в качестве множителя. Наличие подобного элемента в ЭЦП обусловливает возможность легкой подделки подписи путем использования $\mathbf{S}$ в качестве подгоночного параметра. Для предотвращения такой возможности в схемах ЭЦП [7, 8] используют прием удвоения проверочного уравнения, состоящий в следующем. Открытый ключ удваивается, т. е. представляется в виде первого и второго открытых ключей, вычисляемых таким способом, что может быть вычислена одна и та же подпись, удовлетворяющая проверочному соотношению, записанному как для первого, так и для второго открытого ключа. При этом подделки подписи для первого и для второго ключа приводят к разным значениям подписи.

В целом прием удвоения проверочного уравнения представляется источником некоторого класса схем ЭЦП, основанных на вычислительной трудности СЗДЛ и удовлетворяющих общему критерию постквантовой стойкости. Пока предложено только несколько схем ЭЦП, разработанных с использованием этого приема.

В целях расширения упомянутого класса схем ЭЦП авторы предлагают новые схемы подписи и обсуждают их стойкость к подделке подписи путем использования подгоночного параметра.

Используемый алгебраический носитель

В качестве алгебраического носителя схем ЭЦП предлагается использовать четырехмерные КНАА, задаваемые над простым конечным полем $GF(p)$ с 384-битной характеристикой $p = 2q + 1$ (где q — простое число), описанные в работе [9]. Данные КНАА содержат $2^{-1}p(p + 1)$ коммутативных групп порядка $(p - 1)^2$, обладающих двухмерной цикличностью [9]. При этом легко предложить алгоритм генерации векторов порядка q, принад-

лежащих группам такого типа. В частности, может быть использована КНАА, операция векторного умножения в которой задана по табл. 1. Использование прореженных таблиц умножения базисных векторов обеспечивает снижение вычислительной сложности операций умножения и экспоненцирования, а следовательно, повышение производительности алгоритмов генерации и проверки подлинности ЭЦП.

Таблица 1

Задание второй четырехмерной КНАА ($\lambda \neq 0$) с глобальной двухсторонней единицей вида (0, 0, 1, 1) [9]

•	$\mathbf{e}_0$	$\mathbf{e}_1$	$\mathbf{e}_2$	$\mathbf{e}_3$
$\mathbf{e}_0$	0	$\lambda\mathbf{e}_3$	$\mathbf{e}_0$	0
$\mathbf{e}_1$	$\lambda\mathbf{e}_2$	0	0	$\mathbf{e}_1$
$\mathbf{e}_2$	0	$\mathbf{e}_1$	$\mathbf{e}_2$	0
$\mathbf{e}_3$	$\mathbf{e}_0$	0	0	$\mathbf{e}_3$

Схема ЭЦП с двухэлементной подписью

Пусть даны два случайных вектора, **Q** и **G**, порядка q, принадлежащие одной коммутативной группе с двухмерной цикличностью. Вычисление открытого ключа зададим в виде двух пар векторов, ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$), вычисляемых по формулам

$$\mathbf{Y}_1 = \mathbf{A}\mathbf{G}^x\mathbf{B}^{-1};\ \mathbf{Z}_1 = \mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{A}^{-1}; \qquad (1)$$

$$\mathbf{Y}_2 = \mathbf{D}\mathbf{G}^x\mathbf{B}^{-1};\ \mathbf{Z}_2 = \mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{D}^{-1}, \qquad (2)$$

где $x < q$ — случайное натуральное число;
A, **B** и **D** — случайные векторы, которые вместе с числом x образуют личный секретный ключ владельца открытого ключа.

Процедуру формирования цифровой подписи к некоторому документу M зададим в виде следующего алгоритма.

1. Сгенерировать случайные натуральные числа $k < q$ и $t < q$ и вычислить векторы $\mathbf{R}_1 = \mathbf{A}\mathbf{G}^k\mathbf{Q}^t\mathbf{A}^{-1}$ и $\mathbf{R}_2 = \mathbf{D}\mathbf{G}^k\mathbf{Q}^t\mathbf{D}^{-1}$.

2. Используя некоторую специфицированную хэш-функцию $f_h(\ldots)$, вычислить ее значение e от документа с присоединенными векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $e = f_h(M, \mathbf{R}_1, \mathbf{R}_2)$.

3. Вычислить значение $s = e^{-2}(k - ex - e) \bmod q$.

4. Вычислить значение $d = e^{-2}(t - e) \bmod q$.

5. Вычислить вектор $\mathbf{S} = \mathbf{B}\mathbf{G}^s\mathbf{Q}^d\mathbf{B}^{-1}$.

Подписью является пара значений (e, **S**).

Процедура проверки подлинности ЭЦП к документу M включает следующие шаги.

1. Вычислить векторы $\mathbf{R}_1' = (\mathbf{Y}_1\mathbf{S}^e\mathbf{Z}_1)^e$ и $\mathbf{R}_2' = (\mathbf{Y}_2\mathbf{S}^e\mathbf{Z}_2)^e$.

2. Вычислить значение хэш-функции e' от документа, к которому присоединены векторы $\mathbf{R}_1'$ и $\mathbf{R}_2'$: $e' = f_h(M, \mathbf{R}_1', \mathbf{R}_2')$.

3. Если выполняется равенство $e' = e$, то ЭЦП признается подлинной, если нет — ложной.

Доказательство корректности описанной схемы ЭЦП (показываем, что правильно вычисленная подпись проходит проверочную процедуру как подлинная ЭЦП) выполняется следующим образом:

$$\mathbf{R}_1' = \left(\mathbf{Y}_1\mathbf{S}^e\mathbf{Z}_1\right)^e =$$

$$= \left[\mathbf{A}\mathbf{G}^x\mathbf{B}^{-1}\left(\mathbf{B}\mathbf{G}^s\mathbf{Q}^d\mathbf{B}^{-1}\right)^e\mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{A}^{-1}\right]^e =$$

$$= \left(\mathbf{A}\mathbf{G}^x\mathbf{G}^s\mathbf{Q}^d\mathbf{G}\mathbf{Q}\mathbf{A}^{-1}\right)^e = \left(\mathbf{A}\mathbf{G}^{es+x+1}\mathbf{Q}^{ed+1}\mathbf{A}^{-1}\right)^e =$$

$$= \mathbf{A}\mathbf{G}^{e^2s+ex+e}\mathbf{Q}^{e^2d+e}\mathbf{A}^{-1} = \mathbf{A}\mathbf{G}^k\mathbf{Q}^t\mathbf{A}^{-1} = \mathbf{R}_1;$$

$$\mathbf{R}_2' = \left(\mathbf{Y}_2\mathbf{S}^e\mathbf{Z}_2\right)^e =$$

$$= \left[\mathbf{D}\mathbf{G}^x\mathbf{B}^{-1}\left(\mathbf{B}\mathbf{G}^s\mathbf{Q}^d\mathbf{B}^{-1}\right)^e\mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{D}^{-1}\right]^e =$$

$$= \left(\mathbf{D}\mathbf{G}^x\mathbf{G}^s\mathbf{Q}^d\mathbf{G}\mathbf{Q}\mathbf{D}^{-1}\right)^e = \left(\mathbf{D}\mathbf{G}^{es+x+1}\mathbf{Q}^{ed+1}\mathbf{D}^{-1}\right)^e =$$

$$= \mathbf{D}\mathbf{G}^{e^2s+ex+e}\mathbf{Q}^{e^2d+e}\mathbf{D}^{-1} = \mathbf{D}\mathbf{G}^k\mathbf{Q}^t\mathbf{D}^{-1} = \mathbf{R}_2;$$

$$\left\{\mathbf{R}_1' = \mathbf{R}_1;\ \mathbf{R}_2' = \mathbf{R}_2\right\} \Rightarrow e' = e.$$

Рассмотрим попытку подделки подписи, т. е. вычисления подписи к документу M без использования секретных значений. Возьмем произвольное число e' и произвольный вектор $\mathbf{S}'$ и вычислим для них значения $\mathbf{R}_1 = (\mathbf{Y}_1\mathbf{S}'^{e'}\mathbf{Z}_1)^{e'}$ и $\mathbf{R}_2 = (\mathbf{Y}_2\mathbf{S}'^{e'}\mathbf{Z}_2)^{e'}$. Затем вычислим хэш-значение $e = f_h(M, \mathbf{R}_1, \mathbf{R}_2)$. После этого попытаемся вычислить вектор **S**, такой, что пара (e, **S**) будет удовлетворять равенству $\mathbf{R}_1 = (\mathbf{Y}_1\mathbf{S}^e\mathbf{Z}_1)^e$. Для этого следует решить уравнение $(\mathbf{Y}_1\mathbf{S}^e\mathbf{Z}_1)^e = (\mathbf{Y}_1\mathbf{S}'^{e'}\mathbf{Z}_1)^{e'}$ относительно неизвестного **S**. Имеем

$$\mathbf{S} = \left[\mathbf{Y}_1^{-1}\left(\mathbf{Y}_1\mathbf{S}'^{e'}\mathbf{Z}_1\right)^{e'e^{-1}}\mathbf{Z}_1^{-1}\right]^{e^{-1}} =$$

$$= \left[\mathbf{B}\mathbf{G}^{-x}\mathbf{A}^{-1}\left(\mathbf{A}\mathbf{G}^x\mathbf{B}^{-1}\mathbf{S}'^{e'}\mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{A}^{-1}\right)^{ee^{-1}}\mathbf{A}\mathbf{Q}^{-1}\mathbf{G}^{-1}\mathbf{B}^{-1}\right]^e =$$

$$= \left[\mathbf{B}\mathbf{G}^{-x}\mathbf{A}^{-1}\mathbf{A}\left(\mathbf{G}^x\mathbf{B}^{-1}\mathbf{S}'^{e'}\mathbf{B}\mathbf{G}\mathbf{Q}\right)^{ee^{-1}}\mathbf{A}^{-1}\mathbf{A}\mathbf{Q}^{-1}\mathbf{G}^{-1}\mathbf{B}^{-1}\right]^e =$$

$$= \left[\mathbf{B}\mathbf{G}^{-x}\left(\mathbf{G}^x\mathbf{B}^{-1}\mathbf{S}'^{e'}\mathbf{B}\mathbf{G}\mathbf{Q}\right)^{ee^{-1}}\mathbf{Q}^{-1}\mathbf{G}^{-1}\mathbf{B}^{-1}\right]^e.$$

Поскольку вычисленное значение **S** не зависит

от значения **A**, пара (*e*, **S**) удовлетворяет также и уравнению $(\mathbf{Y}_2\mathbf{S}^e\mathbf{Z}_2)^e = (\mathbf{Y}_2\mathbf{S}'^{e'}\mathbf{Z}_2)^{e'}$. Поэтому она пройдет процедуру проверки ЭЦП как подлинная подпись. Таким образом, значение **S** может быть использовано как подгоночный элемент для успешной подделки подписи в схеме ЭЦП с открытым ключом, вычисляемым по формулам (1) и (2).

Описанная схема подделки ЭЦП показывает, что удваиваемое проверочное уравнение должно быть таким, чтобы формула, выражающая **S** через **S**′, включала секретные элементы, которые используются для вычисления только одной из пар ($\mathbf{Y}_1$, $\mathbf{Z}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$) элементов открытого ключа, а именно той, по отношению к которой вычисляется подгоночное значение **S**. При реализации этого положения подделка подписи будет вычислительно невыполнимой. Это демонстрирует следующая схема ЭЦП с удвоенным проверочным соотношением.

Схема ЭЦП с трехэлементной подписью

Пусть даны два случайных вектора, **Q** и **G**, порядка *q*, принадлежащие одной коммутативной группе с двухмерной цикличностью. Вычисление открытого ключа зададим в виде двух троек векторов, ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{T}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{T}_2$), вычисляемых по формулам

$$\mathbf{Y}_1 = \mathbf{A}\mathbf{G}^x\mathbf{A}^{-1};\ \mathbf{Z}_1 = \mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{B}^{-1};\ \mathbf{T}_1 = \mathbf{A}\mathbf{B}^{-1}; \quad (3)$$

$$\mathbf{Y}_2 = \mathbf{D}\mathbf{G}^{ux}\mathbf{D}^{-1};\ \mathbf{Z}_2 = \mathbf{B}\mathbf{G}^u\mathbf{Q}\mathbf{B}^{-1};\ \mathbf{T}_1 = \mathbf{D}\mathbf{B}^{-1}, \quad (4)$$

где $x < q$ и $u < q$ — случайно выбранные натуральные числа;

A, **B** и **D** — случайные векторы, которые вместе с числами *x* и *u* образуют личный секретный ключ владельца открытого ключа.

Процедуру формирования цифровой подписи к некоторому документу *M* зададим в виде следующего алгоритма.

1. Сгенерировать случайные натуральные числа $k < q$ и $t < q$ и случайный обратимый вектор **K**. Затем вычислить векторы $\mathbf{R}_1 = \mathbf{A}\mathbf{G}^k\mathbf{Q}^t\mathbf{K}$ и $\mathbf{R}_2 = \mathbf{D}\mathbf{G}^{uk}\mathbf{Q}^t\mathbf{K}$.

2. Вычислить значение хэш-функции $f_h(\ldots)$ от документа с присоединенными к нему векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $e = f_h(M, \mathbf{R}_1, \mathbf{R}_2)$.

3. Вычислить значение $s = k - ex \bmod q$.

4. Вычислить значение $d = t - s \bmod q$.

5. Вычислить вектор $\mathbf{S} = \mathbf{B}\mathbf{Q}^d\mathbf{K}$.

Подписью является тройка значений (*e*, *s*, **S**).

Процедура проверки подлинности ЭЦП к документу *M* включает следующие шаги.

1. Вычислить векторы $\mathbf{R}_1' = \mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}$ и $\mathbf{R}_2' = \mathbf{Y}_2^e\mathbf{T}_2\mathbf{Z}_2^s\mathbf{S}$.

2. Вычислить значение хэш-функции e' от документа, к которому присоединены векторы $\mathbf{R}_1'$ и $\mathbf{R}_2'$: $e' = f_h(M, \mathbf{R}_1', \mathbf{R}_2')$.

3. Если выполняется равенство $e' = e$, то ЭЦП признается подлинной, если нет — ложной.

Доказательство корректности описанной схемы подписи:

$$\begin{aligned}
\mathbf{R}_1' &= \mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S} = \\
&= \left(\mathbf{A}\mathbf{G}^x\mathbf{A}^{-1}\right)^e\mathbf{T}_1\left(\mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{B}^{-1}\right)^s\mathbf{B}\mathbf{Q}^d\mathbf{K} = \\
&= \mathbf{A}\mathbf{G}^{xe}\mathbf{A}^{-1}\mathbf{A}\mathbf{B}^{-1}\mathbf{B}\mathbf{G}^s\mathbf{Q}^s\mathbf{B}^{-1}\mathbf{B}\mathbf{Q}^d\mathbf{K} = \\
&= \mathbf{A}\mathbf{G}^{ex+k-ex}\mathbf{Q}^s\mathbf{Q}^{t-s}\mathbf{K} = \mathbf{A}\mathbf{G}^k\mathbf{Q}^t\mathbf{K} = \mathbf{R}_1; \\
\mathbf{R}_2' &= \mathbf{Y}_2^e\mathbf{T}_2\mathbf{Z}_2^s\mathbf{S} = \\
&= \left(\mathbf{D}\mathbf{G}^{ux}\mathbf{D}^{-1}\right)^e\mathbf{T}_2\left(\mathbf{B}\mathbf{G}^u\mathbf{Q}\mathbf{B}^{-1}\right)^s\mathbf{B}\mathbf{Q}^d\mathbf{K} = \\
&= \mathbf{D}\mathbf{G}^{uxe}\mathbf{D}^{-1}\mathbf{D}\mathbf{B}^{-1}\mathbf{B}\mathbf{G}^{us}\mathbf{Q}^s\mathbf{B}^{-1}\mathbf{B}\mathbf{Q}^d\mathbf{K} = \\
&= \mathbf{D}\mathbf{G}^{eux+uk-eux}\mathbf{Q}^s\mathbf{Q}^{t-s}\mathbf{K} = \mathbf{D}\mathbf{G}^k\mathbf{Q}^t\mathbf{K} = \mathbf{R}_2; \\
&\left\{\mathbf{R}_1' = \mathbf{R}_1;\ \mathbf{R}_2' = \mathbf{R}_2\right\} \Rightarrow e' = e.
\end{aligned}$$

Рассмотрим попытку подделки подписи. Возьмем произвольные числа $e' < q$, $s < q$ и произвольный вектор **S**′ и вычислим для них значения $\mathbf{R}_1 = \mathbf{Y}_1^{e'}\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}'$ и $\mathbf{R}_2 = \mathbf{Y}_2^{e'}\mathbf{T}_1\mathbf{Z}_2^s\mathbf{S}'$. Затем вычислим хэш-значение $e = f_h(M, \mathbf{R}_1, \mathbf{R}_2)$. После этого попытаемся вычислить вектор **S**, такой, что тройка (*e*, *s*, **S**) будет удовлетворять равенству $\mathbf{R}_1 = \mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}$. Для этого следует решить уравнение $\mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S} = \mathbf{Y}_1^{e'}\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}'$ относительно неизвестного **S**. Таким образом, для выполнения первого проверочного уравнения получаем следующее значение **S**:

$$\begin{aligned}
\mathbf{S} &= \mathbf{Z}_1^{-s}\mathbf{T}_1^{-1}\mathbf{Y}_1^{e'-e}\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}' = \\
&= \mathbf{B}\mathbf{Q}^{-s}\mathbf{G}^{-s}\mathbf{B}^{-1}\mathbf{B}\mathbf{A}^{-1}\mathbf{Y}_1^{e'-e}\mathbf{A}\mathbf{B}^{-1}\mathbf{B}\mathbf{G}^s\mathbf{Q}^s\mathbf{B}^{-1}\mathbf{S}' = \\
&= \mathbf{B}\mathbf{Q}^{-s}\mathbf{G}^{-s}\mathbf{A}^{-1}\mathbf{Y}_1^{e'-e}\mathbf{A}\mathbf{G}^s\mathbf{Q}^s\mathbf{B}^{-1}\mathbf{S}' = \\
&= \mathbf{B}\mathbf{Q}^{-s}\mathbf{G}^{-s}\mathbf{A}^{-1}\mathbf{A}\mathbf{G}^{x(e'-e)}\mathbf{A}^{-1}\mathbf{A}\mathbf{G}^s\mathbf{Q}^s\mathbf{B}^{-1}\mathbf{S}' = \\
&= \mathbf{B}\mathbf{G}^{x(e'-e)}\mathbf{B}^{-1}\mathbf{S}'.
\end{aligned}$$

Аналогичным путем легко установить, что для выполнения второго проверочного уравнения требуется задать следующее значение **S**:

$$\mathbf{S} = \mathbf{Z}_2^{-s}\mathbf{T}_2^{-1}\mathbf{Y}_2^{e'-e}\mathbf{T}_2\mathbf{Z}_2^s\mathbf{S}' = \mathbf{B}\mathbf{G}^{ux(e'-e)}\mathbf{B}^{-1}\mathbf{S}'.$$

Поскольку для выполнения первого и второго проверочных уравнений требуются различные значения вектора **S**, подделка подписи является вычислительно невыполнимой.

Альтернативная схема с трехэлементной подписью

Рассмотрим альтернативный вариант построения схемы ЭЦП с открытым ключом, представляющим две тройки векторов, ($\mathbf{Y}_1$, $\mathbf{Z}_1$, $\mathbf{T}_1$) и ($\mathbf{Y}_2$, $\mathbf{Z}_2$, $\mathbf{T}_2$), вычисляемых по формулам, аналогичным (3) и (4):

$$\mathbf{Y}_1 = \mathbf{A}\mathbf{G}^x\mathbf{A}^{-1};\ \mathbf{Z}_1 = \mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{B}^{-1};\ \mathbf{T}_1 = \mathbf{A}\mathbf{B}^{-1}; \quad (5)$$

$$\mathbf{Y}_2 = \mathbf{D}\mathbf{G}^{ux}\mathbf{D}^{-1};\ \mathbf{Z}_2 = \mathbf{H}\mathbf{G}^u\mathbf{Q}\mathbf{H}^{-1};\ \mathbf{T}_1 = \mathbf{D}\mathbf{H}^{-1}, \quad (6)$$

где $x < q$ и $u < q$ — случайно выбранные натуральные числа;

A, **B**, **D** и **H** — случайные векторы, которые вместе с числами x и u образуют личный секретный ключ владельца открытого ключа.

Процедуру формирования цифровой подписи к некоторому документу M зададим в виде следующего алгоритма.

1. Сгенерировать случайные натуральные числа $k < q$ и $t < q$ и вычислить векторы $\mathbf{R}_1 = \mathbf{A}\mathbf{G}^k\mathbf{Q}^t\mathbf{D}^{-1}$ и $\mathbf{R}_2 = \mathbf{B}\mathbf{Q}^t\mathbf{G}^{uk}\mathbf{H}^{-1}$.

2. Вычислить значение хэш-функции $f_h(\ldots)$ от документа с присоединенными к нему векторами $\mathbf{R}_1$ и $\mathbf{R}_2$: $e = f_h(M, \mathbf{R}_1, \mathbf{R}_2)$.

3. Вычислить значение $s = k - ex \bmod q$.

4. Вычислить значение $d = t - s \bmod q$.

5. Вычислить вектор $\mathbf{S} = \mathbf{B}\mathbf{Q}^d\mathbf{D}^{-1}$.

Подписью является тройка значений (e, s, **S**).

Процедура проверки подлинности ЭЦП к документу M включает следующие шаги.

1. Вычислить векторы $\mathbf{R}_1' = \mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}$ и $\mathbf{R}_2' = \mathbf{S}\mathbf{Y}_2^e\mathbf{T}_1\mathbf{Z}_2^s$.

2. Вычислить значение хэш-функции e' от документа, к которому присоединены векторы $\mathbf{R}_1'$ и $\mathbf{R}_2'$: $e' = f_h(M, \mathbf{R}_1', \mathbf{R}_2')$.

3. Если выполняется равенство $e' = e$, то ЭЦП признается подлинной, если нет — ложной.

Доказательство корректности описанной схемы ЭЦП:

$$\begin{aligned}
\mathbf{R}_1' &= \mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S} = \\
&= \left(\mathbf{A}\mathbf{G}^x\mathbf{A}^{-1}\right)^e\mathbf{T}_1\left(\mathbf{B}\mathbf{G}\mathbf{Q}\mathbf{B}^{-1}\right)^s\mathbf{B}\mathbf{Q}^d\mathbf{D}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{xe}\mathbf{A}^{-1}\mathbf{A}\mathbf{B}^{-1}\mathbf{B}\mathbf{G}^s\mathbf{Q}^s\mathbf{B}^{-1}\mathbf{B}\mathbf{Q}^d\mathbf{D}^{-1} = \\
&= \mathbf{A}\mathbf{G}^{ex+k-ex}\mathbf{Q}^s\mathbf{Q}^{t-s}\mathbf{D}^{-1} = \mathbf{A}\mathbf{G}^k\mathbf{Q}^t\mathbf{D}^{-1} = \mathbf{R}_1;
\end{aligned}$$

$$\begin{aligned}
\mathbf{R}_2' &= \mathbf{S}\mathbf{Y}_2^e\mathbf{T}_2\mathbf{Z}_2^s = \\
&= \mathbf{B}\mathbf{Q}^d\mathbf{D}^{-1}\left(\mathbf{D}\mathbf{G}^{ux}\mathbf{D}^{-1}\right)^e\mathbf{T}_2\left(\mathbf{H}\mathbf{G}^u\mathbf{Q}\mathbf{H}^{-1}\right)^s = \\
&= \mathbf{B}\mathbf{Q}^d\mathbf{D}^{-1}\mathbf{D}\mathbf{G}^{uxe}\mathbf{D}^{-1}\mathbf{D}\mathbf{H}^{-1}\mathbf{H}\mathbf{G}^{us}\mathbf{Q}^s\mathbf{H}^{-1} = \\
&= \mathbf{B}\mathbf{Q}^{t-s}\mathbf{G}^{eux+u(k-ex)}\mathbf{Q}^s\mathbf{H}^{-1} = \mathbf{D}\mathbf{G}^k\mathbf{Q}^t\mathbf{H}^{-1} = \mathbf{R}_2;
\end{aligned}$$

$$\left\{\mathbf{R}_1' = \mathbf{R}_1;\ \mathbf{R}_2' = \mathbf{R}_2\right\} \Rightarrow e' = e.$$

Рассмотрим попытку подделки подписи. Возьмем произвольные числа $e' < q$, $s < q$ и произвольный вектор $\mathbf{S}'$ и вычислим для них значения $\mathbf{R}_1 = \mathbf{Y}_1^{e'}\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}'$ и $\mathbf{R}_2 = \mathbf{S}'\mathbf{Y}_2^{e'}\mathbf{T}_2\mathbf{Z}_2^s$. Затем вычислим хэш-значение $e = f_h(M, \mathbf{R}_1, \mathbf{R}_2)$. После этого попытаемся вычислить вектор **S**, такой, что тройка (e, s, **S**) будет удовлетворять равенству $\mathbf{R}_1 = \mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}$. Для этого следует решить уравнение $\mathbf{Y}_1^e\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S} = \mathbf{Y}_1^{e'}\mathbf{T}_1\mathbf{Z}_1^s\mathbf{S}'$ относительно неизвестного **S**, что дает $\mathbf{S} = \mathbf{B}\mathbf{G}^{x(e'-e)}\mathbf{B}^{-1}\mathbf{S}'$.

Теперь вычислим значение вектора **S**, при котором будет выполняться равенство $\mathbf{S}\mathbf{Y}_2^e\mathbf{T}_2\mathbf{Z}_2^s = \mathbf{S}'\mathbf{Y}_2^{e'}\mathbf{T}_2\mathbf{Z}_2^s$:

$$\begin{aligned}
\mathbf{S} &= \mathbf{S}'\mathbf{Y}_2^{e'}\mathbf{T}_2\mathbf{Z}_2^s\mathbf{Z}_2^{-s}\mathbf{T}_2^{-1}\mathbf{Y}_2^{-e} = \\
&= \mathbf{S}'\mathbf{Y}_2^{e'-e} = \mathbf{S}'\mathbf{D}\mathbf{G}^{ux(e'-e)}\mathbf{D}^{-1} \neq \\
&\neq \mathbf{B}\mathbf{G}^{x(e'-e)}\mathbf{B}^{-1}\mathbf{S}'.
\end{aligned}$$

Таким образом, при подделке подписи с использованием вектора **S** в качестве подгоночного параметра в альтернативной схеме ЭЦП с открытым ключом, вычисляемым по формулам (5) и (6), первое и второе проверочные уравнения также требуют различного модифицирования подгоночного параметра, что делает подделку подписи вычислительно невыполнимой задачей. При этом имеет место различие не только по значению степени вектора **G**, но также и по параметрам **D** и **B** и по положению множителя $\mathbf{S}'$ (что в случае некоммутативной алгебры имеет весьма существенное значение).

Обсуждение

Способ построения схем ЭЦП, включающий прием удвоения открытого ключа и проверочного уравнения, представляется весьма перспективным для построения практичных постквантовых алгоритмов цифровой подписи, основанных на вычислительной трудности СЗДЛ. Однако следует учитывать, что упомянутый прием сам по себе не решает автоматически задачу предотвращения возможности подделки подписи, как это демонстрируется описанной схемой ЭЦП с двухэле-

ментной подписью. Для предотвращения возможности использования элемента подписи **S** в качестве подгоночного параметра в процессе потенциальной подделки подписи следует соответствующим образом составить проверочные уравнения, используемые в процедуре проверки ЭЦП, и задать согласованные с последними формулы для вычисления удвоенного открытого ключа. При этом следует рассмотреть саму процедуру подделки подписи и убедиться, что используемые проверочные уравнения требуют различных модифицированных значений подгоночного параметра **S**.

При соблюдении этих положений разработанная схема ЭЦП будет представлять интерес как кандидат на практичную постквантовую схему ЭЦП, удовлетворяющую общему критерию постквантовой стойкости. Примерами являются две предложенные схемы ЭЦП с трехэлементной подписью вида (*e, s,* **S**), размер которой равен 288 байт, и открытым ключом, имеющим длину 1152, при ожидаемой 128-битной стойкости (2^{128} операций умножения в КНАА, используемой в качестве алгебраического носителя).

При этом указанные две схемы ЭЦП являются достаточно производительными. Вычислительная сложность процедуры генерации (проверки подлинности) подписи составляет примерно 23040 (18430) операций умножения по модулю 385-битного простого числа p. В схеме подписи RSA с 2048-битным модулем (обеспечивает 109-битную стойкость) и 256-битной экспонентой открытого ключа вычислительная сложность указанных процедур примерно равна 85800 (10750) умножений по 385-битному модулю. Таким образом, разработанные постквантовые схемы подписи обладают сопоставимой производительностью с алгоритмом RSA-2048, сохраняя возможность ее увеличения путем выбора 385-битного простого числа p вида $p = 2^{385} + b$, где b — небольшое нечетное натуральное число (модульное умножение может быть осуществлено без выполнения арифметического деления). Например, генерация нужного простого числа может быть выполнена по формуле $p = 2(2^{384} + b') + 1 = 2^{385} + 2b' + 1$, где b' — подбираемое нечетное 16-битное значение, при котором числа $q = 2^{384} + b'$ и $p = 2^{385} + 2b' + 1$ одновременно являются простыми.

Всемирный конкурс НИСТ по разработке постквантовых двухключевых криптосхем [10] перешел в завершающую стадию [11]. Финалистами конкурса по номинации кандидатов на постквантовый стандарт цифровой подписи стали следующие схемы ЭЦП: Falcon [12], Crystals-Dilithium [13] и Rainbow [14]. Представляет интерес сравнение характеристик перечисленных финалистов с предложенными в данной работе постквантовыми схемами ЭЦП, которое представлено в табл. 2.

Примечательно, что две предложенные постквантовые схемы ЭЦП обладают производительностью, сопоставимой с производительностью схем-финалистов конкурса НИСТ, но существенно меньшими размерами подписи и открытого ключа, что делает их более удобными для практического применения. Отдельно выделяется алгоритм Rainbow, который обладает наименьшим размером подписи. Однако размер открытого ключа в нем чрезвычайно велик (150000 байт).

Несмотря на то что оценка стойкости предложенных постквантовых схем подписи требует дальнейшего самостоятельного и более объемного исследования, естественно предположить, что итоговый результат конкурса НИСТ может оказаться несколько неудачным в плане удобства практического применения из-за возможного появления более конкурентноспособных разработок постквантовых схем ЭЦП. В качестве последних представляют значительный интерес схемы подписи с удвоенным проверочным уравнением, основанные на вычислительной трудности СЗДЛ.

Таблица 2

Сравнение некоторых характеристик двух предложенных схем ЭЦП с характеристиками схем-финалистов конкурса НИСТ и RSA-2048

Схема подписи	Размер подписи, байт	Размер открытого ключа, байт	Скорость генерации подписи, отн. ед.	Скорость верификации подписи, отн. ед.
Falcon	1280	1793	50	25
Crystals-Dilithium	2701	1472	15	2
Rainbow	64	150000	—	—
RSA-2048	256	288	10	80
Предложенные	288	1152	35	30

Заключение

Прием удвоения проверочного уравнения представляет интерес для реализации постквантовых схем ЭЦП, основанных на СЗДЛ и удовлетворяющих общему критерию постквантовой стойкости. Отдельный интерес представляет рассмотрение алгебраических носителей других типов для реализации таких схем ЭЦП, в том числе четырехмерных и шестимерных КНАА, заданных над конечными расширениями двоичного поля $GF(2)$, и конечных алгебр матриц размерностей 2×2 и 3×3.

Существенным моментом дальнейшего обоснования алгоритмов ЭЦП предложенного типа как кандидатов на постквантовые криптосхемы является проведение детальных исследований по обоснованию их стойкости, в том числе выполненных независимыми специалистами.

Работа выполнена при частичной финансовой поддержке бюджетной темы № 0060-2019-0010.

Литература

1. *Kuzmin A. S., Markov V. T., Mikhalev A. A., Mikhalev A. V., Nechaev A. A.* Cryptographic Algorithms on Groups and Algebras // J. Mathematical Sciences. 2017. V. 223. № 5. P. 629—641.

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

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

4. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer // SIAM J. Computing. 1997. V. 26. P. 1484—1509.

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

6. *Jozsa R.* Quantum algorithms and the Fourier transform // Proc. Roy. Soc. London Ser A. 1998. V. 454. P. 323—337.

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

9. *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

10. 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: 22.04.2021).

11. 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: 22.04.2021).

12. Fast-Fourier lattice-based compact signatures over NTRU [Электронный ресурс]. Режим доступа: https://falcon-sign.info/ (дата обращения: 22.04.2021).

13. *Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D.* CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme [Электронный ресурс]. Режим доступа: https://eprint.iacr.org/2017/633.pdf https://pq-crystals.org/dilithium/index.shtml (дата обращения: 22.04.2021).

14. *Ding J., Schmidt D.* Rainbow, a New Multivariable Polynomial Signature Scheme: Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science. — Berlin, Heidelberg: Springer. 2005. V. 3531. P. 164—175.

Digital signature schemes with doubled verification equation

A. A. Moldovyan, N. A. Moldovyan, D. N. Moldovyan, R. Sh. Fakhrutdinov
St. Petersburg Federal Research Center of the RAS, St. Petersburg, Russia

Doubling of the verification equation is used to design digital signature schemes based on computational difficulty of the hidden discrete logarithm problem. This design technique allows one to use one of the signature elements as a factor in the verification equation. Due to the latter a two-dimensional cyclicity group can be used as a hidden group and general criterion of post-quantum security is satisfied. Two new digital signature algorithms are introduced as candidates for practical post-quantum cryptoschemes.

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

Bibliography — 14 references. *Received April 23, 2021*

ОБЩИЕ ВОПРОСЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И ОБЪЕКТОВ

УДК 004.056
DOI: 10.52190/2073-2600_2021_2_37

Политика информационной безопасности — элемент защиты киберпространства

М. М. Тараскин, д-р техн. наук; *С. А. Матюнин*, канд. пед. наук; *Ю. И. Коваленко*
РТУ МИРЭА, Москва, Россия

Рассмотрены основные международные, межгосударственные и национальные нормативные акты, используемые при разработке одного из важнейших документов обладателя информации — Политики информационной безопасности организации.

Ключевые слова: защита информации, информационная безопасность, инцидент информационной безопасности, политика информационной безопасности, система менеджмента информационной безопасности.

Выступая на коллегии Федеральной службы безопасности Российской Федерации Владимир Владимирович Путин подчеркнул, что против нас ведётся целенаправленная информационная кампания с безапелляционными и бездоказательными обвинениями по целому ряду вопросов. В этих условиях важно повышать уровень защиты конфиденциальной информации, не допускать утечек закрытых сведений военного характера, совершенствовать пограничную инфраструктуру, реализовывать инновационные подходы по обеспечению кибербезопасности [1].

Цели и задачи в сфере информационной безопасности описываются в Политике информационной безопасности (ИБ), которая является концептуальным документом высокого уровня [2].

Нормативными документами Российской Федерации определено, что в общем случае "политика — общее намерение и направление, официально выраженное руководством" [3]. При этом целью политики ИБ является обеспечение управления и поддержки высшим руководством организации процессов обеспечения ИБ в соответствии с требованиями уставной деятельности организации (обладателя информации) и соответствующими законами и нормами.

Еще в 2008 г. в Российской Федерации было установлено, что политика информационной безопасности (организации) представляет собой формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области ИБ, которыми руководствуется организация в своей деятельности [4].

Политика, как документ, должна содержать:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;
- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

Целью информационной безопасности организации является заранее намеченный результат обеспечения ИБ организации в соответствии с установленными требованиями в политике ИБ организации.

Политика безопасности должна быть оформлена документально на нескольких уровнях управления. На уровне управляющего высшего звена руководства должны быть определены цели политики безопасности, структура и перечень решаемых задач и ответственные за реализацию политики.

Тараскин Михаил Михайлович, профессор.
E-mail: professor.59@mail.ru
Матюнин Сергей Александрович, преподаватель.
E-mail: pam-1986@yandex.ru
Коваленко Юрий Иванович, доцент.
E-mail: pam-1986@yandex.ru

Статья поступила в редакцию 12 апреля 2021 г.

Основной документ должен быть детализирован администраторами безопасности информационных систем (управляющими среднего звена) с учётом принципов деятельности организации, соотношения важности целей и наличия ресурсов. Детальные решения должны включать ясные определения методов защиты технических и информационных ресурсов, поведение сотрудников в конкретных ситуациях, а также инструкции, определяющие порядок работы с документами организации.

Актуальность подготовки специалистов в области обеспечения кибербезопасности и разработки ранжированных политик отражена в многочисленных источниках, в том числе в учебных пособиях [5].

Наиболее значимыми нормативными документами в области ИБ, определяющими критерии для оценки защищенности автоматизированных систем в глобальном цифровом пространстве, и требования, предъявляемые к механизмам защиты, являются:

- Общие критерии оценки безопасности ИТ (The Common Criteria for Information Technology Security Evaluation/ISO 15408), которые в Российской Федерации представлены семейством гармонизированных национальных стандартов ГОСТ Р ИСО/МЭК 15408. В данных стандартах наиболее полно изложены критерии для оценки механизмов безопасности программно-технического уровня [6—8].
- На основании опыта, накопленного в области управления информационной безопасностью, в Подкомитете SC 27 Совместного технического комитета ISO/IEC JTC 1 эксперты достигли согласия по созданию системы международных стандартов по ИБ, известной как семейство стандартов системы менеджмента информационной безопасности (СМИБ) [3, 9—11]. При использовании семейства стандартов СМИБ организации любой формы собственности, в том числе и органы безопасности, могут реализовывать и совершенствовать систему управления защитой информации и готовиться к независимой оценке их СМИБ, применяемой для защиты информации, такой, как оперативная или финансовая информация, интеллектуальная собственность, информация о персонале, а также информация, доверенная клиентами или третьей стороной. Семейство стандартов СМИБ предназначено для помощи организациям любой формы собственности и величины в реализации и функционировании СМИБ. Семейство стандартов СМИБ состоит из международных стандартов под общим названием Information Technology — Security Techniques (Информационные технологии. Методы и средства обеспечения безопасности).

Здесь и далее под термином "менеджмент информационной безопасности организации" будем понимать скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации [4].

ГОСТ Р ИСР/МЭК 15408-1-2012 содержит положения по следующим вопросам: контекст оценки, доработка требований безопасности для конкретного применения, профили защиты и пакеты, результаты оценки [6]. Стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, служащего в качестве основы при оценке характеристик безопасности продуктов ИТ. В стандарте представлен краткий обзор и дано описание всех частей ИСО/МЭК 15408, определены термины и сокращения, используемые во всех частях ИСО/МЭК 15408, установлено основное понятие объекта оценки, контекста оценки, описание целевой аудитории, которой адресованы критерии оценки. Представлены основные положения, необходимые для оценки продуктов ИТ. В стандарте определяются ключевые понятия профилей защиты, пакетов требований безопасности, рассматриваются вопросы, связанные с утверждениями о соответствии, описываются выводы и результаты оценки. Даны инструкции по спецификации заданий по безопасности и описание структуры компонентов в рамках всей модели. Также дана общая информация о методологии оценки.

ГОСТ Р ИСО/МЭК 15408-2-2013 содержит положения по следующим вопросам: парадигма функциональных требований; функциональные компоненты безопасности и их каталог; аудит безопасности и его анализ; криптографическая поддержка, включая генерацию, распределение, доступ и управление криптографическими ключами; управление доступом, основанное на атрибутах безопасности; аутентификация данных; политика управления информационными потоками; мониторинг целостности хранимых данных; защита конфиденциальности данных пользователя; базовая конфиденциальность обмена данными [7]. Стандарт устанавливает структуру и содержание компонентов функциональных требований безопасности для оценки безопасности. Он также содержит каталог функциональных компонентов, отвечающих общим требованиям к функциональным возможностям безопасности многих продуктов ИТ.

ГОСТ Р ИСО/МЭК 15408-3-2013 содержит положения по следующим вопросам: требования доверия к безопасности, краткий обзор оценочных уровней доверия, составные пакеты доверия, оценка профиля защиты, оценка задания по безопасности (определение проблемы безопасности, цели безопасности, требования безопасности), архитектура безопасности, оценка уязвимостей, анализ уязвимостей [8]. Стандарт определяет требования доверия на сформулированные на основе положений международного стандарта ИСО/МЭК 15408 и включает оценочные уровни доверия, задающие шкалу для измерения доверия через составные пакеты доверия, определяющие шкалу для измерения доверия для составных компонентов; отдельные компоненты доверия, из которых составлены уровни и пакеты доверия, а также критерии.

Третью часть стандарта 15408 целесообразно использовать совместно с первыми двумя его частями.

ГОСТ Р ИСО/МЭК 27001-2006 содержит положения по вопросам внедрения системы менеджмента информационной безопасности применительно ко всей деловой деятельности организации, разработке СМИБ и управлению этой системой с учетом характеристик деловой активности организации, ее размещения и активов, внедрению и функционированию СМИБ; проведению мониторинга и анализа этой системы, поддержке и улучшению СМИБ и ответственности руководства, внутреннему аудиту СМИБ и анализу этой системы менеджмента со стороны руководства, улучшению СМИБ и т. п. [9]. Стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими). Стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной СМИБ для минимизации деловых рисков организации. Кроме того, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности.

ГОСТ Р ИСО/МЭК 27002-2012 действует с 1 января 2014 г. содержит положения по вопросам информационной безопасности, включая цели ее создания, определение требований к информационной безопасности, оценку рисков, а также выбор мер и средств контроля и управления информационной безопасностью [9].

Стандарт состоит из 12 разделов, посвященных мерам и средствам контроля и управления безопасностью, которые все вместе содержат 39 основных категорий безопасности, и одного вводного раздела, знакомящего с оценкой и обработкой рисков.

В зависимости от обстоятельств каждый из разделов может быть важным. Следовательно, каждой организации, использующей стандарт, следует определить значимые разделы, их важность, а также их применимость для отдельных процессов бизнеса. Особое внимание в стандарте уделено организационным аспектам информационной безопасности. С точки зрения современных управленческих задач актуальны: задачи, решаемые внутри организации; вопросы взаимодействия со сторонними организациями; менеджмент активов и описание ответственности за активы; классификация информации; аспекты безопасности, связанные с персоналом (перед трудоустройством, в течение занятости, при прекращении или смене занятости). Также стандарт формирует описание и характеристику физической безопасности, включая вопросы защиты от воздействий окружающей среды, зон безопасности, безопасности оборудования, менеджмента коммуникаций и работ (эксплуатационные процедуры и обязанности, менеджмент оказания услуг третьей стороной, планирование и приемка систем, защита от вредоносной и мобильной программы, резервирование, менеджмент безопасности сети, обращение с носителями информации, обмен информацией, услуги электронной торговли, мониторинг безопасности); управления доступа (уставные требования по управлению доступом, менеджмент доступа пользователей, обязанности пользователя, управление доступом к сети, эксплуатируемой системе, к информации и прикладным программам, мобильная вычислительная техника и дистанционная работа); приобретения, разработки и эксплуатации информационных систем (требования безопасности информационных систем, корректная обработка в прикладных программах, применяемые криптографические меры и средства контроля и управления, безопасность системных файлов, безопасность в процессах разработки и поддержки, менеджмент технических уязвимостей). Серьезное внимание в стандарте уделено вопросам управления: менеджмент инцидентов информационной безопасности (оповещение о событиях и уязвимостях информационной безопасности, необходимое совершенствование по управлению инцидентами информационной безопасности, менеджмент не-

прерывности уставной деятельности и обеспечение при этом всех аспектов информационной безопасности); соответствие требованиям законодательства; соответствие политикам безопасности и стандартам, включая техническое соответствие; вопросы аудита информационных систем. Особый интерес представляют разделы 15.1.3 "Защита документов организации" и 15.1.4 "Защита данных и конфиденциальность персональных данных", содержащие рекомендации по реализации политики в отношении обеспечения защиты данных и персональных данных от потери, разрушения и фальсификации. Соблюдение указанной политики и всех применимых требований законодательных и нормативных актов по защите данных подразумевает наличие соответствующей структуры управления и контроля. Часто это лучше всего достигается путем назначения ответственного лица, например должностного лица, отвечающего за защиту данных. Ответственный должен предоставить инструкции руководителям среднего звена, пользователям и поставщикам услуг в отношении их персональной ответственности и специальных процедур, обязательных для выполнения. Стандарт имеет ключевое значение для специалистов в области защиты информации.

ГОСТ Р ИСО/МЭК 27003-2012 представляет дальнейшее развитие подходов по обеспечению ИБ и содержит положения по вопросам определения приоритетов организации для разработки СМИБ, включая разработку технического обоснования и плана проекта, определение области действия и границ политики СМИБ, разработку этой политики, проведение анализа требований к системе СМИБ и проведение оценки этой системы, правила разработки СМИБ организации и создание условий для обеспечения ее надежного функционирования [10]. В стандарте рассматриваются важнейшие аспекты, необходимые для успешной разработки и внедрения СМИБ в соответствии со стандартом ИСО/МЭК 27001-2006.

В нем описывается процесс определения и разработки СМИБ от "запуска" до составления планов внедрения. На практике лица, принимающие решения в организации, получившие высшее образование до 2012 г., в рамках образовательного процесса не могли слышать о существовании ГОСТ Р ИСО/МЭК 27002-2012 и ГОСТ Р ИСО/МЭК 27003-2012, в которых излагаются новые подходы к новым информационным технологиям в области безопасности.

В стандарте ГОСТ Р ИСО/МЭК 27003-2012 описывается процесс получения одобрения руководством организации первостепенных процедур для внедрения СМИБ, определяются требования к проекту внедрения такой системы и даются рекомендации по планированию проекта СМИБ, в результате которого формируется окончательный план внедрения этой системы в организации. Особого внимания заслуживают приложения к стандарту, включающие готовые решения по целям, принципам действия и методикам внедрения политики ИБ.

ГОСТ Р ИСО/МЭК 27005-2010 содержит положения по вопросам менеджмента рисков информационной безопасности, включая процессы и организационную структуру, оценку рисков и их предотвращение, мониторинг, анализ и переоценку риска информационной безопасности [11]. Стандарт представляет руководство по менеджменту рисков информационной безопасности и содержит положения по его совершенствованию. Стандарт поддерживает общие концепции, определенные в ИСО/МЭК 27001-2006, и предназначен для соответствующего обеспечения защиты информации на основе подхода, связанного с менеджментом риска. Стандарт применим для организаций всех типов (например, коммерческих предприятий, государственных учреждений, некоммерческих организаций), планирующих осуществлять менеджмент рисков, которые могут скомпрометировать информационную безопасность организации.

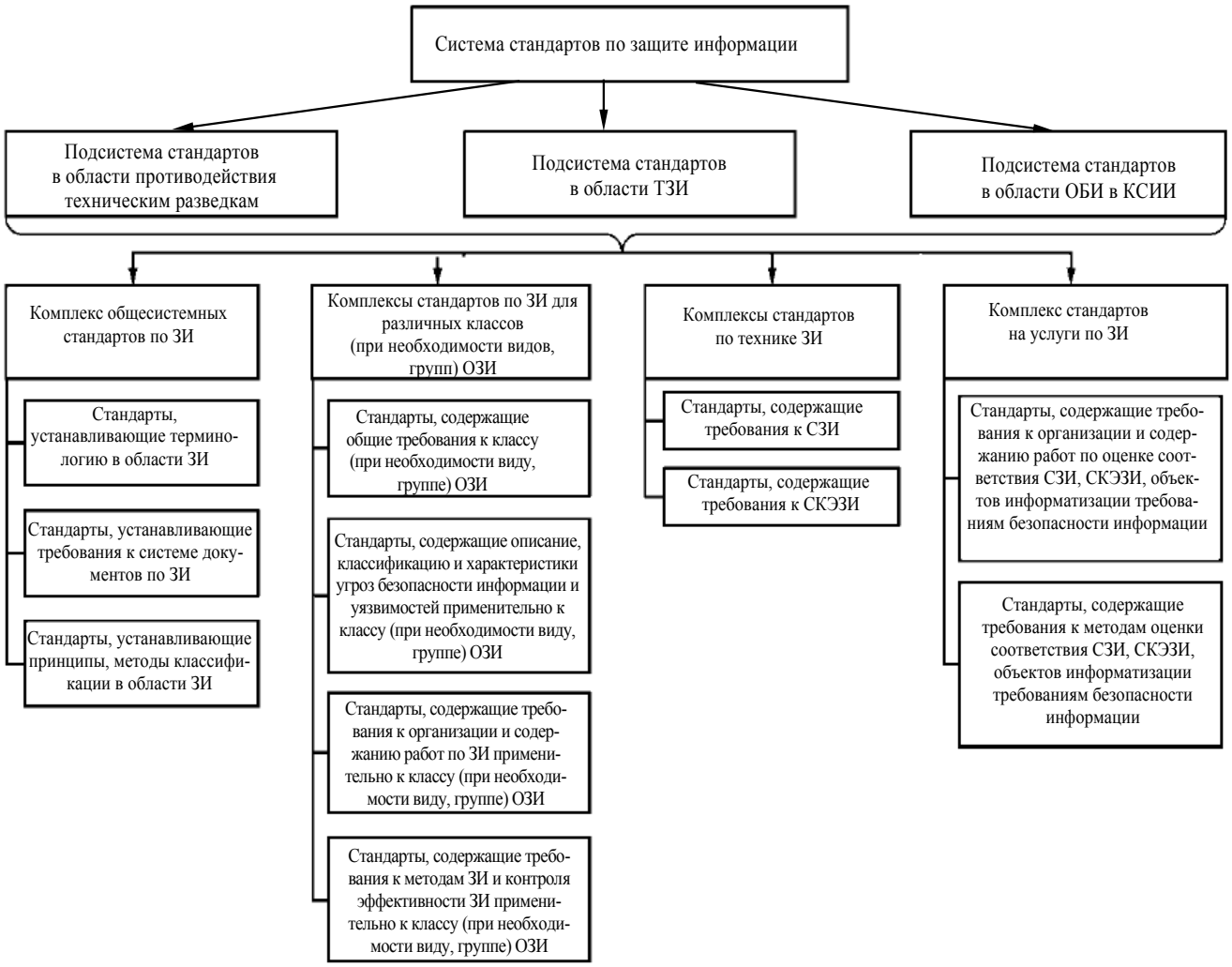
Регулирование межгосударственных отношений, направленных на противодействие угрозам информационной безопасности, в том числе разработке и применению систем информационного оружия, актам информационного терроризма и проявления случаев информационной преступности, т. е. факторам, создающим опасность для личности, общества, государства и их интересов в информационном пространстве СНГ, осуществляется на основании Соглашения о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности [11]. При этом в целях взаимоподдержки Стороны организуют взаимодействие и сотрудничество: в области сближения нормативных правовых актов и нормативно-методических документов государств-участников Соглашения, регламентирующих отношения в сфере обеспечения ИБ; разработке нормативных правовых актов для проведения совместных скоординированных мероприятий в информационном пространстве, направленных на обеспечение ИБ в государствах-участниках; разработке и доведении до пользователей нормативных документов, регулирующих вопросы обеспечения ИБ; реализации согласованных мero-

приятий, направленных на недопущение несанкционированного доступа к информации, размещенной в информационных системах, и ее утечки по техническим каналам; профессиональной переподготовке и повышении квалификации кадров в области обеспечения ИБ и т. п.

Наряду с международными и межгосударственными нормативными актами при разработке политики ИБ применяют также и национальные стандарты, основные из которых будут перечислены далее.

Говоря о национальных стандартах, содержащих методику защиты информации и используемых для обеспечения ИБ организации, следует отметить, что она не носит ярко выраженного характера и всегда привязана к направлениям деятельности организации, ее предназначению, масштабу и финансовым возможностям. Отсюда и многообразие национальных стандартов, используемых в этой сфере. Вместе с тем существует национальный стандарт, устанавливающий единые требования к самим национальным стандартам, разрабатываемым для сферы защиты информации и ИБ.

ГОСТ Р 52069.0-2013 определяет объекты стандартизации в данной сфере и аспекты этой деятельности [12]. Положения стандарта применяются при проведении работ по стандартизации в области противодействия техническим разведкам, технической защиты информации некриптографическими методами, обеспечения безопасности информации в ключевых системах информационной инфраструктуры. Стандарт является основополагающим национальным стандартом Российской Федерации в области защиты информации, осуществляемой некриптографическими методами. Структура системы стандартов по защите информации (ЗИ) показана на рисунке.



Структура системы стандартов по защите информации

ГОСТ Р 53114-2008 устанавливает основные термины, применяемые при проведении работ по стандартизации в области обеспечения ИБ в организации [4]. Термины, установленные данным стандартом, рекомендуется использовать в нормативных документах, правовой, технической и организационно-распорядительной документации, научной, учебной и справочной литературе. Приведенные определения можно при необходимости изменять, вводя в них производные признаки, раскрывая значения используемых в них терминов, указывая объекты, входящие в объем определяемого понятия. Такие изменения не должны нарушать объем и содержание понятий, определенных в настоящем стандарте.

Стандарт содержит и дает определения группам терминов, относящихся к:

- объекту защиты информации;
- угрозам безопасности информации;
- менеджменту ИБ организации;
- контролю и оценке ИБ организации;
- средствам обеспечения ИБ организации.

ГОСТ Р 51583-2014 содержит положения по вопросам содержания и порядка выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении, содержания и порядка выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении и т. п. [13]. Положения данного стандарта дополняют положения межгосударственного комплекса стандартов "Информационная технология. Комплекс стандартов на автоматизированные системы" в части порядка создания автоматизированных систем в защищенном исполнении.

Стандарт распространяется на создаваемые (модернизируемые) автоматизированные системы, в отношении которых законодательством или заказчиком установлены требования по их защите, и устанавливает содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищенном исполнении, содержание и порядок выполнения работ по защите информации о создаваемой (модернизируемой) автоматизированной системе в защищенном исполнении. В качестве основных видов автоматизированных систем рассматриваются автоматизированные рабочие места и информационные системы. Стандарт устанавливает, что автоматизированная система в защищенном исполнении должна соответствовать требованиям нормативных правовых актов, методических документов и национальных стандартов в области защиты информации. Стандарт может быть использован при создании автоматизированных систем в защищенном исполнении для органов безопасности.

ГОСТ Р 51275-2006 содержит положения по вопросам классификации факторов, воздействующих на безопасность защищаемой информации, которые он делит на объективные и субъективные [14]. Стандарт классифицирует факторы, воздействующие на безопасность защищаемой информации, и формирует их перечень в целях обоснования угроз безопасности информации и формулирования требований по защите информации "на объекте информатизации", в том числе в организации. Стандарт распространяется на объекты информатизации, создаваемые и эксплуатируемые в различных областях деятельности (оборона, безопасность, экономика, наука, управление и другие).

Общие выводы

Важнейшим условием реализации уставных целей организаций любой формы собственности является обеспечение необходимого и достаточного уровня ИБ юридических лиц, их активов (в том числе информационных), который во многом определяется уровнем ИБ исполняемых уставных технологических процессов (управленческих, производственных, информационных и т. д.), защитой автоматизированных систем, эксплуатирующийся организациями, в том числе в органах безопасности.

На основании действующих международных, межгосударственных и национальных стандартов разрабатывается важнейший документ обладателя информации — Политика информационной безопасности организации.

Решающее значение для успеха программы защиты информации, разработки Политики информационной безопасности и обеспечения ИБ имеет поддержка руководства организации (лиц, принимающих решения), а также персональная ответственность должностных лиц за состояние ИБ. Особое значение при этом имеет назначение специалистов, отвечающих за внедрение административных мер и правил безопасности. Каждый сотрудник организации должен хорошо знать правила безопасности, пройдя полный курс по программе изучения ИБ, сдать зачеты и получить документ, подтверждающий прохождение курса обучения.

Литература

1. http://www.kremlin.ru/events/president/news/65068
2. *Бармен С.* Разработка правил информационной безопасности / Пер. с англ. — М.: Изд. дом Вильяме, 2002. — 208 с.
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод

норм и правил менеджмента информационной безопасности. — М.: Стандартинформ, 2012.

4. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. — М.: Стандартинформ, 2008.

5. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель. — М.: Стандартинформ, 2012.

6. ГОСТ Р ИСО/МЭК 15408-2-2013 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2. Функциональные компоненты безопасности. — М.: Стандартинформ, 2013.

7. ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 3. Компоненты доверия к безопасности. — М.: Стандартинформ, 2013.

8. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — М.: Стандартинформ, 2006.

9. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности. — М.: Стандартинформ, 2012.

10. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. — М.: Стандартинформ, 2010.

11. Соглашение о сотрудничестве государств-участников Содружества независимых государств в области обеспечения информационной безопасности (Санкт-Петербург, 20 ноября 2013 г.). Текст Соглашения опубликован на официальном интернет-портале правовой информации (www.pravo.gov.ru) 4 июня 2015 г., в Бюллетене международных договоров, октябрь 2015 г., № 10.

12. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. — М.: Стандартинформ, 2013.

13. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. — М.: Стандартинформ, 2014.

14. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — М.: Стандартинформ, 2006.

Information security policy as an element of cyberspace protection

M. M. Taraskin, S. A. Matyunin, Yu. I. Kovalenko
RTU MIREA, Moscow, Russia

The article examines the main international, interstate and national regulations used in the development of one of the most important documents of the owner of the information — the Information Security Policy of the organization.

Keywords: information protection, information uecurity, information security incident, information security policy, information security management system.

Bibliography — 14 references. *Received April 12, 2021*

УДК 004.056
DOI: 10.52190/2073-2600_2021_2_44

Современные подходы к управлению состоянием информационной безопасности организации

Ю. И. Коваленко; П. А. Монахов
РТУ МИРЭА, Москва, Россия

Рассмотрены процедуры, необходимые для успешной разработки и внедрения системы управления информационной безопасностью (СУИБ) организации в соответствии с ГОСТ Р ИСО/МЭК 27001-2006. Описаны процесс получения одобрения руководством мер по внедрению СУИБ, процесс определения и разработки системы управления от запуска до составления планов внедрения, определен проект внедрения СУИБ на основании ГОСТ Р ИСО/МЭК 27003-2012, представлены рекомендации по планированию проекта такой системы, в результате которого получается окончательный план внедрения СУИБ.

Ключевые слова: защищенность информации, информационная безопасность, система менеджмента информационной безопасности, политика информационной безопасности.

Информация, которая хранится и обрабатывается в автоматизированной информационной системе организации, является объектом угроз компьютерных атак, сбоев в работе оборудования, ошибок персонала, деструктивного воздействия стихии (например, наводнения или пожара) или нарушителя.

Обеспечение защищенности информационной среды организации является комплексным системным процессом, затрагивающим все этапы жизненного цикла автоматизированной информационной системы, и представляет собой совокупность мер, которые характеризуются правовой, технической и организационной направленностью и которые нацелены на решение следующих задач [1]:

- реализация права на доступ к информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- обеспечение защиты информации, циркулирующей в автоматизированной информационной системе, от любых неправомерных действий в ее отношении на протяжении всего жизненного цикла.

Практика показывает, что с внедрением информационных технологий в управленческие процессы в целом проблемы защиты информации вышли за пределы компетенции только специалистов в области информационных технологий и распространились на специалистов всех направлений уставной деятельности организации.

Национальные стандарты, которые являются документами государственного уровня, рекомендуют начинать формирование правил управления информационной безопасностью (ИБ) с документа, в котором отражено общее намерение и направление, официально выраженное руководством в области защиты данных [2]. Это документ политического характера, который должен носить понятийный характер и быть доведен до всех сотрудников. Именно на него должны опираться все службы, участвующие в обеспечении информационной безопасности организации. Для обозначения документов, содержащих изложение общего подхода к безопасности в организации, и инструкций по использованию конкретных средств защиты информации, носящих преимущественно технический характер, широко используется термин "политика безопасности" [3].

В общем случае политика — это общее намерение и направление, официально выраженное руководством [3].

Анализ практического состояния вопроса в российской информационной сфере показывает, что подавляющее большинство руководителей (лиц, принимающих решение) получило высшее образование до 2005 г. При этом анализ ранее действовавших и ныне действующих федеральных образовательных стандартов высшего образования позволяет сделать вывод, что изучение вопросов анализа защищенности компьютерных систем, которые являются основой информационной среды любой организации, в том числе с использованием современных стандартов, осуществляется только по одной специализации основных профессиональных образовательных программ высшего об-

Коваленко Юрий Иванович, доцент.
E-mail: pam-1986@yandex.ru
Монахов Павел Алексеевич, сотрудник.
E-mail: pam-1986@yandex.ru

Статья поступила в редакцию 12 апреля 2021 г.

разования (программ специалитета) — по специальности 10.05.01 "Компьютерная безопасность" [4].

Такая ситуация обусловила ускорение процесса гармонизации национальных стандартов с международными документами в области создания систем управления информационной безопасностью.

Приказом Росстандарта от 27 декабря 2006 года № 375-ст "Об утверждении национального стандарта" утвержден национальный стандарт ГОСТ Р ИСО/МЭК 27001-2006 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования", который идентичен одноименному международному стандарту ИСО/МЭК 27001:2005 с датой введения в действие 1 февраля 2008 г. с правом досрочного применения. Таким образом, России понадобился только год для введения соответствующего гармонизированного нормативного документа [3]. Структура национального стандарта ГОСТ Р ИСО/МЭК 27001-2006 приведена на рис. 1.

Отметим, что термин "менеджмент" нормативно закреплен. Он означает скоординированные действия по руководству и управлению организацией и широко применяется для процессов описания защищенности в информационной сфере [2—5].

Как показывает анализ ГОСТ Р ИСО/МЭК 27001-2006 и других стандартов в этой области, внедрение информационных технологий в повседневную управленческую деятельность выдвигает специфические требования по обеспечению скоординированных действий к системе управления обеспечения ИБ организации. Таким образом, в данной области система менеджмента информационной безопасности (СМИБ) представляет собой СУИБ.

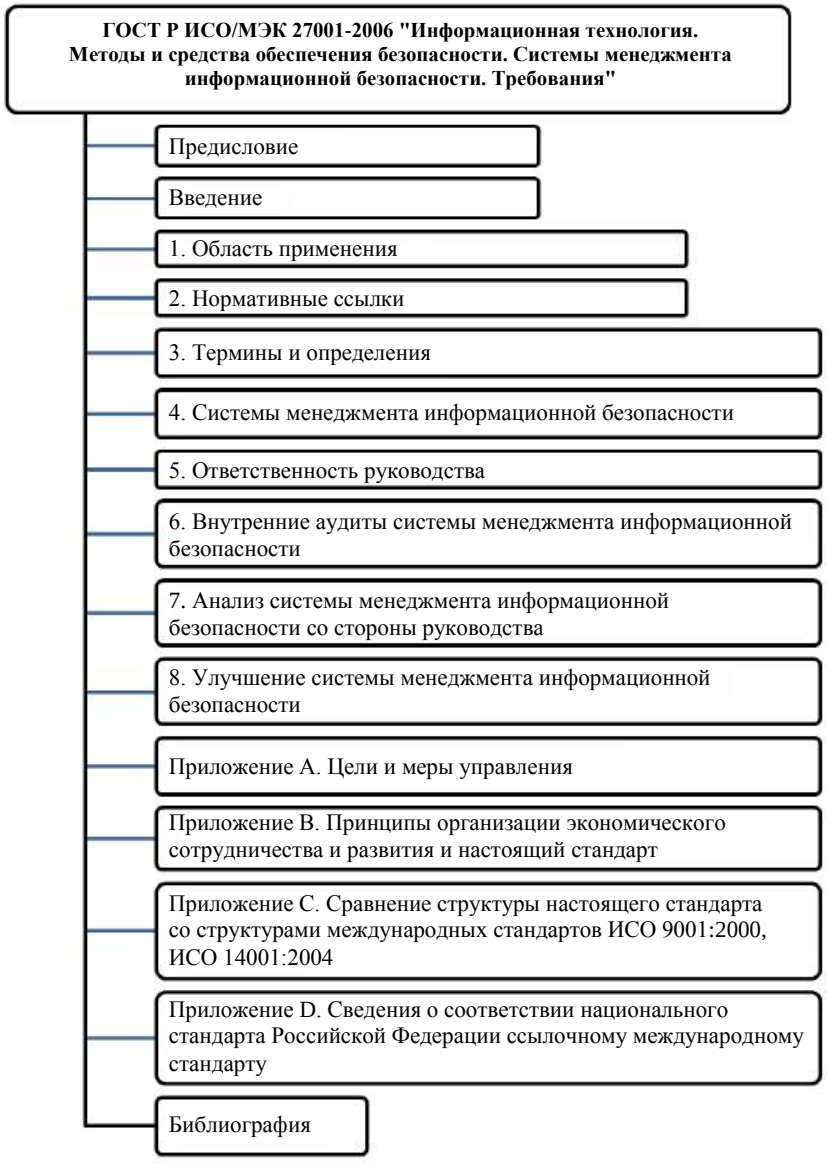


Рис. 1. Структура стандарта ГОСТ Р ИСО/МЭК 27001-2006

Как видно из структуры стандарта, обязательства лиц, принимающих управляющие решения в области обеспечения ИБ, изложены в 5-м разделе.

На основании данного нормативного документа руководство организации должно предоставлять доказательства выполнения своих обязательств в отношении разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ, т. е. СУИБ.

Функционирование такой системы реализуется путем следующих мер [2]:

a) разработки политики СМИБ;

b) обеспечения разработки целей и планов СМИБ;

c) определения функций и ответственности в области ИБ;

d) доведения до всех сотрудников организации информации о важности достижения целей ИБ и соответствия ее требованиям политики организации, об их ответственности перед законом, а также о необходимости непрерывного совершенствования в реализации мер ИБ;

e) выделения необходимых и достаточных ресурсов для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ;

f) установления критериев принятия рисков и уровней их приемлемости;

g) обеспечения проведения внутренних аудитов СМИБ;

h) проведения анализа СМИБ со стороны руководства.

Латинская нумерация в данном списке обусловлена необходимостью текстуальной привязки к основному нормативному документу [2].

По существу, данный раздел стандарта представляет собой практический план совершенствования ИБ организации. Конкретный план, естественно, потребует для реализации затрат ресурсов (интеллектуальных, временных, материальных) и учета уставных особенностей организации.

Бурное развитие информационных технологий выдвигает повышенные требования к скоординированной деятельности по руководству и управлению организацией применительно к обеспечению ИБ.

Практическая деятельность специалистов в информационной сфере привела к осознанию в мировом профессиональном сообществе того факта, что инерция мышления, просто человеческий консерватизм, недостаточная осведомленность лиц, принимающих решения, препятствуют внедрению современных требований по обеспечению ИБ. Это обстоятельство привело к разработке следующего международного стандарта — ИСО/МЭК 27003:2010 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности".

В России идентичный стандарт — ГОСТ Р ИСО/МЭК 27003-2012 — был введен в действие 1 декабря 2013 г. [6]. Структура национального стандарта ГОСТ Р ИСО/МЭК 27003-2012 приведена на рис. 2.

Таким образом, совершенствование процессов управления защищенностью информационной среды организации на основании современных стандартов в области менеджмента информационной безопасности начинается с процедур внедрения соответствующей системы управления.

Для успешной разработки и внедрения СМИБ необходимо получить разрешение руководства организации.

Подробное описание запуска, планирования и внедрения проекта СМИБ содержит национальный стандарт ГОСТ Р ИСО/МЭК 27003-2012. Процесс планирования конечного внедрения СМИБ включает пять фаз (рис. 3).

В стандарте каждая фаза представлена в отдельном пункте.

А. *Получение одобрения запуска проекта СМИБ руководством*. Существует несколько факторов, которые необходимо учитывать при принятии решения о внедрении СМИБ. Чтобы учесть эти факторы, высшее руководство организации должно рассмотреть деловые аргументы в пользу внедрения проекта СМИБ и утвердить его. Следовательно, цель этой фазы — получить одобрение руководства для запуска проекта СМИБ посредством определения случая применения СМИБ для данного предприятия и плана проекта.

Ожидаемым результатом этой фазы является предварительное разрешение руководства и принятие им обязательств по внедрению СМИБ и выполнению действий, описываемых в стандарте ГОСТ Р ИСО/МЭК 27003-2012.

Б. *Определение области действия и политики СМИБ*. Одобрение руководством внедрения СМИБ основывается на предварительном определении области действия СМИБ, случая применения СМИБ для данной организации и первоначальном плане проекта. Подробное определение области действия и границ СМИБ, определение политики СМИБ и ее принятие и поддержка руководством являются ключевыми первичными факторами для успешного внедрения СМИБ.

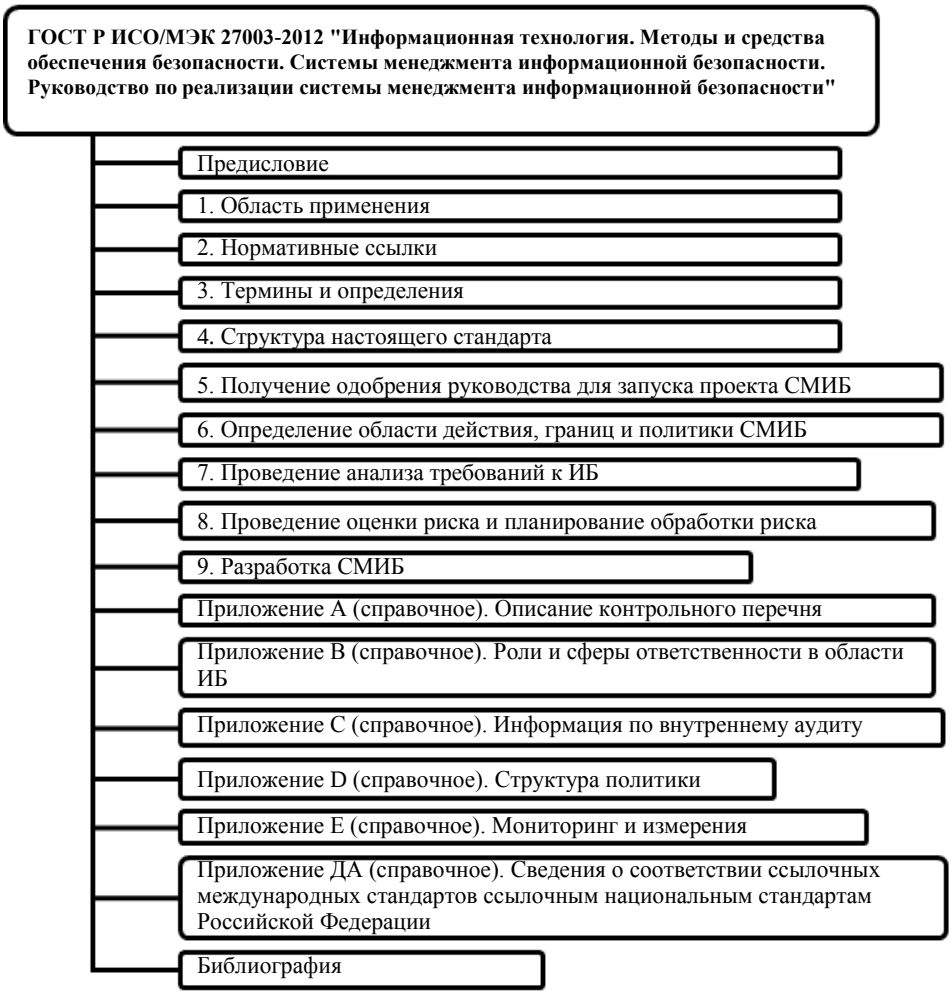


Рис. 2. Структура стандарта ГОСТ Р ИСО/МЭК 27003-2012

Рис. 3. Процесс планирования конечного внедрения СМИБ

В. *Проведение анализа организации*. При проведении анализа организации производится анализ требований к информационной безопасности. Анализ текущего положения состояния защищенности информации в организации важен, поскольку существуют требования и информационные активы, которые необходимо принять во внимание при внедрении СМИБ. Действия, описываемые в этой фазе, могут предприниматься в основном параллельно с действиями, описываемыми в рамках реализации предыдущей фазы, из соображений эффективности и практичности.

Г. *Проведение анализа рисков и планирование обработки рисков*. При внедрении СМИБ необходимо учитывать связанные с этим риски для информационной безопасности. Определение, оценка и планируемые действия в случае возникновения риска, а также выбор целей и средств управления являются важными этапами внедрения СМИБ и должны быть проработаны на данном этапе. Стандарт ГОСТ Р ИСО/МЭК 27005-2010 содержит специальные рекомендации по менеджменту риска для информационной безопасности и должен упоминаться при реализации данной фазы. Предполагается, что руководство дало поручение на внедрение СМИБ. Область действия и политика СМИБ определены, а также известны информаци-

онные активы и результаты оценки информационной безопасности.

Д. *Разработка СМИБ*. На данном этапе должны быть разработаны рабочий проект СМИБ и планируемые действия по внедрению системы. Конечный проект СМИБ должен быть уникальным в деталях для конкретной организации в зависимости от результатов предыдущих действий, а также результатов конкретных действий в фазе разработки, описываемых в данном пункте. Результатом выполнения этапа является конкретный конечный план проекта СМИБ.

Таким образом, правильно подготовленный и реализованный процесс получения одобрения внедрения СМИБ высшим руководством организации позволит создать такую политику ИБ, которая будет адекватна информационным рискам [2, 3, 6].

Рассматриваемый подход может быть использован организациями, применяющими системы ИБ, всеми типами таких организаций в любой сфере деятельности и любых масштабов. Четко выстроенное управление документами в организации является неотъемлемой частью политики ИБ, которая предполагает защиту и контроль документов как информационных активов организации, определение и защиту важной для организации информации.

Литература

1. ФЗ от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с измен. и доп.).
2. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
4. Приказ Министерства образования и науки РФ от 1 декабря 2016 г. № 1512 "Об утверждении федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалиста)".
5. ГОСТ ISO 9000-2011 Системы менеджмента качества. Основные положения и словарь.
6. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.

Modern approaches to managing the state of information security of an organization

Yu. I. Kovalenko, P. A. Monakhov
RTU MIREA, Moscow, Russia

The article discusses the procedures necessary for the successful development and implementation of an information security management system (ISMS) of an organization in accordance with the GOST R ISO / IEC 27001-2006 standard. The process of obtaining management approval of measures for the implementation of an ISMS is described, the process of determining and developing a management system from launch to drawing up implementation plans, a project for implementing an ISMS is determined on the basis of GOST R ISO/IEC 27003-2012, recommendations for planning a project of such a system, which result the final ISMS implementation plan.

Keywords: information security, data security, information security management system, information security policy.

Bibliography — 6 references. *Received April 12, 2021*

ВСЕМ ПУБЛИКАЦИЯМ ВСЕХ НАШИХ НАУЧНЫХ ИЗДАНИЙ БУДЕТ ПРИСВАИВАТЬСЯ КОД DOI!

Издательство ФГУП «НТЦ оборонного комплекса «Компас» заключило с Научной электронной библиотекой договор на оказание услуг по обслуживанию кодов DOI всех научных изданий, начиная с первых выпусков 2021 г.

DOI (Digital Object Identifier) – это уникальный код публикации, указывающий на ее электронное местонахождение, используемый в качестве международного стандарта предоставления информации в сети Интернет. DOI разработан компанией International DOI Foundation (IDF), основанной на членстве регистрационных агентств, предоставляющих конечным пользователям услуги по присвоению префиксов DOI.

Регистрационные агентства назначаются IDF и предоставляют услуги владельцам префиксов DOI: они распределяют префиксы DOI, регистрируют DOI для объектов и предоставляют необходимую инфраструктуру, позволяющую владельцам объектов присваивать DOI и передавать метаданные объектов. CrossRef — это международное регистрирующее агентство, предоставляющее DOI для научных публикаций (книги, журнальные статьи, материалы конференций и т. д.). Научная электронная библиотека с декабря 2019 года является официальным представителем компании CrossRef.

Разработанный компанией Научная электронная библиотека Сервис DOI позволяет без непосредственного участия представителей издательств осуществлять передачу метаданных публикаций в базу данных Crossref. eLIBRARY.RU берет на себя все функции, связанные с проверкой данных, формированием XML-файлов для загрузки в CrossRef, контролем и исправлением возможных ошибок в процессе загрузки. Подавляющее большинство российских научных издательств на регулярной основе размещает информацию в РИНЦ. Эта информация проходит проверку, нормализуется, структурируется и преобразуется в формат, поддерживаемый системой CrossRef. По мере поступления новых публикаций в РИНЦ они автоматически отправляются в CrossRef на регистрацию. Таким образом, подключение к сервису DOI на eLIBRARY.RU избавляет издательства от дополнительных хлопот, связанных с поддержкой DOI в своих изданиях.

В результате оказания услуги **статьям выпусков издательства ФГУП «НТЦ оборонного комплекса «Компас» будет присваиваться уникальный идентификационный номер (DOI), начиная с первых выпусков 2021 года**, с помощью которого можно определить метаданные опубликованных научных статей, их местонахождение в сети Интернет (URL), и иные данные путем обращения к поисковой системе Международного фонда DOI.

Приглашаем к публикации результатов научных разработок и исследований всех тружеников науки: руководителей научных организаций, ведущих научных сотрудников, разработчиков, аспирантов, докторантов в наших научных изданиях!

По материалам сайта: https://www.elibrary.ru

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 2021 г.
на издания ФГУП «НТЦ оборонного комплекса «Компас»

Наименование издания	Периодич-ность 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, 8 (495) 491-77-20.
E-mail: ivleva@ntckompas.ru
Адрес редакции: 125424, Москва, Волоколамское шоссе, д.77.
ФГУП «НТЦ оборонного комплекса «Компас».