УДК: 004.75, 004.41

Тенденции развития и практические реализации решений по обеспечению безопасности криптографических сетей

V. Kuzmenko, V. Makarov, K. Razgulyaev, D. Khan, P. Cherkashin, A. Shcherbakov

Development Trends and Practical Implementation of Solutions to Ensure the Security of Cryptographic Networks

Abstract. *Modern trends in ensuring the security of data transmission networks and ensuring the security of business processes are considered, the concepts and properties of cryptographic networks are formulated, the concepts of a service model and key containers are considered based on the development of quantum-protected networks, a practical solution and its architecture are described.*

Keywords: *cryptographic networks, service model, protocol, keys, key containers, electronic signature, key exchange, security, encryptor, HSM (hardware security module) - module for trusted storage of keys.*

***В.В. Кузьменко*[1]**
***В.Л.Макаров*[2]**
***К.А. Разгуляев*[3]**
***Д.В. Хан*[4]**
***П.А.Черкашин*[5]**
***А.Ю.Щербаков*[6]**

[1] Вице-президент Ассоциации РКЦФА по направлению Финтех.
v.kuzmenko@c3da.org
[2] Президент Некоммерческого партнерства разработчиков программного обеспечения «Руссофт»
[3] Центр научно-технологического форсайта Университета ИТМО, Санкт-Петербург.
E-mail: kirill.razgulyaev@gmail.com
[4] ООО «Финдинамика», Санкт-Петербург.
E-mail: dkhan@findinamika.com
[5] Научный сотрудник Ассоциации РКЦФА.
E-mail: pcherkashin@gmail.com
[6] Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник ЦРКЦФА, ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: x509@ras.ru

Аннотация. *Рассмотрены современные тренды в обеспечении безопасности сетей передачи данных и обеспечения безопасности бизнес-процессов, сформулированы понятия и свойства криптографических сетей, рассмотрены понятия сервисной модели и ключевых контейнеров с опорой на развитие квантово-защищенных сетей, описано практическое решение и его архитектура.*

Ключевые слова: *криптографические сети, сервисная модель, протокол, ключи, ключевые контейнеры, электронная подпись, обмен ключами, безопасность, шифратор, HSM (hardware security module) – модуль доверенного хранения ключей.*

ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ И СОВРЕМЕННЫЕ ТРЕНДЫ

В последние годы наметилось несколько примечательных и принципиально важных мировых трендов в области интернет-технологий.

Это в первую очередь повсеместное использование облачных сервисов. Благодаря развитию персональных мобильных устройств и всё большему распространению Интернета, сервисы все чаще переходят на облачную архитектуру для работы в непрерывном режиме. Однако развитие таких бизнес моделей как Iaas, PaaS, SaaS приводит к увеличению нагрузки на сеть, а огромное количество подключенных устройств повышает риск кибератак.

Криптографические сети (Cybersecurity Mesh, сети кибербезопасности). Подключения к облачным сервисам все большего количества устройств повышает риски отказа всей системы при внешних киберугрозах. Для того, чтобы не фокусироваться на построении единого «периметра» вокруг всех устройств и узлов ИТ-сети, а установить меньшие индивидуальные периметры вокруг каждой точки доступа, используются специальные криптографические сети, целью которых является обеспечение не только безопасности передаваемой и хранимой в сети информации, но и эффективного управле-

ния безопасностью каждой точки доступа (узла сети) из центра управления без предоставления доступа к более широкой части сети в случае нарушения безопасности данного узла. Такой подход позволяет устанавливать более надежные и гибкие модульные системы сетевой безопасности, дифференцируя уровни доступа к различным частям сети и предотвращая использование слабых мест данного узла для доступа к другим сетям и информации пользователей.

Цифровые активы. Благодаря применению технологии распределенных реестров пользователь получил инструменты контроля за перемещением информации и её состоянием, что в сочетании с безопасными криптографическими решениями позволило превратить любую информацию в цифровой актив. Вместе с тем эволюционировали учетно-расчетные системы данных: объединенные с платежными сервисами и инструментами цифровых подписей, они представляют собой легитимную для большинства юрисдикций цифровую среду полного цикла для работы с практически любым типом документов.

Сквозная аутентификация и универсальные аккаунты. Повсеместное использование открытых программных интерфейсов (API) позволило сделать бесшовную интеграцию приложений и сервисов для конечного пользователя и выстроить интерфейсы взаимодействия вокруг единого идентификатора пользователя. На основе этого тренда крупнейшие мировые и российские технологические платформы строят свои экосистемы, собирая персональные данные и подстраиваясь под потребительские особенности каждого клиента.

Сервисные модели. Сервисная модель (СМ), применяемая в первую очередь для квантово-защищенных сетей (КЗС) передачи данных, представляет собой инфраструктурное понятие, необходимое для целостного описания и моделирования процессов оказания услуг клиентам, в первую очередь связанных с защищенной передачей данных и защитой информации.

Принципиальное отличие квантово-защищенной сети от произвольной сети передачи данных – наличие механизма выработки и распределения квантовых и связанных с ними ключей, соответственно, основа СМ – процедуры распределения и хранения ключевой информации пользователей и построенные на их основе разнообразные сервисы [1].

СВОЙСТВА КРИПТОГРАФИЧЕСКИХ СЕТЕЙ

Таким образом, главным в новом технологическом укладе в сфере кибербезопасности является получение безопасного доступа к любому цифровому активу, независимо от того, где находится актив или человек. По прогнозам компании Gartner[1], к 2025 году криптографические сети будут поддерживать более половины запросов на управление цифровым доступом и станут главной архитектурой систем кибербезопасности.

Учитывая изложенные выше тренды, криптографические сети должны выполнять следующий минимальный набор функций:

- **Регистрация пользователя по его персональному идентификатору.** Не требуется специальный интерфейс для использования привычных приложений, система аутентификации автоматически подключается ко всем доступным сервисам. Пользователю должна быть предоставлена возможность реализации входа в систему без удостоверяющих центров и посредников.
- **Использование КЗС.** Вследствие повышения требований к безопасности инфраструктуры информационных систем, а также в связи с участившимися случаями компрометации классических методов шифрования, использование квантовой криптографии становится обязательным не только для защиты критически важной инфраструктуры, но и в массовом сегменте корпоративных систем обмена данных. Появление квантового компьютера в среднесрочной перспективе (3-5 лет) только ускоряет имплементацию данной технологии.
- **Необратимая или «сингулярная» загрузка ключей.** Все процессы управления ключами осуществляются по их номеру или идентификатору в хранилище, понимаемом как изоли-

[1] https://www.gartner.com/en/newsroom/press-releases/2020-10-19-gartner-identifies-the-top-strategic-technology-trends-for-2021 - Top Industry Trends at Gartner IT Symposium/Xpo 2020 Americas, October 19-22

рованное техническое устройство, в котором нет возможности прочитать загруженный или сформированный ключ ввиду отсутствия программных и технических интерфейсов извлечения ключа во «внешний мир» [2].

• **Использование безопасных ссылок для передачи файлов.** Хранение и передача файлов осуществляется внутри защищенного контура, доступ к которому имеют только авторизованные пользователи. Обмен файлами строится на передаче не самих исходных данных, а защищенных ссылок, доступ к которым в реальном времени регулируется владельцем.

• **Безопасное хранение ключей шифрования.** Внешний доступ к информации и ключам внутри хранилища ограничен благодаря использованию специального физического модуля хранения ключей (HSM). Данное оборудование позволяет использовать квантовые ключи шифрования без смены архитектуры всей системы.

• **Симметричное шифрование.** В основе криптографических сетей преимущественно используются симметричные алгоритмы шифрования и контроля целостности (имитовставки), являющиеся стойкими к квантовым вычислениям и значительно менее ресуросемкими по сравнению с ассиметричными алгоритмами шифрования (на основе пар приватный – открытый ключ).

• **Низкая стоимость.** Общая стоимость издержек значительно снижается за счет отсутствия необходимости устанавливать сертифицированное средство криптографической защиты (СКЗИ) на каждое пользовательское устройство.

• **Легитимность.** Обеспечение корректной национальной регуляции в части использования криптографических средств.

АРХИТЕКТУРА КЗС И КЛЮЧЕВЫЕ КОНТЕЙНЕРЫ

В силу того, что обмен квантовыми ключами физически возможен только для смежных узлов квантовой сети, для обмена информации транзитного характера (для произвольной топологии КЗС, подключения к другим сетям и обеспечения работы абонентов без квантового оборудования) необходимо использовать другие виды ключей, последовательно используя защищенные каналы, образованные между смежными узлами.

Кроме того, передача ключей абонентам или в оконечные узлы сети, не содержащие квантового оборудования, должна происходить в зашифрованном виде, для чего используется конструкция ключевого контейнера.

Ключевой контейнер – информационный объект КЗС и СМ, использующийся для защищенной (обеспечивающей целостность и конфиденциальность) передачи ключей между элементами КЗС.

Ключевой контейнер (КК) состоит из совокупности открытых и закрытых полей, целостность которых зафиксирована.

КК в обязательном порядке содержит ключи, которые зашифрованы таким образом, чтобы обеспечить их безопасную передачу и хранение внутри или вовне КЗС (для этого используется шифрование на квантовых ключах, на паролях, на ключах аппаратных хранилищ и т.д.). Кроме того, КК содержит дополнительную информацию, обеспечивающую функционирование в рамках сервисной модели: назначение ключа, владельца ключа, количество использований ключа и др.

Перечень возможных сервисов криптографических сетей

Таким образом, возможные виды защищенных сервисов определяются полем «назначение ключа»:

1. Ключи транзитной передачи данных между узлами криптографической сети.
2. Ключи клиентов для связи с опорными узлами.
3. Ключи клиентов для связи между собой (для поддержания режима конфиденциальности абонентской связи).
4. Ключи инициализации датчиков случайных чисел (ДСЧ) для программных ДСЧ, расположенных у клиента или в опорных узлах.
5. Ключи оконечных сервисов (IP-телефония, видеосвязь).
6. Ключи корпоративных хранилищ и облаков.
7. Ключи внутрисетевых и корпоративных распределенных реестров.

8. Ключи для работы с аппаратными хранилищами данных.

9. Ключи для взаимодействия со сторонними сервисами и другими системами защищенной передачи данных.

СЦЕНАРИИ ПРИКЛАДНОГО ИСПОЛЬЗОВАНИЯ

Для прикладного использования системы в качестве типовой задачи защиты бизнес-процессов рассматривается защита данных в открытых сервисах, используемых в бизнес-процессе, включая мессенджеры и открытую почту. Практика показала, что даже при работе с конфиденциальной информацией, приоритет отдаётся в пользу удобства, а не безопасности.

Корпоративные решения неудобны и сложны в использовании, а их ставка на безопасную передачу данных - зачастую лишь маркетинговый ход. Поэтому у многих компаний сформировалась потребность в обеспечении защиты информации при использовании открытых сервисов.

Специалистами российской компании ApiQ был реализован новый подход к обеспечению безопасности бизнес-процессов, который может гарантировать невозможность передачи конфиденциальной информации за периметр организации и связанный с применением модулей хранения пользовательских ключей (подход реализован в виде решения «QuantGuard»). Теоретическая модель и протокол решения рассмотрены в [3, 4].

Под «открытыми сервисами» понимаются абонентские программные средства и обеспечивающая их инфраструктура (например, общедоступные почтовые клиенты Gmail, Outlook, Mail.ru, Yandex mail), обслуживающие их сервера, а также различного рода мессенджеры, например, Telegram, Whatsapp и другие.

Предлагаемая технология позволяет существенно снизить риски ИБ и не нагружать пользователей неудобными и непривычными им сервисами. Кроме того, корпоративная сеть становится замкнутой и нет необходимости устанавливать сертифицированное СКЗИ на каждое устройство, что позволяет снизить издержки и обеспечить корректную национальную регуляцию в части использования криптографических средств.

В данном случае речь идет о модели внешнего нарушителя, т.е. нарушителя, который может читать и изменять информацию в каналах связи (в телекоммуникационной компоненте информационно-телекоммуникационной системы). Полагаем, что владелец системы (организатор бизнес-процессов) является лицом доверенным и не заинтересован в нарушении свойств безопасности.

Угроза безопасности выглядит следующим образом: пользователь использует различные открытые сервисы для передачи служебной информации, что приводит к систематическим инцидентам информационной безопасности (ИБ), связанным с утечками корпоративных данных за периметр безопасности (т.е. к лицам, не участвующим в бизнес-процессах, прямым конкурентам и нарушителям информационной безопасности).

Использование решения «QuantGuard» (рис.1) позволяет нейтрализовать данную угрозу и не допустить попадания защищенной информации за периметр криптографической сети. Кроме того, предложенный подход в сочетании с квантовыми коммуникациями (реализацией сервисов на базе квантового HSM) позволяет решить множество актуальных проблем, например, уйти от зависимости от управляющих ключами электронной подписи удостоверяющих центров, а также вообще уйти от влияния человеческого фактора в вопросах управления безопасностью, создать современную надежную инфраструктуру, обеспечивающую на корпоративном уровне управление доступами и безопасный обмен информацией внутри корпоративного периметра на основе симметричных криптографических алгоритмов, исключая человеческий фактор, при формировании паролей, криптографических ключей, сертификатов открытого ключа.

Использование квантовой криптографии особенно актуально в связи с принятием дорожной карты по созданию в России квантовой сети. Сейчас реализуется первый сегмент сети между Москвой и Санкт-Петербургом, что позволит заинтересованным игрокам использовать уникальные свойства квантовых криптографических ключей в своих сервисах и решениях.

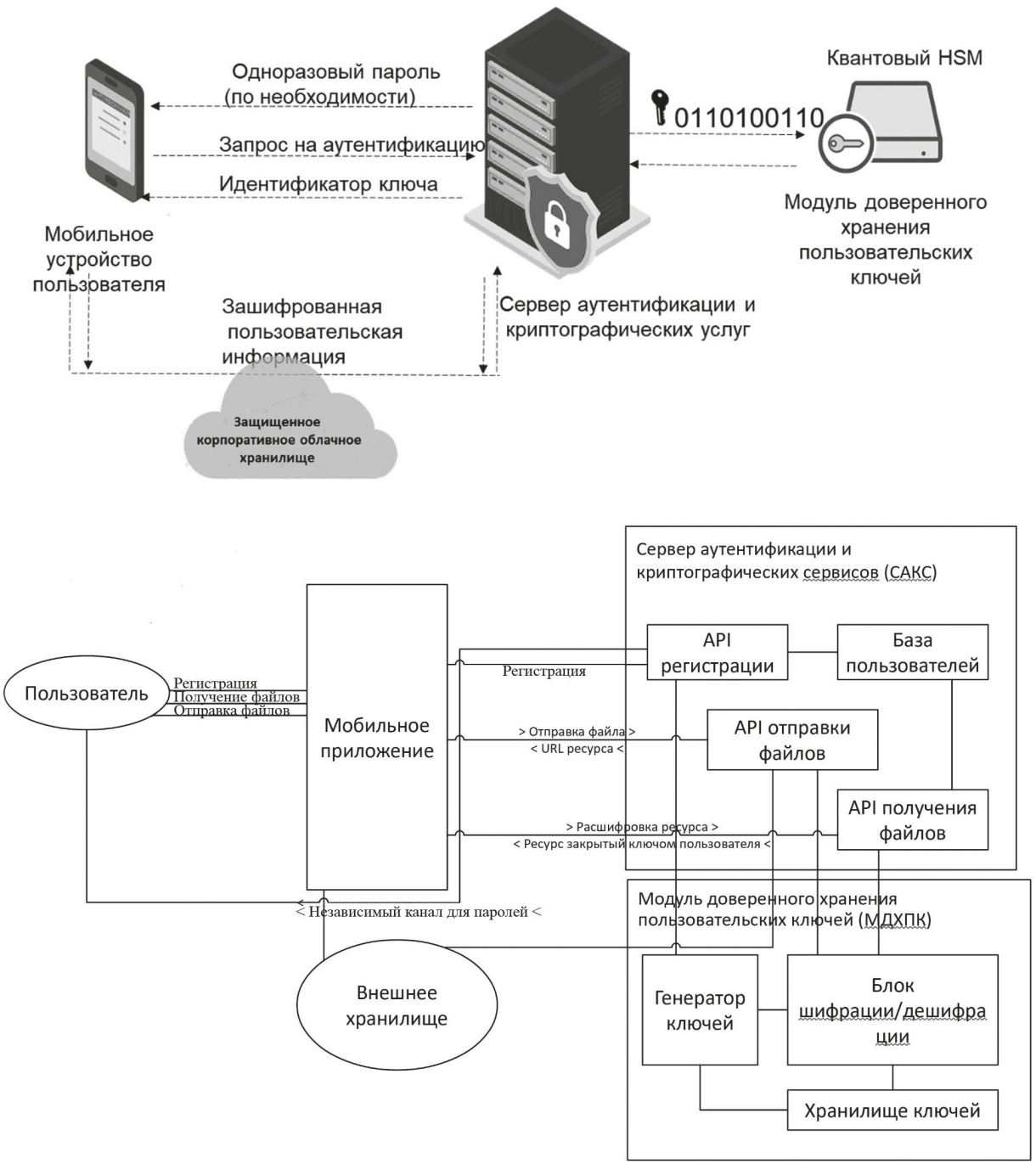

Рис. 1. Варианты архитектуры решения «QuantGuard»

Таким образом, данная система криптографических сетей с применением симметричного шифрования и квантовых коммуникаций способна организовать устойчивую к внешним угрозам безопасную среду работы с файлами и обмена информацией. Учитывая вектор технологического развития, данная архитектура имеет серьезный задел на будущее и отвечает всем современным требованиям как мировых, так и национальных стандартов безопасности.

ВЫВОДЫ

Для реализации сервисной модели криптографической сети необходимо создание подсистемы, обеспечивающей ее функционирование и опирающейся на механизм ключевых

контейнеров, который позволит реализовать и изолировать различные сервисы на базе поля назначения ключа.

Этот же фактор облегчит коммерциализацию СМ, поскольку селектирование и билинг сервисов может быть достаточно просто реализован.

Кроме того, механизм контейнеров позволяет легко добавлять различные сервисы, реализовывать механизмы конвертации ключевых форматов для других систем защищенной передачи данных.

Дополнительными преимуществами использования КК будет повышение устойчивости и надежности сети за счет хранения контейнеров (исключая ключи ЭП) как минимум у пары подсистем или пользователей, а также возможность проведения мониторинга информации о сервисах (с использованием информации в контейнерах, например, об объеме трафика, закрытого на данном ключе) и восстановления КК при сбоях или поломках оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Щербаков А.Ю. Перспективы современной криптографии // Проектирование будущего. Проблемы цифровой реальности. – 2020. – № 1 (3). – С. 227-233.

2. Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра // Научно-техническая информация. Серия 2: Информационные процессы и системы. – 2020. – № 1. – С. 11-18.

3. Кузьменко В.В., Макаров В.Л., Разгуляев К.А., Хан Д.В., Щербаков А.Ю. Новый подход к обеспечению безопасности периметра бизнес-процессов и аутентификации пользователей в корпоративной системе // Вестник современных цифровых технологий. – 2020. – №3. – С. 10-13.

4. Бородулина С.А., Гриневич В.Е., Тихоненко О.О., Щербаков А.Ю. О новом подходе к реализации трансграничной проверки электронных подписей // Вестник современных цифровых технологий. – 2020. – №4. – С. 20-25.