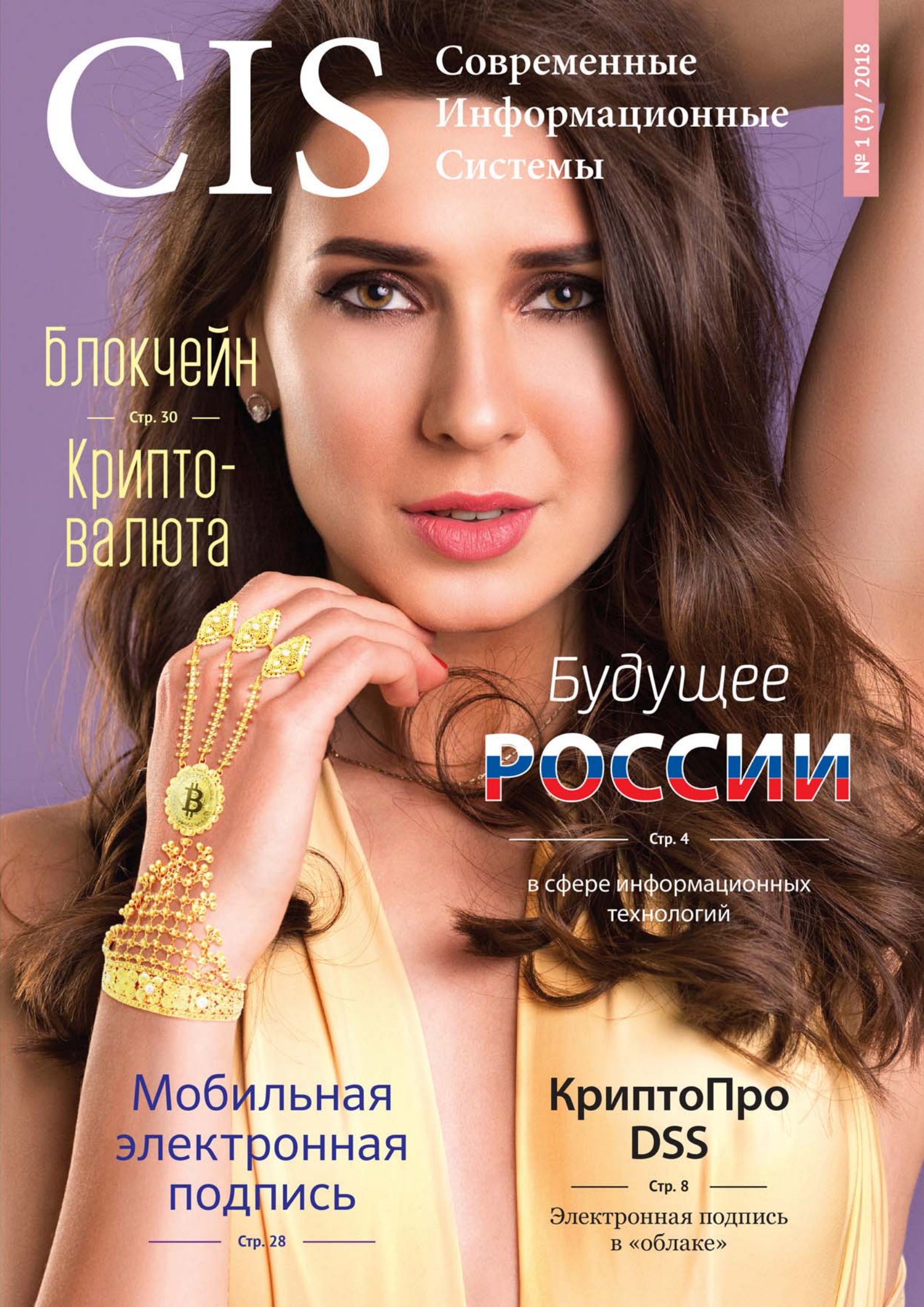
CIS
Современные Информационные Системы
№ 1 (3) / 2018



Блокчейн

Стр. 30

Крипто-валюта

Будущее РОССИИ

Стр. 4

в сфере информационных технологий

Мобильная электронная подпись

Стр. 28

КриптоПро DSS

Стр. 8

Электронная подпись в «облаке»

ПРЕДИСЛОВИЕ

ЦИФРОВАЯ ЭКОНОМИКА

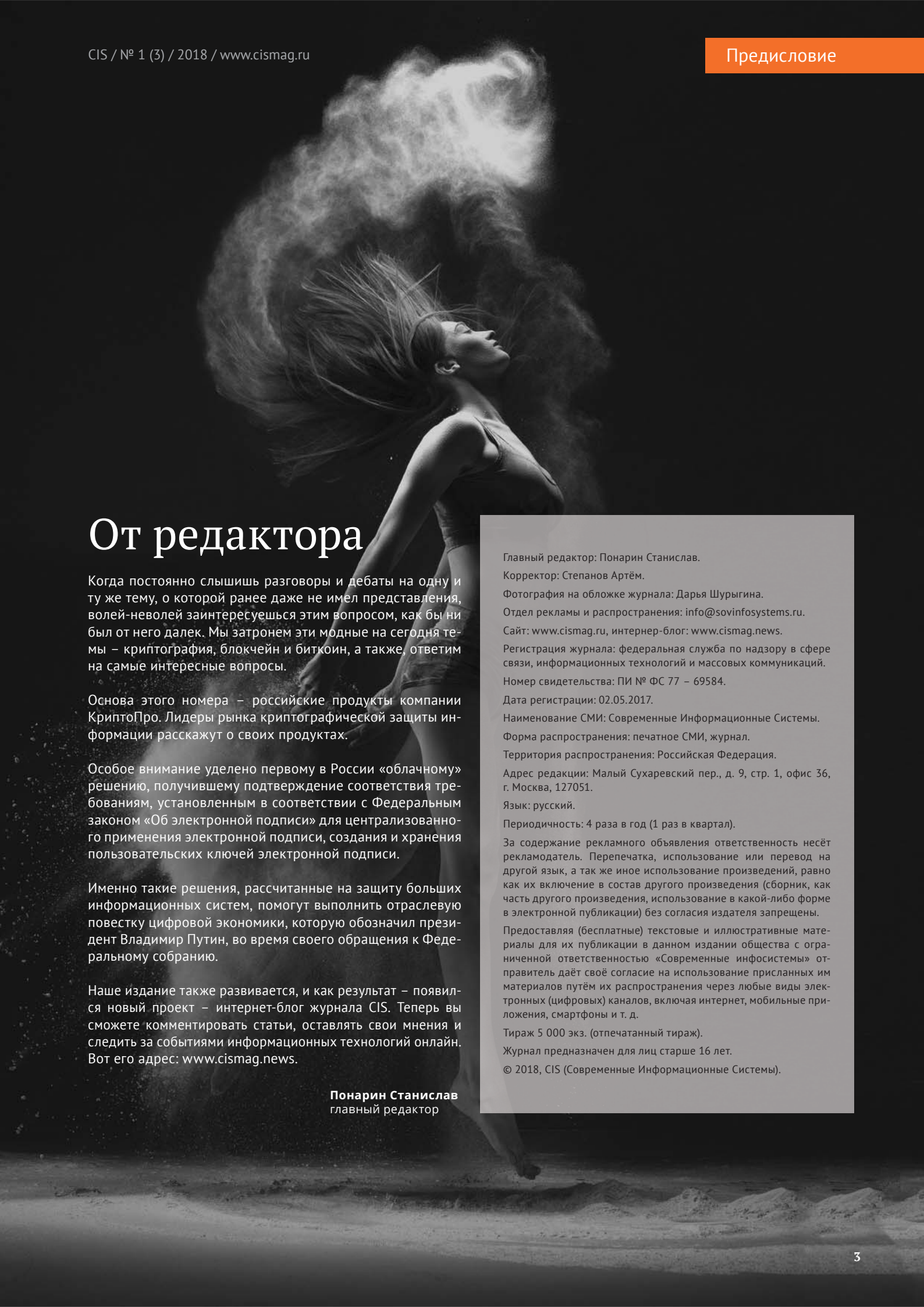
РЕШЕНИЯ

ПРОДУКТЫ

ТЕХНОЛОГИИ

ОПЫТ

КАЛЕНДАРЬ



От редактора

Когда постоянно слышишь разговоры и дебаты на одну и ту же тему, о которой ранее даже не имел представления, волей-неволей заинтересуешься этим вопросом, как бы ни был от него далек. Мы затронем эти модные на сегодня темы – криптография, блокчейн и биткоин, а также, ответим на самые интересные вопросы.

Основа этого номера – российские продукты компании КриптоПро. Лидеры рынка криптографической защиты информации расскажут о своих продуктах.

Особое внимание уделено первому в России «облачному» решению, получившему подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» для централизованного применения электронной подписи, создания и хранения пользовательских ключей электронной подписи.

Именно такие решения, рассчитанные на защиту больших информационных систем, помогут выполнить отраслевую повестку цифровой экономики, которую обозначил президент Владимир Путин, во время своего обращения к Федеральному собранию.

Наше издание также развивается, и как результат – появился новый проект – интернет-блог журнала CIS. Теперь вы сможете комментировать статьи, оставлять свои мнения и следить за событиями информационных технологий онлайн. Вот его адрес: www.cismag.news.

Понарин Станислав
главный редактор

Главный редактор: Понарин Станислав.

Корректор: Степанов Артём.

Фотография на обложке журнала: Дарья Шурыгина.

Отдел рекламы и распространения: info@sovinfosystems.ru.

Сайт: www.cismag.ru, интернер-блог: www.cismag.news.

Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Номер свидетельства: ПИ № ФС 77 – 69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

Адрес редакции: Малый Сухаревский пер., д. 9, стр. 1, офис 36, г. Москва, 127051.

Язык: русский.

Периодичность: 4 раза в год (1 раз в квартал).

Тираж 5 000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

Будущее России в сфере информационных технологий

Президент Российской Федерации Владимир Путин во время своего обращения к Федеральному собранию, заявил о необходимости интегрировать новые технологии в логистическую и транспортную инфраструктуру, в массовые государственные проекты.

«Россия должна стать не только ключевым логистическим и транспортным узлом планеты, но, подчеркну, и одним из основных центров хранения, обработки, передачи и надежной защиты информационных массивов, так называемых больших данных. В целом, развивая инфраструктуру, нужно обязательно учитывать глобальные технологические изменения. То есть, уже сегодня закладывать в проекты конкретные решения, которые позволят совместить инфраструктуру с беспилотным транспортом, цифровой морской и воздушной навигацией и с помощью искусственного интеллекта организовать логистику», – сказал президент.

Если кратко, президент говорил о следующих вещах:

- сделать законы доступными и легко понимаемыми;
- обеспечить повсеместный быстрый доступ в интернет к 2024 году;
- создать национальную социальную сеть;
- создать систему, которой могли бы пользоваться люди с ограниченными возможностями;
- облегчить налоговое бремя для инновационных компаний;
- развивать математическую и физическую науку;
- сделать отечественное образование более конкурентным;
- упростить ведение дел для малого предпринимательства, особенно в части интернет-эквайринга;
- упростить доступ граждан к государственным услугам;
- упростить документооборот за счёт его автоматизации;
- упростить перемещения по стране, усовершенствовать транспортную систему;
- облегчить интернет-коммерцию.

В Проектном офисе по реализации программы «Цифровая экономика» отметили, что обозначенная отраслевая повестка сейчас активно формируется.

«Президент в своем выступлении обозначил отраслевую повестку цифровой экономики: Россия должна интегрировать цифровые технологии в транспорт и логистику, здравоохранение, государственное управление, энергетику. По данному направлению в рамках работы Правительственной Подкомиссии по цифровой экономике сейчас формируются новые направления, где в ближайшее время в программу будут включены отраслевые направления», – сказал руководитель Проектного офиса по реализации программы «Цифровая экономика Российской Федерации» Евгений Кисляков.

eToken

Продукты линейки eToken –
основа инфраструктуры информационной
безопасности современного предприятия

etokenstore.ru

КриптоПро DSS

Программно-аппаратный комплекс предназначен для централизованного защищённого хранения закрытых ключей пользователей, а также для удалённого выполнения операций по созданию электронной подписи с использованием ПАКМ КриптоПро HSM.

ПАК обеспечивает

- Создание электронной подписи любого формата электронного документа.
- Отсутствие необходимости в установке клиентской части.
- Широкий охват платформ и устройств, с которых пользователь может работать с КриптоПро DSS, поскольку необходим лишь веб-браузер.
- Снижение стоимости развёртывания и владения инфраструктурой ЭП, т. к. нет необходимости установки средств ЭП на каждое рабочее место пользователя, а управление всей инфраструктурой сосредоточено на одном сервере.
- Снижение риска компрометации ключей пользователей за счёт их централизованного защищённого хранения.
- Возможность использования стандартного интерфейса CryptoAPI с помощью дополнительного модуля КриптоПро Cloud CSP на базе КриптоПро CSP версии 5.0 для обеспечения совместимости с традиционными приложениями.
- Возможность работы с локальными ключами электронной подписи на рабочих местах пользователей (режим КриптоПро DSS Lite).
- Лёгкость встраивания функций создания ЭП в прикладные системы за счёт наличия простых интерфейсов автоматизации на базе стандартных средств протокола HTTP и веб-сервисов (API), включая SOAP и REST.
- Возможность усиления ранее созданной электронной подписи до усовершенствованного формата (CAdES-T или CAdES-X Long Type 1) путём добавления меток времени и информации о статусе сертификата.
- Возможность применения различных схем аутентификации пользователя для доступа к его ключам, включая возможность интеграции со сторонними центрами идентификации по протоколам SAML (WS-Security) и OAuth (в т. ч. с корпоративным доменом на базе Microsoft AD и OpenLDAP).
- Централизованное/локальное шифрование/расшифрование электронных документов.
- Пакетная обработка электронных документов (подписание/шифрование по API одной командой набора однотипных электронных документов).
- Поддержка нескольких экземпляров сервисов электронной подписи и центров идентификации с различными параметрами настройки функционирования на одном сервере КриптоПро DSS.
- Визуализация (отображение) подписываемых электронных документов формата PDF, DOCX, TXT, XML. Возможно расширение перечня форматов отображаемых файлов.
- Создание видимой подписи с логотипом и текстом и в виде изображения (image appearance) с учётом требований Приказа Минкомсвязи и ФСО России от 27.05.2015 №186/258 для документов формата PDF с использованием API (SOAP/REST).
- Возможность интеграции с корпоративными хранилищами документов, поддерживающими стандарт CMIS.
- Возможность настройки оформления графического веб-интерфейса (цветовой гаммы, логотипов, шрифтов и т. п.) в соответствии с корпоративным стилем и требованиями заказчика.

Поддерживаемые форматы электронной подписи

- Необработанная электронная подпись ГОСТ 34.10 – 2001.
- Усовершенствованная подпись (CAdES-BES, CAdES-T и CAdES-X Long Type 1).
- Подпись XML-документов (XML Digital Signature, XMLDSig).
- Подпись документов PDF.
- Подпись документов Microsoft Office.

Требования к программному обеспечению

КриптоПро DSS предоставляет пользователям интерактивный веб-интерфейс для управления криптографическими ключами и создания ЭП под документом, который пользователь загружает на КриптоПро DSS. Таким образом, для работы с КриптоПро DSS пользователю необходим только веб-браузер – никаких СКЗИ или средств электронной подписи устанавливать не нужно. Благодаря этому использовать функции КриптоПро DSS можно с любого устройства с любой аппаратной платформой и операционной системой, где есть веб-браузер.

Безопасность

Создание и хранение ключей электронной подписи пользователей осуществляется с использованием специального защищённого модуля КриптоПро HSM. Каждый пользователь получает доступ к своим ключам после прохождения процедуры надёжной многофакторной аутентификации в КриптоПро DSS. Дополнительно каждый ключевой контейнер защищается индивидуальным PIN-кодом, который знает и может сменить только владелец ключа электронной подписи.

Пользователями КриптоПро DSS управляет оператор, который имеет возможность посредством веб-интерфейса или API выполнять следующие действия:

- создание пользователя;
- блокирование и удаление пользователя;
- генерация ключа электронной подписи пользователя;
- формирование и передача в удостоверяющий центр запроса на создание сертификата ключа проверки электронной подписи;
- установку полученного сертификата пользователю;
- настройку параметров аутентификации пользователей;
- аудит и формирование аналитической отчётности по выполняемым пользователями операциям;
- сброс пароля в случае его утраты пользователем.

Способы аутентификации

В зависимости от настроек КриптоПро DSS может реализовывать следующие способы аутентификации пользователя:

- классическая однофакторная аутентификация по логину и паролю с дополнительной защитой доступа по протоколу TLS;
- криптографическая аутентификация по алгоритму HMAC в соответствии с Р-50.1.113-2016 с помощью мобильного приложения myDSS или специального апплета на SIM-карте;
- двухфакторная аутентификация с использованием цифровых сертификатов и USB-токенов или смарт-карт;
- двухфакторная аутентификация с дополнительным вводом одноразового пароля, доставляемого пользователю посредством SMS (OTP-via-SMS).

Высокая отказоустойчивость и доступность

Обеспечивается с помощью горячего резервирования и кластеризации всех компонентов КриптоПро DSS и КриптоПро HSM с помощью специализированных балансировщиков нагрузки (например, HAProxy) и SQL-кластера на базе технологий MS SQL Server AlwaysOn availability groups.

В случае нарушения функционирования любого из зарезервированных компонентов переключение на резервные, в т. ч. размещённые на территориально-удалённых технологических площадках (резервных ЦОД), осуществляется автоматически без участия обслуживающего персонала и без потери сохранённых данных.

Мониторинг

В составе с КриптоПро DSS может использоваться специальный программный комплекс класса Network Performance Monitoring and Diagnostics (NPMD) «КриптоПро Центр мониторинга» для мониторинга работоспособности и оперативного уведомление администраторов СЭП о выявленных сбоях, ошибках функционирования и прочих нештатных ситуациях.

КРИПТОПРО

«КриптоПро» *– разработка средств криптографической защиты информации.*

info@cryptopro.ru
www.cryptopro.ru

КриптоПро DSS – электронная подпись в «облаке»

СЭП КриптаПро DSS позволяет существенно снизить стоимость развёртывания и владения инфраструктурой ЭП, т. к. нет необходимости установки средства электронной подписи на каждое рабочее место пользователя, а управление всей инфраструктурой сосредоточено на одном сервере.

Сервер электронной подписи (СЭП) позволяет хранить закрытые ключи пользователей централизованно в «облаке». КриптоПро DSS предоставляет пользователям интерактивный веб-интерфейс для управления криптографическими ключами и создания электронной подписи (ЭП) в документе, который пользователь загружает в «облако». Для работы пользователю необходим только браузер, никаких средств электронной подписи (СКЗИ) устанавливать не нужно.

СЭП КриптоПро DSS поддерживает

- любые устройства;
- любые платформы;
- любые браузеры;
- различные схемы аутентификации.

Типовая схема использования СЭП КриптоПро DSS

На примере систем дистанционного банковского обслуживания (ДБО).

1. Пользователь отправляет сформированный платёжный документ в систему ДБО.
2. Система ДБО, используя штатные механизмы КриптоПро DSS, передаёт подписываемый документ и маркер доступа, содержащий информацию о пользователе (имя пользователя, номер мобильного телефона и т. п.).
3. Для подтверждения подписания документа КриптоПро DSS направляет пользователю SMS-сообщение, содержащее код подтверждения подписания и значимые поля документа (например, получатель, сумма и т. п.) на номер мобильного телефона, полученный в маркере доступа.
4. Пользователь вводит полученный код подтверждения в поле формы веб-интерфейса системы ДБО.
5. Система ДБО передаёт полученный код подтверждения КриптоПро DSS.
6. КриптоПро DSS, используя функции ПАКМ «КриптоПро HSM», отправляет запрос на подписание документа с использованием закрытого ключа пользователя и получает подписанный документ.
7. КриптоПро DSS передаёт подписанный документ в систему ДБО.

Продукты и услуги

Продукты компании КриптоПро применяются в системах электронного документооборота, исполнения госзаказа, сдачи бухгалтерской и налоговой отчётности и т. п.

Продукты компании КриптоПро обеспечивают

- создание и проверку квалифицированной электронной подписи;
- соответствие требованиям законодательства к электронному документообороту и защите персональных данных;
- контроль целостности и подтверждение подлинности документов;
- защиту конфиденциальных данных в информационных потоках компании;
- защиту от несанкционированного доступа;
- надёжную доказательную базу в суде;
- полнофункциональное и защищённое использование мобильных устройств.

Компания КриптоПро оказывает

- полный спектр консалтинговых услуг по применению ЭП и шифрования, включая проектирование и создание удостоверяющих центров;
- услуги аккредитованного и неаккредитованного УЦ;
- услуги центра управления сертификатами VPN.

О компании

С момента создания (2000 г.) КриптоПро занимает лидирующее положение в области разработки средств криптографической защиты информации (СКЗИ) и развития инфраструктуры открытых ключей (PKI) на территории РФ.

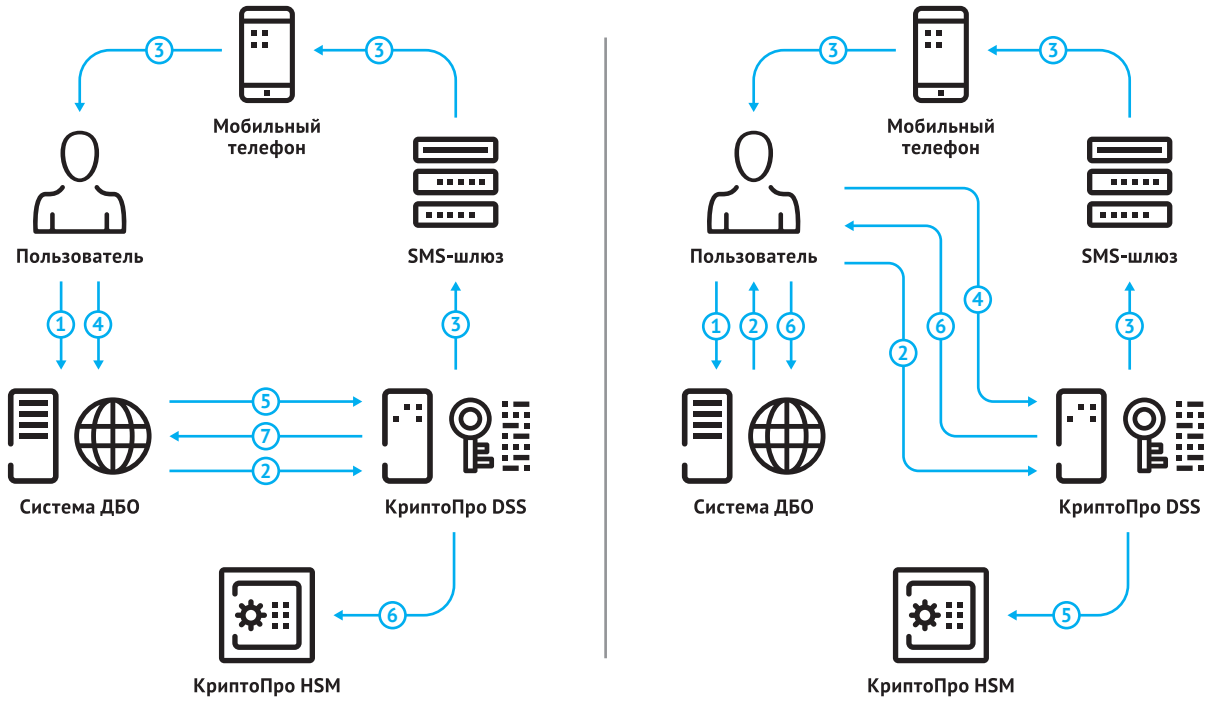
КРИПТОПРО

«КриптоПро» – разработка средств криптографической защиты информации.

info@cryptopro.ru
www.cryptopro.ru

Типовые схемы использования КриптоПро DSS

КриптоПро DSS предоставляет программные интерфейсы автоматизации, которые позволяют интегрировать использование сервера электронной подписи в существующие бизнес-процессы и системы. Ниже представлены типовые схемы использования КриптоПро DSS на примере систем дистанционного банковского обслуживания (ДБО).



HTTP API-интеграция

1. Пользователь отправляет сформированный платёжный документ в систему ДБО.

2. Система ДБО, используя штатные документированные механизмы КриптоПро DSS (HTTP API), перенаправляет пользователя на веб-интерфейс КриптоПро DSS, передавая в этом перенаправлении подписанный маркер доступа (SAML-токен), содержащий информацию о пользователе (имя пользователя, номер мобильного телефона и т. п.), и подписываемый документ.

3. Для подтверждения подписания документа КриптоПро DSS направляет пользователю SMS-сообщение, содержащее код подтверждения подписания и значимые поля документа (например, получатель, сумма и т. п.), на номер мобильного телефона полученный в маркере доступа.

4. Пользователь вводит полученный код подтверждения в поле формы веб-интерфейса КриптоПро DSS.

5. КриптоПро DSS, используя документированные функции ПАКМ «КриптоПро HSM», отправляет запрос на подписание документа с использованием закрытого ключа пользователя и получает подписанный документ.

6. КриптоПро DSS перенаправляет пользователя на веб-интерфейс системы ДБО, передавая в перенаправлении подписанный документ.

SOAP-интеграция

1. Пользователь отправляет сформированный платёжный документ в систему ДБО.

2. Система ДБО, используя штатные документированные механизмы КриптоПро DSS (SOAP), передаёт подписываемый документ и подписанный маркер доступа (SAML-токен), содержащий информацию о пользователе (имя пользователя, номер мобильного телефона и т. п.).

3. Для подтверждения подписания документа КриптоПро DSS направляет пользователю SMS-сообщение, содержащее код подтверждения подписания и значимые поля документа, на номер мобильного телефона полученный в маркере доступа.

4. Пользователь вводит полученный код подтверждения в поле формы веб-интерфейса системы ДБО.

5. Система ДБО передаёт полученный код подтверждения КриптоПро DSS.

6. КриптоПро DSS, используя документированные функции ПАКМ «КриптоПро HSM», отправляет запрос на подписание документа с использованием закрытого ключа пользователя и получает подписанный документ.

7. КриптоПро DSS передаёт подписанный документ в систему ДБО.

КРИПТОПРО

www.cryptopro.ru

CIS / № 1 (3) / 2018 / www.cismag.ru

SD-WAN: упрощённая сеть для предприятий с распределённой инфраструктурой

Как не отстать от меняющихся технологий

За последнее десятилетие произошло слияние двух главных технологических тенденций: виртуальных вычислений и развития «облачных» технологий, которые теперь готовы оказывать значительное влияние на корпоративные сети. Обе эти тенденции резко повышают важность корпоративной сети для производительности бизнеса.

В результате происходит значительное увеличение сетевого трафика из филиала в центр обработки данных, между разными филиалами, а также между различными устройствами и центром обработки данных. И немалая часть этого трафика представляет собой общение в режиме реального времени, включая видео- и голосовую связь. Это приводит к потребности в большей пропускной способности, к большему количеству чувствительных к задержкам приложений, к большей зависимости от доступности и качества сети.

Появление новых технологий означает, что сетевой трафик в организациях с распределённой инфраструктурой используется новыми способами.

Удалённым пользователям необходима не только дополнительная пропускная способность, особенно в сфере видео- и мультимедийных средств, — они ожидают быстрого доступа к облачным приложениям, программному обеспечению как услуге (SaaS) и приложениям для удалённого хранения данных.

Проблема использования традиционных сетей MPLS

Традиционные сети, использующие многопротокольную коммутацию по меткам (Multiprotocol Label Switching, MPLS), по которым идёт трафик из удаленных офисов в центр обработки данных, не могут обеспечить высокую пропускную способность, малую чувствительность к задержкам и высокую производительность, необходимые для доступа к «облачным» приложениям. В сочетании со сложностью выполнения удаленных операций и новыми требованиями в отношении управления и безопасности это делает сети MPLS непригодными для данной цели.

Существующая сетевая архитектура на сегодняшний день не готова для решения современных задач, отли-

чающихся увеличением числа подключенных устройств, «облачных» моделей, требований безопасности и расширением мобильности.

Результат? Существующая инфраструктура неспособна соответствовать требованиям безопасности и современным бизнес-моделям. Для них требуется малое время отклика, недоступное в негибкой сети. Всё это делает приоритетной задачу совершенствования сети не только для директора по информационным технологиям, но и для всей структуры управления.

Новые сети должны соответствовать растущим потребностям бизнеса

Потребности бизнеса и рыночные тенденции стимулируют эволюцию сетей, и руководство больше не может игнорировать этот факт. Предприятиям необходима интеллектуальная сеть, способная адаптироваться соответствующим образом. Сеть с новой концепцией должна:

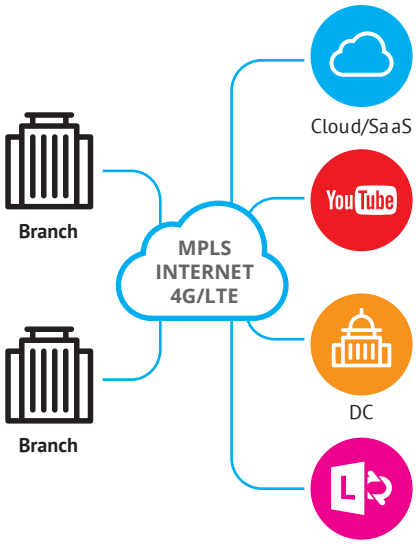
- обеспечивать доступ пользователей к приложениям независимо от устройства десктопа и маршрута соединения, а также от нахождения в частном или общедоступном «облаке»;
- обеспечивать одинаковую комфортность работы независимо,откуда осуществляется подключение;
- оптимизировать трафик для «облака» и мобильных устройств, обеспечив наилучшую комфортность работы пользователей;
- применять критерии приоритизации и оптимизации в зависимости от используемых данных и приложений;
- обеспечивать возможность развертывания приложений без особых требований к сети;
- упрощать управление распределенными сервисами, а в идеале даже автоматизировать их;
- обеспечивать улучшенную видимость для сетевых администраторов, позволяя им исключать потенциальные конфликты в сети;
- интегрировать в сеть систему безопасности с несколькими слоями и несколькими точками контроля;
- быстро осуществлять обслуживание приложений и служб для поддержания конкурентоспособности бизнеса.

Из-за увеличения числа мобильных приложений сетевые администраторы также должны предусматривать и планировать альтернативные способы подключения мобильных устройств к корпоративной глобальной сети, чтобы предоставлять пользователям более качественную связь, когда они находятся вне офиса.

Удовлетворение потребностей предприятий с распределённой инфраструктурой

Компании стремятся получить экономичные решения, упрощающие работу. Программно определяемая глобальная сеть (SD-WAN) интегрируется с имеющейся у вас архитектурой глобальной сети, чтобы оптимизировать управление и повысить эффективность сети.

SD-WAN использует программное обеспечение для определения наиболее эффективного способа маршрутизации трафика в удаленные места. SD-WAN передаёт сетевой мониторинг и управление с физических устройств на центральный контроллер, что даёт сетевым администраторам возможность конфигурирования и контроля трафика на основе централизованных политик и правил безопасности.



Упрощение управления сетями

SD-WAN использует «облачное» программное обеспечение и технологии для упрощения доставки сервисов глобальной сети в удалённые офисы. Программная виртуализация позволяет сетевым администраторам проще управлять сетевыми сервисами посредством абстрактного представления функциональности более высокого уровня.

SD-WAN позволяет ИТ-администраторам и бизнес-менеджерам быстро и легко развертывать связь через интернет, обеспечивая безопасное и надёжное подключение с более высокой пропускной способностью при снижении затрат.

Компаниям, которые ищут альтернативное решение для своих удалённых офисов и мобильных устройств, SD-WAN относительно легко внедрить, что приводит к значительной выгоде.

Сеть стала стратегическим активом, и появилась необходимость в переходе на SD-WAN, благодаря чему решаются серьёзные проблемы сетевых администраторов. Этот новый взгляд на сеть обеспечивает требуемые гибкость и скорость реагирования, а также контроль и безопасность, необходимые для удовлетворения потребностей нового предприятия с распределённой инфраструктурой.

Оптимизация организаций, расположенных в нескольких местах

Итак, каковы преимущества SD-WAN для организаций с распределённой инфраструктурой?

Надёжность сети

Благодаря тому, что решения SDWAN быстро определяют и обходят перебои в сети или некачественные каналы, они могут предотвратить влияние проблем в каком-нибудь одном канале на работу пользователей. Это обеспечивает надёжное соединение пользователей с их приложениями и предотвращает простои бизнеса.

Оперативность бизнеса

SD-WAN даёт возможность быстрого внедрения сервисов глобальной сети в удалённые офисы без необходимости в ИТ-поддержке на месте. Новые схемы можно легко добавлять, не прерывая работы, а бизнес-политики можно менять из одного центрального места и немедленно применять во всей организации.

Экономия пропускной способности

Подключение к интернету всегда доступно, его развёртывание происходит быстро, и расходы на него намного ниже, чем в случае эквивалентных сетей MPLS.

SD-WAN обеспечивает надёжность и безопасность сервисов глобальной сети по ценам интернета.

Архитектура, оптимизированная для «облака»

SD-WAN освобождает вас от неудобств и ограничений традиционных сетей MPLS и сочетает в себе безопасность, производительность и связь между «облаком» и офисом, благодаря чему значительно повышается комфортность работы пользователей в удалённых офисах при использовании ими приложений SaaS или «облачных» приложений.

Факторы, которые необходимо учитывать

При оценке возможности развёртывания SD-WAN сетевым администраторам и бизнес-менеджерам следует учитывать определенные факторы.

- **Внедрить SD-WAN и осуществлять её администрирование просто.** Главным преимуществом SD-WAN является лёгкость и скорость развертывания в удалённых офисах. Нет необходимости посылать ИТ-специалистов в офисы, и не нужно отдельно конфигурировать каждое устройство.
- **Опционально возможна миграция на гибридные сети.** У большинства организаций в удалённых офисах развернуты распределенные сети MPLS. Компании могут осуществлять развёртывание решений SD-WAN без изменения существующих сетей. Однако со временем они могут осуществить миграцию на менее затратные общедоступные широкополосные схемы.
- **Автоматизированное управление трафиком.** SD-WAN обеспечивает возможность приоритизации трафика и смягчения влияния перебоев в работе сети. Самое главное — предоставить сетевым администраторам интуитивно понятные инструменты для простого автоматического конфигурирования приоритетов в зависимости от нагрузки на сеть в режиме реального времени.

Затраты: SD-WAN против MPLS

С учётом осторожного предположения о том, что трафик в глобальных сетях увеличивается на 15 % в год, расходы на коммуникации вызывают серьёзное беспокойство у предприятий. Необходимо принять во внимание, что затраты на сеть MPLS схемы T1 в среднем составляют от 90 долларов США в месяц, а при увеличении пропускной способности они быстро возрастают.

Использовать SD-WAN для таких коммуникаций в три-девять раз дешевле. Помимо стандартных расходов, в случае традиционных систем MPLS установка и внесение изменений занимают в среднем 90 дней, при этом они часто предполагают обязательство заключать многолетние контракты, из-за чего этот вариант является более дорогостоящим и менее гибким.

Задача Citrix в сфере SD-WAN

Традиционные глобальные сети не были предназначены для современных потребностей в пропускной способности. С учётом этого решение для глобальной сети, реализуемое с помощью NetScaler SD-WAN компании Citrix, обеспечивает высокую масштабируемость, надёжность и адаптируемость для предприятий с распределенной инфраструктурой.

Предложение Citrix сочетает в себе сильные стороны других продуктов компании, в то же время используя «умные» технологии глобальной сети, оптимизацию глобальной сети и управление приложениями для создания уникального решения, обеспечивающего высокую комфортность работы пользователей, находящихся в удаленных офисах и в разъездах.

Это решение снижает потребность в пропускной способности для обеспечения такой комфортности работы пользователей с минимумом администрирования удаленных офисов, благодаря чему уменьшается необходимость в технической поддержке на месте. Оно также способно обеспечить это при меньших финансовых затратах благодаря значительной экономии средств на удалённую инфраструктуру коммуникаций.

Основные преимущества NetScaler SD-WAN

- Гарантированная непрерывность бизнеса и восстановление после чрезвычайных ситуаций.
- Снижение расходов на коммуникации.
- Повышенная производительность приложений для мобильных пользователей, а также пользователей в удалённых филиалах и офисах.

Чалан Арас (Chalan Aras), вице-президент и генеральный директор Citrix NetScaler SD-WAN, представляет краткий обзор решения в этом видео.

———————————————————

«NetScaler SD-WAN гарантирует эффективное использование увеличенной пропускной способности сети, снижение затрат и более высокую производительность, а также повышенную надёжность важных для бизнеса приложений».

Хуан Родригес (Juan Rodríguez), директор по развитию бизнеса, отдел сетей доставки, регион Европы, Ближнего Востока и Африки, Citrix Systems.

———————————————————

«Сочетание гибкости XenApp и XenDesktop с экономичностью и эффективностью NetScaler SD-WAN предоставляет клиентам доступ в любое время, в любом месте для их сотрудников, способствуя производительности и эффективности работы».

Кристиан Рейли (Christian Reilly), вице-президент и главный технический директор, отдел сервисов для рабочих мест, Citrix.

Интеграция для входа в систему

redhat

Microsoft

Интеграция с VPN-решениями

FORTINET

CISCO

Check Point

Интеграция с VDI-инфраструктурой

vmware

CITRIX

Microsoft

Интеграция с порталами и «облачными» сервисами

Microsoft

salesforce

Google

Интеграция с «традиционно нашим»

kraftway

TONK

КРИПТОПРО

РусБИТех

infotecs

GiS
ГАЗИНФОРМСЕРВИС

Код Безопасности

Решения Gemalto SafeNet

Решения Gemalto SafeNet в фильме «Фокус»

Решения Gemalto SafeNet

- Двухфакторная аутентификация в любое время с любого устройства в любом месте.
- Соответствие требованиям российского регулятора.
- Решения, которым доверяют во всём мире.

Как мы интегрируемся?

- Безопасный доступ к станции.
- VPN.
- VDI.
- Модули доверенной загрузки.
- Порталы и «облачные» сервисы.
- Криптотокены и ЭЦП.

СВА (eToken)

- Microsoft CryptoAPI.
- PKCS11 (+ SDK).
- APDU level (+ спецификация).

OTP (одноразовые пароли)

- Готовые агенты.
- RADIUS-протокол.
- SAML-протокол.

TESSIS

TESSIS *– официальный дистрибьютор Gemalto в России.*

www.tessis.ru

СКЗИ КриптоПро CSP 5.0

КриптоПро CSP 5.0 – это криптопровайдер нового поколения, развивающий три основные продуктовые линейки: КриптоПро CSP (работа с ключами на классических токенах и в пассивных хранилищах), КриптоПро ФКН CSP/Рутокен CSP (работа с неизвлекаемыми ключами на токенах с безопасной аутентификацией на ключи с помощью протоколов ФКН) и КриптоПро DSS (ключи в «облаке»).

Все преимущества продуктов этих линеек не только сохраняются, но и преумножаются в КриптоПро CSP 5.0: ещё шире список поддерживаемых платформ и алгоритмов, ещё выше быстродействие, удобнее пользовательский интерфейс. Но главное – работа со всеми ключевыми носителями, включая ключи в «облаке», теперь единообразна.

Для перевода прикладной системы, в которой работал КриптоПро CSP любой из версий, на поддержку ключей в «облаке» или на новые носители с неизвлекаемыми ключами не потребуется какая-либо переработка ПО – интерфейс доступа остаётся единым, и работа с ключом в «облаке» будет происходить точно таким же образом, как и с классическим ключевым носителем.

Основные решаемые задачи

- Формирование и проверка электронной подписи.
- Обеспечение конфиденциальности и контроля целостности информации посредством её шифрования и имитозащиты.
- Обеспечение аутентичности, конфиденциальности и имитозащиты соединений по протоколам TLS, EAP-TLS и IPsec.
- Контроль целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования.

Поддерживаемые алгоритмы

- Электронная подпись: ГОСТ Р 34.10-2012, ГОСТ Р 34.10-2001, ECDSA, RSA.
- Хэш-функции: ГОСТ Р 34.11-2012, ГОСТ Р 34.11-94, SHA-1, SHA-2 (224/256/384/512).
- Шифрование: ГОСТ Р 34.12-2015 (Кузнечик и Магма), ГОСТ 28147-89, AES (128/192/256), 3DES, 3DES-112, DES, RC2, RC4

Регулирующие документы

В криптопровайдере используются алгоритмы, протоколы и параметры, определённые в следующих документах российской системы стандартизации.

- Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования» (также см. RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012»).
- Р 50.1.114–2016 «Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов» (также см. RFC 7836 «Guidelines on the Cryptographic Algorithms to Accompany the Usage of Standards GOST R 34.10-2012 and GOST R 34.11-2012»).
- Р 50.1.111–2016 «Информационная технология. Криптографическая защита информации. Парольная защита ключевой информации».
- Р 50.1.115–2016 «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля» (также см. RFC 8133 The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol»).
- Методические рекомендации ТК 26 «Криптографическая защита информации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)».
- Методические рекомендации ТК 26 «Криптографическая защита информации. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS».
- Техническая спецификация ТК 26 «Криптографическая защита информации. Использование ГОСТ 28147-89, ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012 в протоколах обмена ключами IKE и ISAKMP».
- Техническая спецификация ТК 26 «Криптографическая защита информации. Использование ГОСТ 28147-89 при шифровании вложений в протоколах IPsec ESP».
- Техническая спецификация ТК 26 «Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10, ГОСТ Р 34.11 в профиле сертификата и списке отзыва сертификатов (CRL) инфраструктуры открытых ключей X.509».
- Техническая спецификация ТК 26 «Криптографическая защита информации. Расширение PKCS#11 для использования российских стандартов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012».

Поддерживаемые технологии хранения ключей

«Облачный» токен

В криптопровайдере КриптоПро CSP 5.0 впервые появилась возможность использования ключей, хранящихся в «облачном» сервисе КриптоПро DSS, через интерфейс CryptoAPI.

Теперь ключи, хранимые в «облаке», могут быть легко использованы как любыми пользовательскими приложениями, так и большинством приложений компании Microsoft. Для тестирования данного сервиса можно воспользоваться открытым сервисом DSS.

ФКН-носители с неизвлекаемыми ключами и безопасной аутентификацией

В КриптоПро CSP 5.0 была добавлена поддержка протокола выработки общего ключа с аутентификацией на основе пароля SESPAKE. Использование данного протокола позволяет защитить канал данных между криптопровайдером и токеном с неизвлекаемым ключом от активного нарушителя. Компании Актив, ИнфоКрипт, СмартПарк, Аладдин Р. Д. и Gemalto разработали новые защищённые токены, которые поддерживают данный протокол и полностью решают проблему безопасной работы с неизвлекаемыми ключами.

Ключевые носители с неизвлекаемыми ключами

Многие пользователи хотят иметь возможность работать с неизвлекаемыми ключами, но при этом не обновлять токены до уровня ФКН. Специально для них в провайдер добавлена поддержка популярных ключевых носителей Рутокен ЭЦП 2.0, JaCarta-2 ГОСТ и InfoCrypt VPN-Key-TLS. Теперь пользователи могут быть уверены, что при работе КриптоПро CSP с данными токенами закрытый ключ не будет покидать устройство.

Классические пассивные USB-токены и смарт-карты

Большинство пользователей предпочитает быстрые, дешёвые и удобные решения для хранения ключей. Как правило, предпочтение отдаётся токенам и смарт-картам без криптографических сопроцессоров. Как и в предыдущих версиях провайдера, в КриптоПро CSP 5.0 сохранена поддержка всех совместимых носителей производства компаний Актив, Аладдин Р. Д., Gemalto/SafeNet, Multisoft, NovaCard, Rosan, Alioth, MorphoKST и СмартПарк.

Кроме того, конечно, как и раньше, поддерживаются способы хранения ключей в реестре Windows, на жёстком диске, на флэш-накопителях на всех платформах.

Поддерживаемое программное обеспечение

КриптоПро CSP позволяет быстро и безопасно использовать российские криптографические алгоритмы в следующих стандартных приложениях:

- офисный пакет Microsoft Office;
- почтовый сервер Microsoft Exchange и клиент Microsoft Outlook;
- продукты Adobe Systems Inc.;
- браузеры Яндекс.Браузер, Спутник, Internet Explorer, Edge;
- средство формирования и проверки подписи приложений Microsoft Authenticode;
- веб-серверы Microsoft IIS, nginx, Apache, Tomcat;
- средства удалённого администрирования Microsoft Terminal Server и Citrix;
- Microsoft Active Directory.

Интеграция с платформой КриптоПро

С первого же релиза обеспечивается поддержка и совместимость со всеми нашими продуктами:

- КриптоПро УЦ;
- Службы УЦ;
- КриптоПро ЭЦП;
- КриптоПро IPsec;
- КриптоПро EFS;
- КриптоПро .NET;
- КриптоПро JCSP.

Совместимость с технологией ФКН, реализованной в продуктах КриптоПро Рутокен CSP, КриптоПро ФКН CSP 3.9, отсутствует.

Интерфейсы для встраивания

Для встраивания в приложения на всех платформах КриптоПро CSP доступен через стандартные интерфейсы для криптографических средств:

- Microsoft CryptoAPI;
- PKCS#11;
- OpenSSL (в виде engine);
- Qt SSL.

Производительность на любой вкус

Огромный опыт разработки позволяет нам охватить все решения от миниатюрных ARM-плат, таких как Raspberry Pi, до многопроцессорных серверов на базе Intel Xeon, AMD EPYC и PowerPC, отлично масштабируя производительность.

КРИПТОПРО

«КриптоПро» – разработка средств криптографической защиты информации.

info@cryptopro.ru
www.cryptopro.ru

Легко и просто

КриптоПро ЭЦП Browser plug-in легко встраивается и применим в любом из современных браузеров с поддержкой сценариев JavaScript.

Что можно подписывать?

- электронный документ;
- данные веб-формы;
- файл, загруженный с компьютера пользователя;
- текстовое сообщение и т. п.

Где использовать?

С точки зрения бизнес-функций, плагин позволяет использовать ЭП:

- на клиентских порталах;
- в системах интернет-банкинга;
- в электронных офисах.

Создание и проверка ЭП

КриптоПро ЭЦП Browser plug-in позволяет создавать и проверять как обычную электронную подпись, так и усовершенствованную электронную подпись. Поскольку плагин является частью стандарта применения усовершенствованной электронной цифровой подписи, автоматически решаются задачи:

- доказательство момента подписи документа и действительности сертификата ключа подписи на этот момент;
- отсутствие необходимости сетевых (онлайн) обращений при проверке подписи;
- архивное хранение электронных документов.

Создание и проверка подписи происходят на стороне пользователя. При создании подписи с помощью КриптоПро ЭЦП Browser plug-in электронная подпись может быть либо добавлена к подписываемым данным (присоединённая ЭП), либо создана отдельно (отделённая ЭП).

КРИПТОПРО

«КриптоПро» – разработка средств криптографической защиты информации.

info@cryptopro.ru
www.cryptopro.ru

КриптоПро CSP 5.0: «Облачный» провайдер

Криптопровайдер КриптоПро CSP 5.0 обладает довольно широкой функциональностью, поэтому мы решили выпустить статью-инструкцию, которая покажет, как можно протестировать наиболее существенные нововведения.

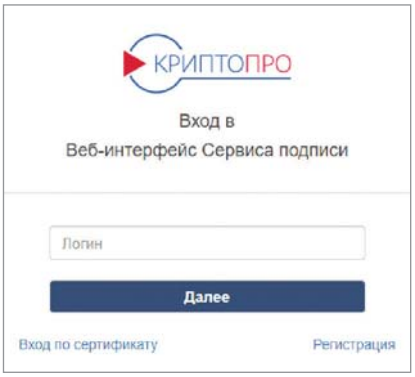


Рисунок 1

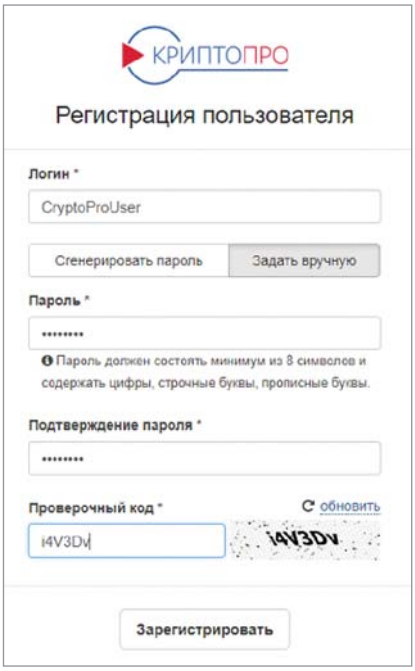


Рисунок 2

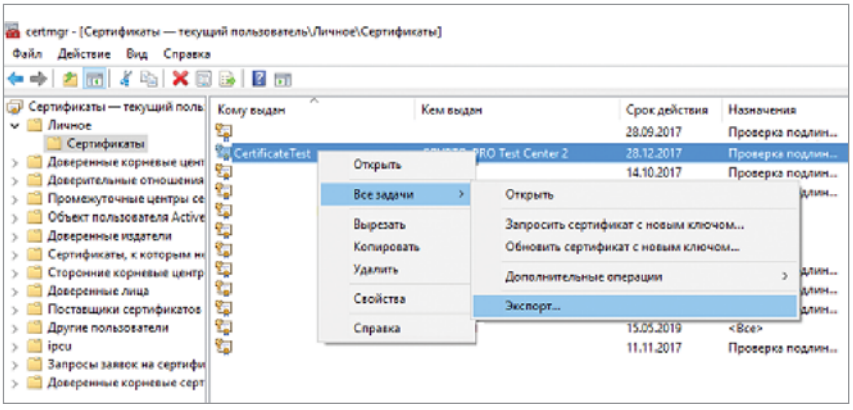


Рисунок 3

Начнём с самой крупной иннова-ции — работы с «облачными» токенами: удалёнными хранилищами неизвлекаемых ключей. В качестве непосредственного хранилища ключей выступает защищённый сервер КриптоПро HSM, к которому подключён сервер удалённой подписи КриптоПро DSS. Использование КриптоПро CSP 5.0 позволяет получить доступ к ключам HSM через использование стандартного интерфейса CryptoAPI.

Данная инструкция покажет, как за пару кликов научить CSP видеть ваши ключи. В качестве примера мы будем пользоваться тестовым сервером dss.cryptopro.ru. Заранее заметим, что данный тестовый сервис поддерживает только ключи алгоритма ГОСТ Р 34.10-2001.

Создание тестового пользователя

Первым делом заведём пользователя на тестовом сервере. Для этого зайдём в его веб-интерфейс и нажмём кнопку Регистрация (рис. 1).

Заполним форму регистрации и подтвердим создание пользователя (рис. 2).

После регистрации мы попадаем на основной экран пользователя, где перечислены сертификаты, соответствующие хранящимся на сервере закрытым ключам. У нового пользователя, разумеется, сертификатов нет. Есть два пути, как их добавить: скопировать существующий контейнер и создать новый. Рассмотрим оба.

Копирование пользовательского контейнера

Прежде всего, у вас должен быть ключевой контейнер формата КриптоПро, а сертификат для него должен быть установлен в системное хранилище. Если сертификата нет, его можно выпустить на нашем тестовом сервисе (открывать через Internet Explorer). При генерации не забудьте пометить ключ как экспортируемый.

Для переноса ключа открываем системное хранилище сертификатов (Win+R > certmgr.msc > **OK**), выбираем сертификат, нажимаем правой кнопкой >**Все задачи** > **Экспорт** (рис. 3).

В мастере экспорта сертификатов указываем, что хотим экспортировать сертификат с закрытым ключом и выполняем экспорт в формат PFX, установив произвольный пароль.

Возвращаемся на экран управления DSS и нажимаем кнопку **Установить сертификат** (рис. 4).

Здесь выбираем экспортированный PFX-контейнер и нажимаем кнопку **Загрузить сертификат**. В результате в списке сертификатов должен появиться ваш скопированный сертификат, который можно просмотреть.

Создание запроса через DSS

Второй путь получения сертификата — это создание запроса на удовтоверяющий центр (УЦ), который непосредственно подключён к DSS.

Нажимаем **Создать запрос** на сертификат, вводим данные (обязательно только поле CN) и создаём запрос. Во всплывающем окне PIN-код можно оставить пустым (рис. 5).

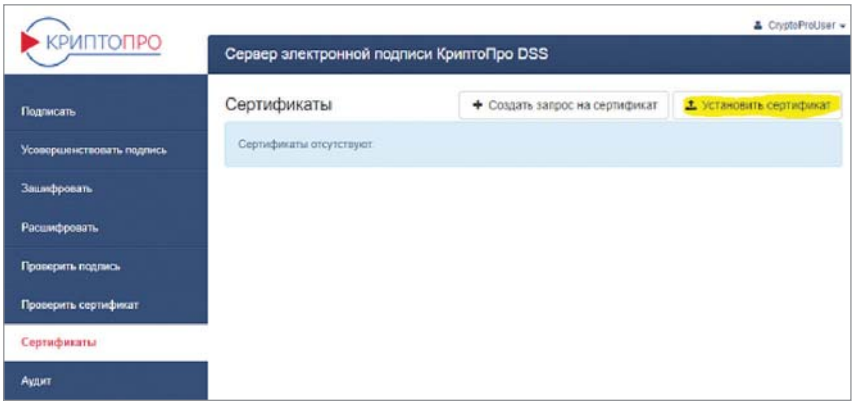


Рисунок 4

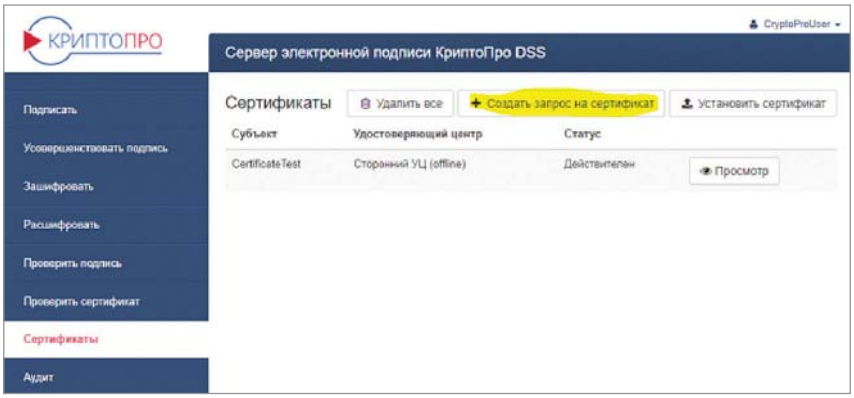


Рисунок 5

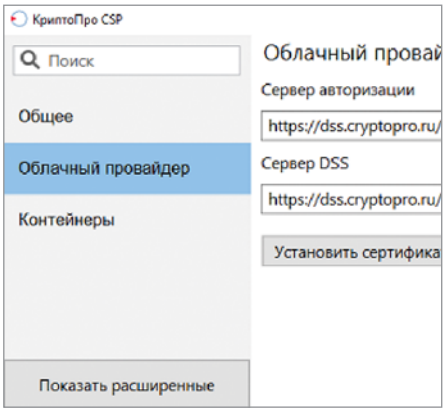


Рисунок 6

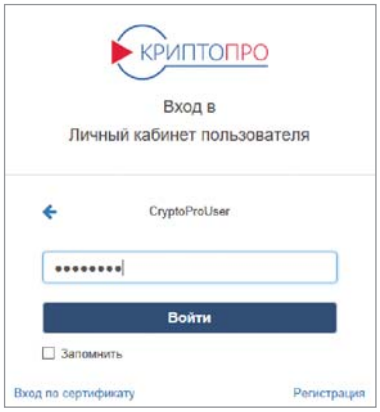


Рисунок 7

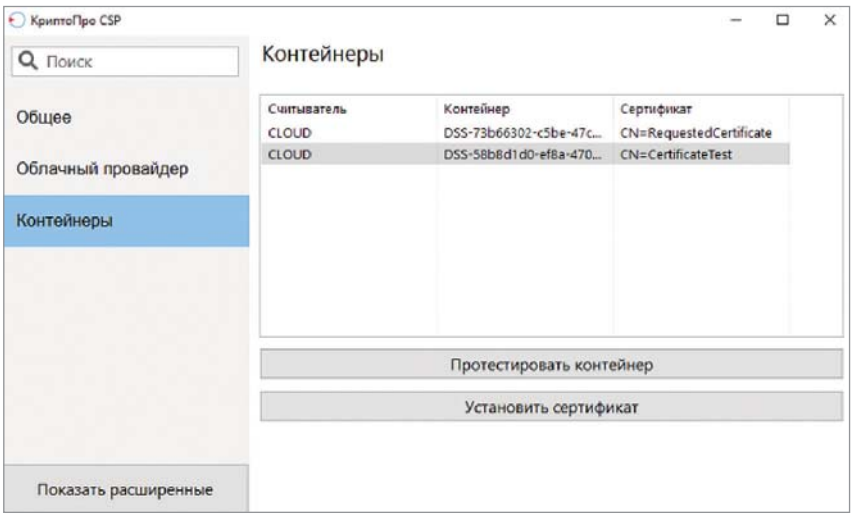


Рисунок 8

Выпущенный сертификат сразу попадает в список и также доступен для просмотра.

Подключение к CSP

Через эту же веб-форму можно напрямую подписывать и зашифровывать документы, проверять данные и т. д., но если вам нужно использовать ключи во внешних приложениях, нужно зарегистрировать эти сертификаты в CSP. Самый простой способ — воспользоваться утилитой CryptoPro Tools (Инструменты КриптоПро), входящей в состав КриптоПро CSP 5.0.

Запускаем её из меню **Пуск** и выбираем пункт **Облачный провайдер** (рис. 6).

В появившемся окне вбиваем адреса используемых сервисов авторизации и доступа к DSS. Для тестового сервиса пользуемся адресами по умолчанию.

Нажимаем кнопку **Установить сертификаты**. Если вы правильно указали адреса, должно появиться браузерное окно аутентификации на DSS. Вводим учётные данные, указанные при регистрации (рис. 7).

В процессе установки сертификатов с сервера будут скачаны и установлены цепочки сертификатов, что может приводить к окнам с предупреждениями.

Если всё настроено корректно, приложение сообщит об успешной установке сертификатов и их можно будет просмотреть на вкладке **Контейнеры** или в любом приложении, использующем CryptoAPI (рис. 8).

Теперь данные контейнеры можно использовать в любых приложениях. Если, например, установленный сертификат является квалифицированным, то с его помощью можно подключиться к сайту gosuslugi.ru или nalog.ru.

CIS / № 1 (3) / 2018 / www.cismag.ru

«Облачный» токен

Продукты компании КриптоПро включают поддержку всех современных платформ, имеют версии для мобильных устройств, интегрированы с ведущими российскими и зарубежными ИТ-решениями, широко используются органами власти и коммерческими организациями всех отраслей.

Они применяются в системах электронного документооборота, исполнения госзаказа, сдачи бухгалтерской и налоговой отчётности и т. п.

Средства электронной подписи КриптоПро CSP/JCP установлены более чем на 10 000 000 серверах, рабочих местах и мобильных устройствах пользователей.

Разработанные компанией КриптоПро средства обеспечения деятельности удостоверяющих центров внедрены более чем в 1000 организациях; в том числе и в составе Головного удостоверяющего центра Минкомсвязи России.

Наивысшая степень защиты ключей от компрометации

Ключи пользователей создаются и хранятся в защищённом криптографическом модуле HSM, оставаясь неизвлекаемыми. HSM снабжён датчиками вскрытия, контролем портов, механизмами доверенной генерации и уничтожения ключей, защитой от утечек по побочным каналам – и это далеко не всё. Ключи надёжно защищены даже от внутреннего нарушителя, являющегося администратором.

Схемы аутентификации пользователей имеют уровень безопасности не ниже, чем у самих хранимых ключей. Ключи становятся не просто неизвлекаемыми, но и некомпрометируемыми.

Подлинная мобильность подписи

Забудьте про связку из токенов, USB-концентраторы и установку драйверов. Вы больше не будете привязаны к одному рабочему месту – к вашему ключу в «облаке» вы можете получить доступ из любого места и с любого устройства: с настольного компьютера, ноутбука, планшета, смартфона и простого «телефона-звонилки» даже без интернета.

Не отчаивайтесь, если в день торгов вы забыли ключевой носитель дома – альтернативный способ аутентификации к «облачному» токену позволит даже в таких ситуациях всё подписать в срок.

Установка средств электронной подписи не требуется

На рабочее место пользователя, которым может быть и мобильное устройство, нужно установить лишь простое в использовании легковесное средство аутентификации.

Работу по настройке всех криптографических механизмов и форматов, а также по управлению ключами возьмут на себя наши серверные компоненты.

Отсутствие средств электронной подписи на рабочем месте позволяет обеспечить централизованное управление ключами пользователей в корпоративной сети.

Производительность, надёжность и отказоустойчивость

Вычисление электронной подписи на «облачном» токене происходит со скоростью, сравнимой со скоростью работы «фермы» из тысяч USB-токенов.

Простым увеличением аппаратных ресурсов можно масштабировать производительность до любого необходимого уровня. В отличие от физического, «облачный» токен никогда не сломается, не утонет в кофе и не потеряется.

Вы наконец-то можете забыть о страхе в критический момент оказаться один на один с отказавшим устройством, у которого попросту исчерпан ресурс. Аппаратное резервирование серверных компонентов позволит пережить любой сбой незаметно для пользователей.

Сохранение инвестиций

Вам не придётся менять или дорабатывать систему документооборота. Не нужно отказываться от привычного ПО для работы с электронной подписью.

Всё, что умеет работать со стандартом де-факто российского рынка средств ЭП – КриптоПро CSP, при установке «облачного» криптопровайдера бесшовно сможет использовать «облачные» токены. Не спешите выбрасывать и аппаратные токены – они смогут послужить в качестве средств аутентификации к ключам пользователей в «облаке». Для перехода на алгоритм ГОСТ Р 34.10-2012 не нужно покупать ни новые токены, ни новое ПО – переход не потребует дополнительных вложений (в рамках расширенной технической поддержки).

Снижение стоимости владения

По сравнению с локальными средствами ЭП, аппаратными токенами и смарт-картами, при использовании «облачных» токенов существенно упрощаются процедуры передачи СКЗИ пользователям и установки средств ЭП на рабочие места.

Централизованное хранение ключей с аппаратным резервированием, высокая производительность и возможность обслуживания множества пользователей одним сервером значительно уменьшают стоимость владения данным решением.

Первое сертифицированное средство «облачной» подписи

Сервер электронной подписи КриптоПро DSS является первым и единственным (на 1 августа 2017 г) сертифицированным ФСБ Росси и «облачным» средством электронной подписи. Идёт процесс сертификации исполнений с новыми способами аутентификации и «облачным» криптопровайдером.

Первые в России

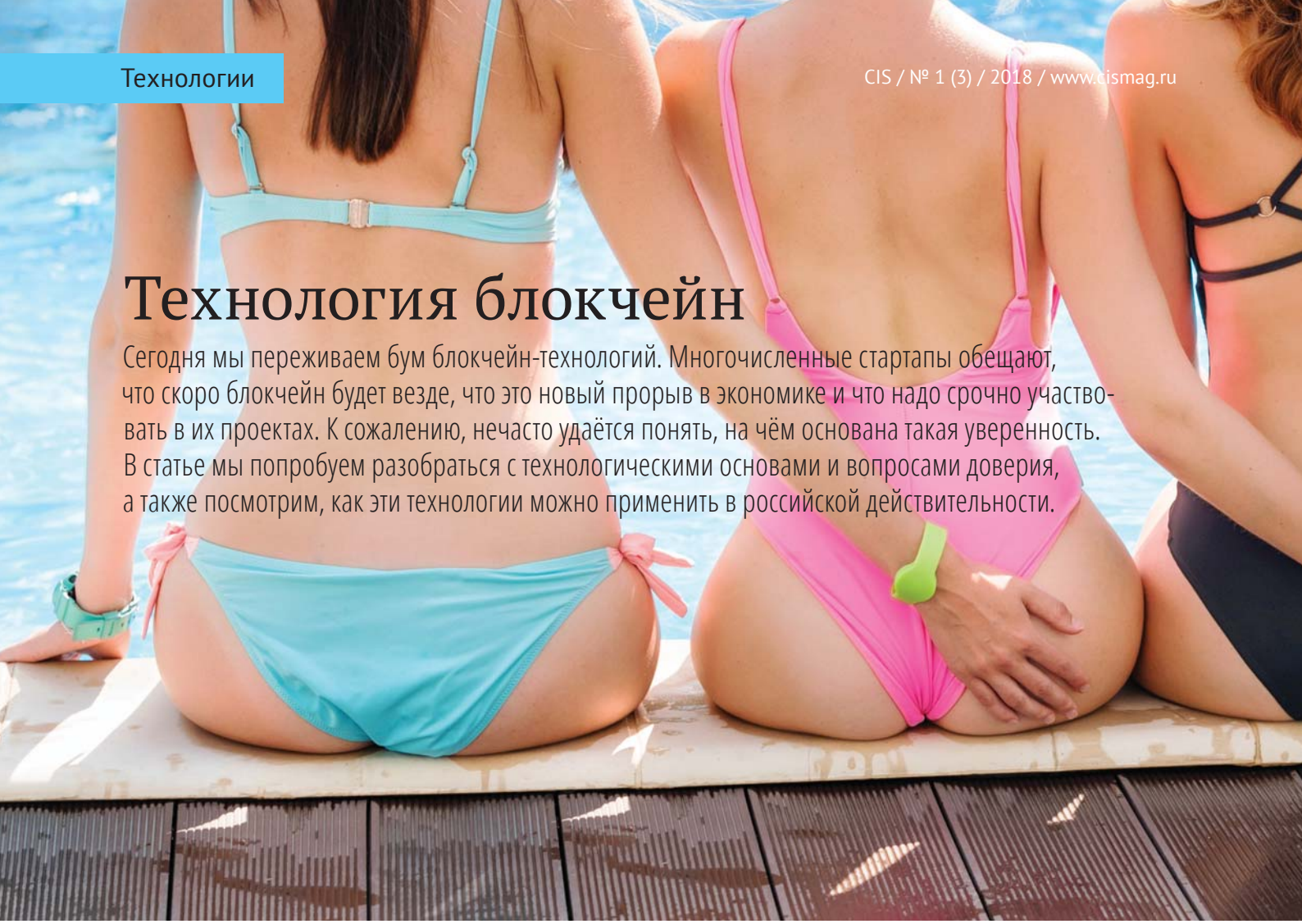
- Первое в России сертифицированное СКЗИ, интегрированное с ОС Microsoft Windows - КриптоПро CSP.
- Первое в России сертифицированное средство обеспечения деятельности удостоверяющих центров КриптоПро УЦ.
- Первые в России сертифицированные службы актуальных статусов сертификатов и меток времени – КриптоПро OCSP и КриптоПро TSP.
- Первые в России сертифицированные аппаратные криптографические модули – Атликс HSM и КриптоПро HSM.
- Первые в истории сообщества интернет стандарты , описывающие применение российских криптоалгоритмов – RFC 4357: RFC 4490, RFC 4491, RFC 7836, RFC 8133.
- Первые стандартизированные параметры эллиптических кривых для российских алгоритмов электронной подписи, а также сопутствующие криптографические алгоритмы (HMAC, KDF, PRF, VKOI для российского стандарта функции хэширования.
- Первый в России стандартизированный протокол для защиты взаимодействия с ключевыми носителями (SESPAKE) и реализующие его СКЗИ.
- Первые утверждённые методические рекомендации по применению российских криптографических алгоритмов в протоколах TLS, IPsec, CMS.
- Первое в России сертифицированное СКЗИ, разработанное в соответствии со спецификацией JCA Java Cryptography Architecturel – Криптоpo JCP.
- Первое в России «облачное» решение, получившее подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом «Об электронной подписи» для централизованного применения (создания и проверки) электронной подписи, создания и хранения пользовательских ключей электронной подписи, – КриптоПро DSS.

КРИПТОПРО

«КриптоПро» *– разработка средств криптографической защиты информации.*

info@cryptopro.ru
www.cryptopro.ru

CIS / № 1 (3) / 2018 / www.cismag.ru



Технология блокчейн

Сегодня мы переживаем бум блокчейн-технологий. Многочисленные стартапы обещают, что скоро блокчейн будет везде, что это новый прорыв в экономике и что надо срочно участвовать в их проектах. К сожалению, нечасто удаётся понять, на чём основана такая уверенность. В статье мы попробуем разобраться с технологическими основами и вопросами доверия, а также посмотрим, как эти технологии можно применить в российской действительности.

Основы

Базовой технологией является связанный список файлов или иных кусков данных, в котором связи между элементами списка создаются с использованием криптографии. Элементы такого списка как раз и называются блоками, отсюда и название блокчейн или в переводе с английского – цепочка блоков.

Целью построения таких списков является желание защитить от изменений блоки в середине цепочки. Из-за того, что при построении списка применяется криптография, любые изменения в блоках приводят к тому, что цепочка не проходит проверку на целостность. Отсюда возник термин – неизменяемый реестр; все старые записи такого реестра можно подвергнуть проверке и определить, были внесены изменения или нет. Также можно употреблять термин «блокчейн-реестр» вместо «неизменяемый реестр».

Вследствие неизменности такой реестр можно скопировать на любое число узлов и быть при этом уверенным, что владельцы этих узлов не смогут менять имеющиеся записи реестра; более того, реестр может распространяться по принципу peer-to-peer, так как нет разницы, от кого получать куски реестра, если есть способ проверки целостности всего реестра.

Важным свойством реестра является возможность добавления в него новых записей, причём все эти записи будут выстроены в порядке их поступления. Новые записи могут быть добавлены только в начало реестра, вставить запись где-то в середине списка невозможно. По мере добавления формируются новые криптографические связи, что даёт дополнительную защиту старым блокам реестра, а также позволяет доказать очерёдность поступления записей.

Криптографические связи между блоками можно создавать различными способами. За счёт этого помимо неизменяемости реестра можно получать различные эффекты, которые могут быть важны для выбранного применения реестра. Далее будут рассмотрены варианты реестров, основанные на хэшировании и электронной подписи с асимметричными ключами.

Реестр на функции хэширования

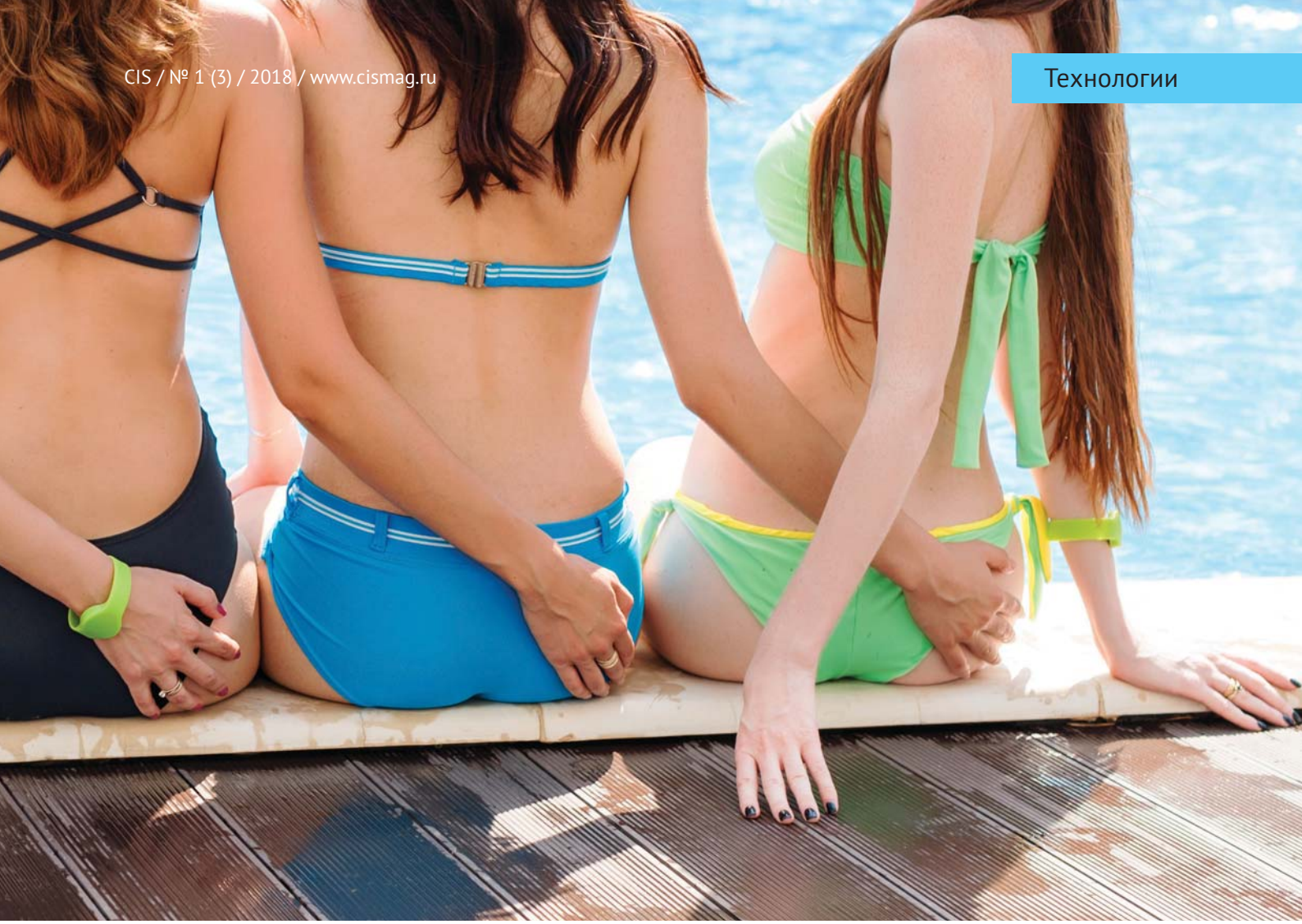
Первый вариант построения реестров – с использованием функций хэширования. Пусть после применения функции к порции данных получается значение, которое называется хэш (hash). Будем считать, что хэш обладает двумя важными свойствами: а) по хэшу нельзя восстановить исходные данные; б) при любом изменении исходных данных функция выдаст совершенно другое значение хэша.

С применением функций хэширования связи между элементами цепочки делаются следующим образом.

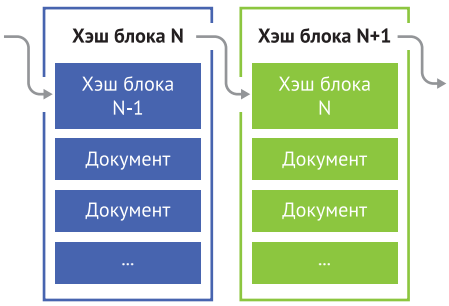
1. Из реестра извлекается последний добавленный блок, и рассчитывается его хэш. Получаем хэш последнего блока.

2. Хэш последнего блока объединяется с новыми добавляемыми данными. Получаем новый блок.

3. Новый блок добавляется в реестр и становится последним добавленным блоком.



Визуально такая цепочка блоков выглядит следующим образом.



Предположим теперь, что во время хранения данные одного из блоков были повреждены или заменены. В этом случае перерасчёт хэша блока покажет несовпадение хэшей, так как у повреждённого блока будет другой хэш.

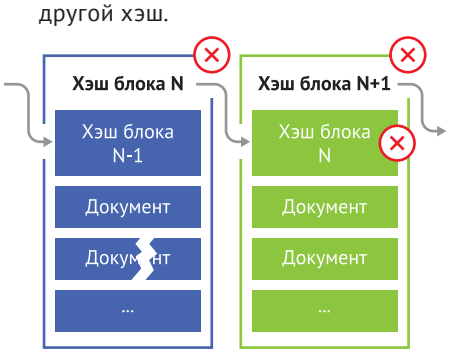
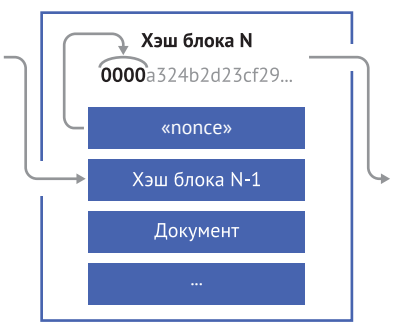


Схема имеет недостаток – злоумышленник может изменить данные одного из блоков, быстро пересчитать все хэши до последнего блока и сделать замену в реестре, перезаписав файлы с содержимым блоков. Чтобы затруднить эту задачу, можно использовать метод, называемый «proof of work». Суть его состоит в том, чтобы затруднить пересоздание блоков, но оставить простоту и скорость проверки. Для этого к данным добавляют число, называемое «nonce», после чего начинают менять это число, добиваясь, чтобы получающийся хэш начинался с нулевых битов. Известно, что чем больше нулевых битов в начале хэша, тем большее количество значений nonce нужно перебрать. Получаемая структура данных блока имеет теперь следующий вид.



Проверка такой структуры производится так же быстро, но подменить данные и пересчитать все блоки до текущего теперь гораздо сложнее.

Для этого нужно потратить примерно столько же ресурсов, сколько уже было затрачено на подбор nonce для изменяемых блоков. Если блоки для цепочки генерируются непрерывно и nonce подбирается для большого количества нулей в начале хэша, то задача подмены цепочки становится очень сложной для отдельно взятого злоумышленника.

Именно по такому принципу работают криптовалюты типа биткойна: данными блока являются записи о переводах расчётных единиц между пользователями, а генерация nonce для новых блоков называется майнингом.

Доверие к такому реестру возникает из-за уверенности, что пересчёт nonce и генерация новых блоков будут происходить быстрее, чем это делает злоумышленник. Это утверждение скорей всего верно для больших распределенных сетей, где участники сети заинтересованы в не-

зависимой генерации новых блоков. Но для защиты данных в приватных сетях такой блокчейн-реестр подходит плохо по следующим причинам.

- Нужно тратить ресурсы на постоянный подбор nonce для генерации блоков, что выливается в потребление электричества, за которое надо немало платить.
- Неизвестно, какие мощности есть у злоумышленников для пересчёта цепочки, нужно всё время наращивать мощность генерации блоков.

Чтобы этого избежать, был придуман второй способ защищать реестр.

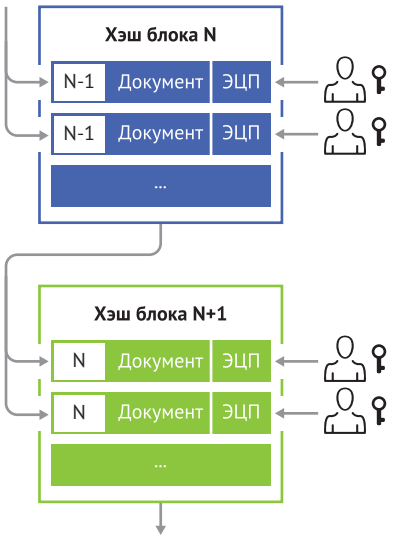
Реестр на электронной подписи

Второй вариант формирования связей между блоками предполагает использование не только хэшей блоков, но и электронноой цифровой подписи (ЭЦП) пользователей. ЭЦП формируется с использованием закрытого ключа асимметричной ключевой пары пользователя, а проверяется – открытым ключом этой пары. После расчёта ЭЦП данные нельзя изменить без знания закрытого ключа.

С использованием ЭЦП формирование связей между блоками выглядит следующим образом.

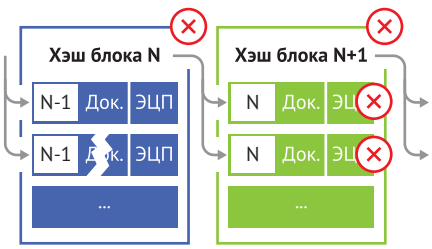
1. Из реестра извлекается последний добавленный блок и рассчитывается его хэш. Получаем хэш последнего блока.
2. Хэш последнего блока объединяется с информацией, которая должна быть подписана пользователем. После этого пользователь использует свою ключевую пару и подписывает эти данные. Получаем пользовательский документ.
3. Свежеподписанный документ объединяется с другими подобными документами и образует данные блока. Получаем новый блок.
4. Новый блок добавляется в реестр и становится последним добавленным блоком.

Получаемая структура данных представлена на рисунке.



На рисунке ниже показано, что документ подписываемый пользователем, содержит блок текста, блок машиночитаемых атрибутов, а также хэш последнего блока. Такая структура делает документ пригодным как для чтения человеком, так и для автоматической обработки в информационных системах.

Попытка подмены какого-либо документа в блоке из середины цепочки приводит к изменению хэша блока и требует пересчёта всех ЭЦП документов, входящих в последующие блоки. Без знания закрытых ключей задача пересчёта цифровой подписи путем подбора ключей считается нерешаемой – в силу того, что пользователи заинтересованы хранить закрытые ключи в тайне, то собрать их все и переподписать документы практически нереально. На рисунке ниже показано, где будут возникать ошибки проверки при повреждении документа в блоке.



Именно за счёт этого обстоятельства и возникает доверие к данному варианту реестра. В отличие от предыдущего варианта, для защиты реестра можно не тратить ресурсы на расчёт nonce, также генерацию новых блоков можно делать по мере необходимости. Ресурсы нужно тратить только на хранение реестра, но хранение данных необходимо в обоих вариантах реестра. Для проверки цепочки блоков в реестре дополнительно нужно хранить открытые ключи пользователей и чем больше пользователей будет участвовать в системе и подписывать своими ключами данные с хэшем последнего блока, тем надёжнее будет защищён блокчейн-реестр.

Такой вид блокчейна уже можно применять для защиты данных в приватных и корпоративных сетях. Для этого нужно найти документы, которые требуется защитить от внесения правок, после чего организовать их добавление в блоки реестра по описанной выше схеме.

Например, в системах документооборота через блокчейн-реестр можно проводить вообще все документы; в бухгалтерском учёте в реестр можно поместить первичные документы – договора, счета, чеки, накладные и акты. После этого реестр можно использовать для контроля и аудита. Становится возможным проверять целостность архива документов; можно проверять соответствие бизнес-процессов и порядка возникновения документов в блокчейне.

Законы и блокчейн

Как видно из предыдущих разделов, для построения реестров вполне достаточно операций хэширования и электронно-цифровой подписи. К счастью, в нашей стране на уровне стандартов и законов эти операции вполне доступны. Основным законом на эту тему является № 63-ФЗ «Об электронной подписи», согласно которому ЭЦП может быть приравнена к собственноручной подписи. Это означает, что мы можем положить в блокчейн-реестр электронные документы, которые будут приниматься судами Российской Федерации при разрешении спорных ситуаций. Такие документы будем называть юридически значимыми.

Именно это обстоятельство должно являться определяющим при анализе на полезность существующих публичных блокчейн-проектов и создании новых: как именно документы из блокчейна будут применяться при разрешении споров, в идеале в судах. Существующие системы в виде криптовалют таких документов не предоставляют в принципе: всё, что есть внутри их реестров, – это записи о передаче неких расчётных единиц между открытыми ключами пользователей.

Следует отметить, что любой блокчейн-реестр целиком на данный момент бесполезен с юридической точки зрения, так как нет законов, которые позволяют устанавливать правовые последствия присутствия документа в реестре.

Например, законом можно установить, что документ должен находиться в реестре, иначе документ не будет считаться юридически значимым. Далее, можно принять закон, который позволяет устанавливать очерёдность появления документов в реестре без использования меток времени. Даже если метки времени будут присутствовать в подписанных документах, порядок документов в реестре можно сделать более приоритетным, чем метка времени. Но даже несмотря на отсутствие таких законов можно строить информационные системы, опираясь только на существующие законы об ЭЦП.

Практический блокчейн

В целях демонстрации обрисуем концепт блокчейна, имеющий практическое применение. Понятное дело, что такой блокчейн должен быть P2P и потенциально как можно более массовым, приносить несомненную пользу своим участникам, не требовать много ресурсов на свое поддержание и быть юридически значимым. Последнее условие легче всего выполнить, обратившись к Гражданскому кодексу и выбрав оттуда подходящий вид взаимоотношений.

Итак, пусть гражданин решает взять у кого-то денег в долг. Эта ситуация в РФ регулируется в Гражданском кодексе в главе 42, статьях 807-823. Из этих статей следует:

- берущий в долг выдает расписку;
- дающий в долг имеет право на проценты;
- всё это может происходить между физлицами и никаких посредников не нужно.

Также эти долговые расписки можно перепродавать третьим лицам, на это указывает глава 24 ГК, статьи 382-392. По сути, на пустом месте можно наплодить долговых расписок, которыми можно торговать и делать прочие вещи, предусмотренные в кодексе.

Теперь пусть происходит следующее: берущий в долг подписывает с использованием ЭЦП файл с договором займа, аналогичный расписке. При правильном оформлении такой документ будет равноценен долговой расписке и от него нельзя так просто отказаться, заявив например, что расписка подделана. Суд такой документ должен принять, так как есть закон об ЭП, где она приравнивается к обычной подписи.

Долговая расписка в электронной форме – отличный документ для включения в блок. Смысл расписки предельно прост и понятен всем участникам процесса, как следствие, расписку можно сделать машиночитаемой, выделив поля для сумм долга, процентов и даты погашения.

Распиской можно торговать при надлежащем документальном оформлении, что открывает широкие бизнес-возможности. В случае форс-мажоров можно решать споры в правовом поле, копируя документы с ЭЦП из блокчейна и подавая иски в суд. Электронный вид долговой расписки значительно упрощает судебный процесс, так как не требуется экспертиза почерка. Так как в расписке используется ЭЦП, то при её формировании можно использовать вариант реестра, не требующий майнинга.

Расписка в электронной форме внутри блокчейна может быть выглядеть следующим образом.

На картинке показан документ для второго варианта блокчейна, где связь между блоками возникает за счёт ЭЦП.

Также никто не мешает использовать первый вариант – суть долговой расписки и её юридическая сила от этого никак не изменятся. Это означает, что реализовать концепцию можно на базе любой существующей криптовалюты, если в распределенный реестр этой криптовалюты можно поместить произвольный документ. После уточнения форматов документов и написания клиентского приложения можно получить сеть, которая хранит на своих узлах копии блокчейн-реестра долговых расписок.

Доверие к содержимому реестра основывается на цифровой подписи с использованием асимметричных ключей. Этот реестр не может быть изменён узлами, иначе копия реестра не будет проходить проверку: пользователи узлов могут быть уверены, что они обладают корректной копией реестра.

Каждый отдельный документ внутри блокчейна также не может быть изменён, так как для этого надо обладать закрытыми ключами пользователей. Как результат – можно верить документам из блокчейна и использовать их в собственных целях.

Клиентское приложение должно предоставлять основные операции, позволяющие пользователям взаимодействовать со своими долгами в реестре. Это формирование документа с распиской; отправка документов в распределённый реестр и извлечение из него копии документов для судебных споров; также оно должно следить за появлением новых расписок в распределённом реестре и выкачивать обновления с других узлов.

Дополнительно клиентское приложение должно уметь формировать пакеты документов, оформляющих погашение долгов. Это может быть банковская выписка или расписка в получении денег в электронной форме. Также для погашения долга должна быть возможность передать другую долговую расписку, по которой заимодавец сможет получить долг с третьего лица.

Основной смысл реестра в том, что он будет вытаскивать на белый свет все долговые обязательства P2P. На базе этого факта можно строить различные приложения, использующие реестр.

Применение блокчейна

Как видно из предыдущих разделов, совершенно не затронуты вопросы так называемой экономики блокчейна. Намеренно не затрагивались вопросы майнинга/вознаграждения участников, распределения реестра по узлам, генерации новых блоков и тому подобных вещей, которые требуют от участников сети тратить ресурсы на поддержание сети распределенного реестра. Вместо этого приведем несколько примеров, как можно использовать содержимое реестра долгов.

Очевидная задача – нужно обеспечить участников сети средством для поиска партнёра по сделкам. Фактически, это будет сайт-биржа, на котором займодавцы смогут выставлять предложения по выдаче средств в долг, а потенциальные заёмщики – запросы на получение средств.

Смысл биржи может быть в том, что она за комиссию обеспечивает посредничество в вопросе передачи средств в обмен на долговую расписку. Стороны сделки могут быть уверены, что получат желаемое (займодавец – комплект документов с ЭЦП заёмщика, заёмщик – денежные средства). Биржа должна уметь формировать пакет юридически значимых документов, по которым оформляется долговое обязательство.

Во время работы блокчейна может сложиться ситуация, когда участник набирает в долг существенную сумму средств, причём под не очень большие проценты. Используя блокчейн, он вполне может все эти средства (свои и заёмные) выдать в долг под гораздо более высокий процент.

Фактически, тем самым моделируется работа банка, который за счёт депозитов вкладчиков выдаёт кредиты и на этом живёт.

Если предположить, что есть способ выбрать добросовестных участников, возвращающих долги с процентами вовремя, то это может являться основой для рынка перепродажи долга. Когда займодавцу вдруг срочно понадобятся деньги, он может выставить долг на продажу с некоторым дисконтом – покупатель такого долга может рассчитывать на прибыль за счёт получения процентов, которые недополучил основной займодавец.

Аналоги такой деятельности известны – это рынок векселей и облигаций. Технически это может быть сайт, аналогичный бирже, но который оформляет договора цессии (передачи долга) в электронной форме.

К сожалению, в реальной жизни не все долги возвращаются. В таком случае долг с большим дисконтом может купить лицо, профессионально занимающееся возвратом долгов. Это коллекторский рынок – просроченные долги передаются тем лицам, которые имеют возможности для взыскания долга.

Не секрет, что кредиты и депозиты играют важную роль в финансовой жизни бизнесов. Финансовые директора и бухгалтеры наверняка могут многое рассказать о применении кредитов и депозитов в бизнесе, но в рамках статьи можно лишь сказать, что в блокчейне долгов кредиты и депозиты создаются элементарно. Вместо упоминания и разбора различных финансовых схем рассмотрим более глобальный пример.

Пусть некто публикует в блокчейне долговые расписки, по которым можно получить ноль процентов и которые не имеют сроков погашения. Казалось бы, абсолютно бесполезная вещь. Но представим себе, что Казначейство РФ, Федеральная налоговая служба РФ и прочие органы госвласти внезапно заявляют, что эти странные долговые расписки будут приниматься в уплату налогов и сборов по номиналу. Если этим загадочным некто является Центробанк РФ, то ситуация становится вполне логичной: такая электронная долговая расписка является примерным аналогом рублёвой банкноты.

Банк России (или Центробанк РФ)

Долговая расписка 1 000 рублей

=

В предыдущем разделе было сказано, что долги можно гасить другими долговыми расписками, и в данной ситуации такая техническая возможность будет очень кстати: погашать долги между участниками сети можно будет долговыми расписками Центробанка. Фактически, получается пресловутый крипторубль, которым можно платить налоги и сборы, использовать в финансовых операциях и все это практически в рамках действующего законодательства и технических средств.

Подводя итоги

В статье было показано, за счёт чего возникает неизменяемость реестра и отчего можно верить своей локальной копии. Далее было рассказано о юридической значимости, и в каких частях блокчейна её можно получить. После этого на основе Гражданского кодекса РФ были выбраны отношения и описывающие их документы, которые можно положить в блокчейн. И наконец, было рассказано, что можно делать с блокчейном, содержащим эти самые документы.

За рамками статьи были оставлены вопросы приватности документов в блокчейне и транзакций между участниками. Также не рассматривались вопросы P2P-обмена, генерации блоков и вознаграждения участников сети за трату ресурсов на поддержание сети.

Ваши вопросы по применению блокчейн-технологий в существующих системах и предложения по участию в разработке новых систем вы можете адресовать нам.

Криптопровайдер будущего: прозрачный переход на неизвлекаемые ключи

Задача безопасного хранения и использования криптографических ключей является одной из наиболее важных для защиты информации.

Основная цель

Обеспечение максимальной безопасности аутентификации: ключевой носитель должен быть стойким по отношению к активному противнику в канале связи токен-машина.

Основное дополнение к стандартным требованиям

Активный противник в канале не должен иметь возможность получить критерий для бесконтрольного угадывания пароля (так называемого «offiine-перебора»).

Протокол SESPAKE

Росстандарт: Р 50.1.115-2016 «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля».

Smyshlyaev S.V. et al, RFC 8133, The Security Evaluated Standardized Password-Authenticated Key Exchange (SESPAKE) Protocol.

Итого

Четыре способа хранения ключей, отличающиеся аспектами защищённости, быстродействия, надёжности и стоимости:

- пассивное хранилище;
- активный токен;
- активный токен с безопасной аутентификацией (ФКН);
- хранение и работа с ключами в «облаке».

Задачи заказчика/интегратора/разработчика прикладной системы

- Проблема выбора способа хранения ключей.
- Проблема изменений в существующих системах.
- Проблема построения системы, разнородной в части хранения ключей.

Типичная ситуация

- Криптосредство встроено через несколько стандартных криптографических API (.NET, Java, CNG, CADESCOM, PKCS# ll, CryptoAPI).
- Реализации интерфейсов зачастую сводятся к CryptoAPI.
- Система настроена на работу с единым установленным провайдером.
- И возникает вопрос – как перевести часть пользователей на неизвлекаемые ключи?

Текущее решение

Части пользователей поставить ФКН, обеспечить работу с неизвлекаемыми ключами с безопасной ФКН-аутентификацией.

- А если в рамках одной машины требуется работать с разными типами носителей?
- А если для части пользователей требуется работа с ключами в «облаке»?
- А если часть пользователей работает с усиленными организационными мерами, и им не требуется безопасная ФКН-аутентификация?

Вопрос

Как обеспечить прозрачный переход между способами хранения ключей в системе?

- Без внесения модификаций в прикладную систему.
- Без доработок для поддержки альтернативных API ради неизвлекаемых ключей.
- Без рисков возникновения проблем совместимости.
- Минимизируя количество формуляров, актов, лицензий...

Ответ

Использовать единый криптопровайдер КриптоПро CSP 5.0 вместе с носителями Рутокен/Gemalto, обеспечивающий работу с любыми способами хранения ключей.

- Со всем многообразием методов аутентификации/неизвлекаемости/защищённости.
- Предоставляющий полный набор привычных интерфейсов КриптоПро CSP для бесшовного встраивания и прозрачного перехода.

КриптоПро CSP 5.0

- Поддержка всех способов хранения ключей.
- Поддержка алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, а также полного набора рекомендаций ТК 26.
- Поддержка Windows, Linux, MacOS, iOS, Android.
- Все интерфейсы КриптоПро CSP, а также Java-интерфейс для работы с CSP.
- Поддержка «облачного» хранения ключей.
- Планируемый срок сертификации: осень 2017.
- Обеспечение прозрачного перехода на неизвлекаемые ключи.
- Подходят бессрочные лицензии от 4.0, а срочные вовсе не привязаны к версиям.

КРИПТОПРО

«КриптоПро» – разработка средств криптографической защиты информации.

info@cryptopro.ru
www.cryptopro.ru

Мобильная электронная подпись: российские реалии

Программные интерфейсы автоматизации КриптоПро DSS позволяют интегрировать использование сервера электронной подписи в существующие бизнес-процессы и системы. Ниже представлены типовые схемы использования КриптоПро DSS на примере систем дистанционного банковского обслуживания (ДБО).

Мобильная подпись

Основные программные технологии мигрируют на мобильные устройства. В первую очередь как раз те, что, как и работа с электронной подписью, предполагают повседневное использование.

Основные вопросы

- Пожелания к порядку использования?
- Как обеспечить безопасность с учётом ограничений мобильных устройств?

Пожелания

Дать пользователю инструмент, позволяющий с помощью его мобильного телефона воспользоваться своим ключом ЭП.

- Произвольного телефона, не только на iOS или Android.
- Всюду, где есть связь, необязательно мобильный интернет.
- Работа с ключом ЭП без 40 минут (включая 25 минут на перезагрузку ОС с обновлениями) на начало работы с токенами (с пользователем, который может забыть воткнуть токен).

Цель

Обеспечить работу с использованием ключевой информации на SIM-картах.

- Нет ограничений по телефону (работа через STK).
- Требуется только работа с сервисными сообщениями (SMS).
- Существенные ограничения по визуализации.

Подход «в лоб»

Ключ электронной подписи непосредственно на SIM-карте (аналогично мобильным приложениям для ЭП на iOS/Android).

Проблема

В ряде аспектов, важных для средств ЭП с учётом российских требований, SIM существенно отличается от привычных сред функционирования.

Причины

- Принципиальные отличия ГОСТ Р 34.10 от RSA.
- Необходимость доверенной реализации VS Производительность.
- «Тяжеловесность» криптографии с открытым ключом при реализации с учётом российских требований (даже KCL) при работе на низкоресурсных вычислителях.
- Требования по визуализации: однозначное соответствие подписываемого документа визуализируемому.

Безопасность подписи

- В отличие от RSA, для ГОСТ Р 34.10 требуется доверенный источник случайности.
- Его сбой влечёт компрометацию ключа ЭП.
- Это событие крайне трудно обнаружить автоматически (подпись останется корректной).

Доверенные реализации криптографии на эллиптически кривых

- Реализация работы с эллиптическими кривыми на уровне апплета – 2-3 минуты.
- Реализация на SIM- карте с сопроцессором не соответствует требованиям в случае зарубежной SIM, дорого в случае специальной российской.
- Необходимость противодействия атакам по побочным каналам (в т. ч. по времени) – дополнительное снижение производительности.

Итого

Безопасная реализация процедур вычисления электронной подписи непосредственно на SIM-карте существенно затруднена.

Разумная цена за возможность пользоваться преимуществами асимметричных схем.

Но действительно ли в случае мобильной подписи есть смысл платить эту цену?

Дополнительная проблема: визуализация

- Российские требования строго обязывают в полной мере визуализировать документ.
- Требуется обеспечить эквивалентность визуализируемого документа подписываемому.
- Невозможно выполнить для сервисных (SMS) сообщений.
- Исключения: отдельные случаи коротких текстов /xml.

Следствие 1

Требуется отдельно обеспечить доверенную визуализацию документа дополнительными средствами.

Следствие 2

Требуются доверенные серверные компоненты, их взаимодействие с SIM и с компьютером пользователя. К этим серверным компонентам не может не требоваться полное доверие: наличие злоумышленника, имеющего к ним доступ, немедленно приводит к угрозе подмены подписываемого сообщения.

- Требуется доверенная серверная часть.
- Отношения доверия пользователя с серверной частью устанавливаются явным образом.

- Аутентификация в рамках замкнутой системы.
- А это значит что потребности в «асимметричности» криптографии нет.

Альтернатива

- Аутентификацию сообщений между мобильным устройством и серверной стороной можно осуществлять с использованием симметричных алгоритмов.
- HMAC ГОСТ Р 34.11-2012 256, стандартизированный в Р 50.1.113-2016 Росстандарта.
- Задача безопасной реализации данного алгоритма на SIM-карте является беспроблемно выполнимой.
- Производительности базовой (без криптосопроцессора) архитектуры достаточно.
- Учесть необходимость противодействия атакам по побочным каналам можно без вреда для эффективности вычислений.
- Нет требований по доверенным ДСЧ на клиентской стороне.

Преимущества

Централизованное хранение ключей ЭП пользователей на серверной стороне решает и ряд других задач:

- Повреждение/утеря телефона не приводит к утере ключей ЭП, в случае утери доступ к ключам блокируется мгновенно на серверной стороне (а не через CRL с задержкой).
- Наличие журналов аудита на сервере при любой нештатной ситуации позволяет гарантированно установить, был ли осуществлён несанкционированный доступ к ключу подписи.
- Пользователь имеет возможность доступа к своим ключам подписи сразу с нескольких устройств, что удобно для «мобильных» сотрудников и для руководителей высшего звена.
- Преимущества симметричных алгоритмов в части сроков действия ключей – нет априорно известного нарушителю открытого ключа, не начать атаку до использования ключа.
- На телефоне – только средство аутентификации, компонент, не являющийся самостоятельным СКЗИ. Важно для массовой криптографии с пониженным регулированием.
- КриптоПро DSS (первые 11 исполнений) сертифицирован (СКЗИ, СЭП) в августе 2017.
- Работа КриптоПро DSS в составе КриптоПро УЦ 2.0 – согласование новых (включающих в свой состав DSS) исполнений КриптоПро УЦ 2.0 в процессе.
- КриптоПро DSS с поддержкой SIM с ключом аутентификации (HMAC) – отчёт на экспертизе с июня 2017.

Криптовалюты и блокчейн: вопросов много больше, чем ответов

«Я не технический специалист, но начал погружаться в тематику и понял, что это очень надёжно, так как никто не может манипулировать данными», – из одного неназванного интервью.

Популярность биткойна, вызванная стремительным ростом его стоимости в 2017 году, с одной стороны повлекла за собой взрывной рост интереса не только к нему самому и другим криптовалютам, но и к сопутствующим технологиям (прежде всего – к блокчейну), что в целях общего повышения осведомлённости очень даже хорошо, а с другой – породила целый ряд мифов и заблуждений, которые, в свою очередь, создали плодотворную почву для различного рода мошенничества, мелкого и не очень.

Публикаций, новостей, обсуждений по теме КВ и БЧ (криптовалют и блокчейна) уже стало так много, что про них слышали даже и не особо интересующиеся, при этом такое постоянное нахождение на слуху у части аудитории может вызвать ощущение того, что общие основы они себе в целом представляют, а детали не так уж важны.

Однако известно, кто скрывается в деталях, да и мифы, если они не Древней Греции, вряд ли могут доставить хотя бы эстетическое удовольствие и несут в себе хоть какую-то ценность.

В статье рассмотрены некоторые основные вопросы, чаще всего возникающие по поводу биткойна и других криптовалют, а также связанных с ними технологий, таких как блокчейн, смарт-контракты, ICO. При этом, как честно и указано в названии статьи – вопросов много больше, чем ответов.

Вопрос №1 Можно ли заработать на самостоятельном майнинге криптовалют?

Сама логика платформы, на которой построен биткойн и его многочисленные аналоги, иногда называемые альткойнами, казалось бы, позволяет делать деньги из воздуха в процессе так называемого майнинга.

На самом деле майнинг изначально предполагает прежде всего деятельность по поддержанию работоспособности платформы, но за эту деятельность любой желающий (если ему повезёт и он обладает достаточными вычислительными ресурсами) может получить вознаграждение в виде биткойнов, эмитируемых примерно каждые 10 минут (это вообще единственный способ появления новых биткойнов, кстати).

Первоначально вознаграждение составляло 50 биткойнов, с ноября 2012 уже 25 биткойнов, а с июля 2016 только 12,5 биткойна. К слову, следующее уменьшение по прогнозу состоится примерно в середине 2020 года.

Технически упрощённо майнинг выглядит примерно так: все одновременно решают некоторую математическую задачу (получение красивого с математической точки зрения значения хэш-функции для очередного блока с транзакциями) и тот, кто решит её первым, получает вознаграждение.

Такая простая возможность заработка биткойнов сначала привлекала только энтузиастов, но в скором времени были вовлечены и более широкие слои населения: недавний бум «ферм для майнинга» трудно было не заметить. По мере роста числа «майнеров» зарабатывать таким образом становилось всё сложнее.

По мнению многих специалистов, сейчас стоит инвестировать в оборудование для майнинга только в расчёте на очень долгосрочную перспективу или при наличии возможности сразу привлечь существенные вычислительные ресурсы.

Для понимания того, что означает «существенные», можно привести как пример, что, согласно некоторым источникам, КНДР с 2017 года использует майнинг криптовалют для поддержки своей национальной валюты – северокорейской воны.

Другой пример – российский холдинг RMC интернет-омбудсмена Дмитрия Мариничева в ходе первичного размещения монет (ICO) на постройку майнинговой фермы мощностью 20 мегаватт в районе с излишками электроэнергии собрал сумму, эквивалентную 43,2 миллиона долларов (изначально планировалось привлечь 100 миллионов долларов).

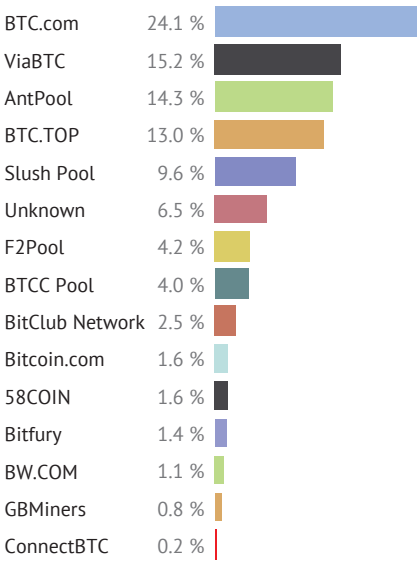
Алексей Колесник, ранее руководивший комитетом природных ресурсов в Минприроды Татарстана, а в конце декабря 2017 года возглавивший ООО «Губахинская энергетическая компания» (ГЭК, в которую входят Кизеловская ГРЭС в Пермском крае мощностью 23,6 МВт и Сарапульская ТЭЦ в Удмуртии мощностью 10 МВт), подтвердил изданию «Коммерсантъ», что рассматривает вариант с майнингом криптовалюты на площадке в Удмуртии.

Думаю, масштабы, при которых сегодня индивидуальный (самостоятельный) майнинг является инвестиционно привлекательным, примерно понятны.

Вопрос №2 Можно ли заработать майнинге криптовалют через пулы?

Решаемая в процессе майнинга математическая задача легко поддаётся распараллеливанию, поэтому отлично зарекомендовали себя так называемые пулы – объединения пользователей, предоставляющих свои вычислительные ресурсы. Пул, действуя как один майнер, получает достаточную производительность для более эффективной работы и существенно увеличивает свои шансы на решение очередной задачи первым.

Крупнейшие пулы и их приблизительные оценки мощности представлены на рисунке ниже.



Так как заработанные пулом биткойны распределяются между всеми его участниками (конкретные схемы распределения могут быть различными), то даже при частом успешном майнинге пула отдельному его участнику достаётся не такая уж крупная сумма. Понятно, что верно и обратное – у пулов с небольшим числом участников доля каждого частника больше, но и шансов на получение биткойнов в ходе майнинга существенно меньше. Не стоит забывать и про комиссию, которую берёт себе пул.

Кроме того, появление в цепочке дополнительно звена в виде пула создаёт дополнительные риски. Например, 6 декабря 2017 года один из

популярных пулов NiceHash подвергся взлому, в результате которого было похищено 4700 биткойнов (64 млн долларов по курсу на тот момент). Справедливости ради стоит сказать, что в конце января NiceHash обязался компенсировать потери всем своим пострадавшим пользователям, правда частями на протяжении нескольких месяцев и, как мы все понимаем, без учёта колебаний курса биткойна к доллару.

Вопрос №3
Можно ли заработать на торговле криптовалютой?

Впрочем, майнинг давно уже не единственный способ для заработка на криптовалютах. Красивые графики динамики роста курса того же биткойна привлекают многих – и профессиональных спекулянтов, и рядовых пользователей.

Вот, например, как выглядел график курса биткойна с января 2017 по январь 2018 (рис 1).

Фантастические проценты годовых вполне могут заглушить даже самый громкий голос разума – и вот уже открыто несколько страниц, найденных через поисковики, с пошаговыми инструкциями о том, как максимально просто и выгодно приобрести немного криптохайпа.

Миллиардер Уоррен Баффетт (инвестор с мировым именем) не так давно в интервью телеканалу CNBC заявил, что не будет инвестировать в криптовалюты: «Я могу почти с уверенностью сказать, что они плохо кончат. Когда это случится или как именно — я не знаю».

Генеральный директор банка JPMorgan Chase Джейми Даймон, в сентябре назвавший биткойн мошенничеством (он сравнил его с тюльпанной лихорадкой в Голландии и предупредил, что если кто-либо из трейдеров JPMorgan решит заняться криптовалютами, то будет уволен за «глупость»), позже заявил, что сожалеет о своих словах о биткойне, но криптовалюта ему по-прежнему неинтересна. Он отметил, что сейчас многие относятся к биткойну «как к чему-то весьма значимому», но у него самого другое мнение.

Заработать на торговле биткойном, несомненно, можно – как и на любой торговле на бирже. Но ровно также можно и потерять свои сбережения. Пожалуй, если учесть сложности с конвертированием криптовалюты в реальные деньги, риски потери денег из-за несовершенства системы в целом (см. следующие вопросы), а также слабое регулирование этой сферы (проблемы «обманутых криптодольщиков» никто точно за них решать не будет), то вполне разумной альтернативой приобретению криптовалюты с целью заработка будет приобретение лотерейного билетика.

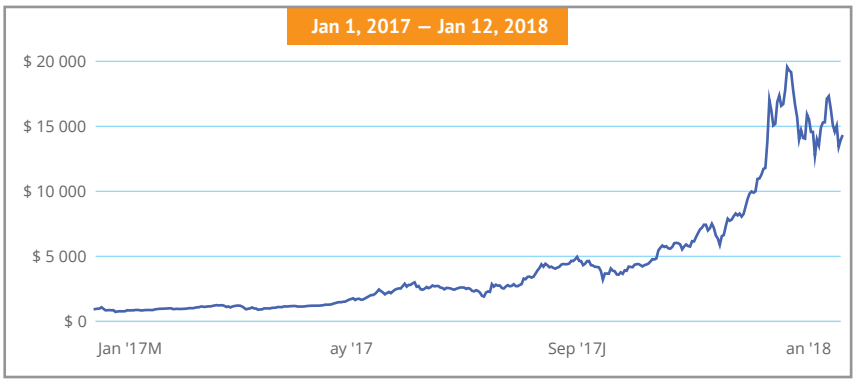


Рисунок 1

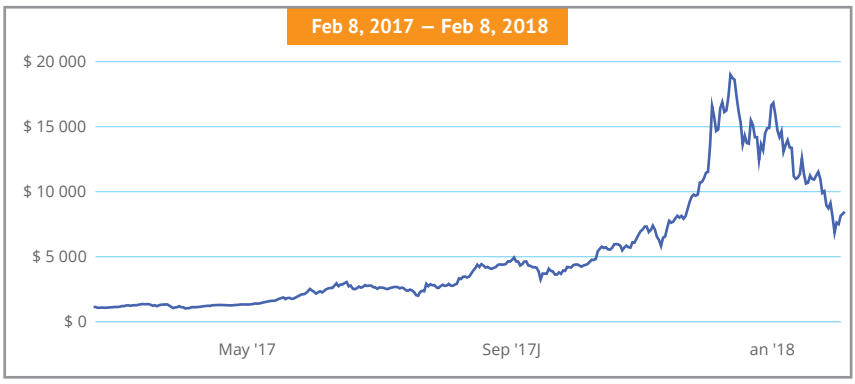


Рисунок 2

Для иллюстрации – вот тот же график курса биткойна, только уже с февраля 2017 по февраль 2018 (рис 2).

Далеко не так привлекательно выглядит. Впрочем, красивое слово волатильность (финансовый показатель, характеризующий изменчивость цены) для кого-то как раз лакмусовая бумажка, показывающая, что при таких резких скачках можно сделать отличные деньги (за счёт тех, кому это слово, например, кажется не красивым, а непонятным).

Вопрос №4
Являются ли криптовалютные технологии безопасными?

Приставка «крипто» легко может ввести в заблуждение. Однако криптография – это лишь часть системы и, пока квантовые компьютеры окончательно не изменили установившийся порядок вещей, – самая, пожалуй, надёжная её часть.

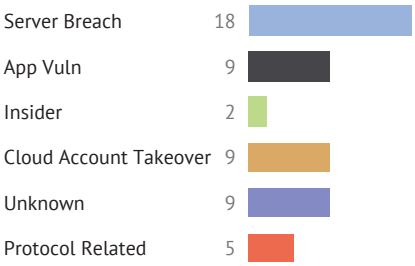
Лежащие в основе большинства криптовалют алгоритмы вычисления электронной подписи на базе асимметричной криптографии и последовательного хэширования сами по себе вполне надёжны, широко применяются (не только на рынке криптовалют) и при необходимости могут быть заменены на аналоги, более стойкие, чем текущие.

Вместе с тем, по некоторым оценкам, менее чем за 10 лет хакерами было похищено только биткойнов и эфира на сумму порядка 1,2 миллиарда долларов.

Компрометация закрытых ключей пользователей (читай – их криптокошельков), взлом криптовалютных бирж, майнинговых пулов – далеко не полный перечень возможных инцидентов. Какие бы надёжные алгоритмы и протоколы ни лежали в основе самой криптовалюты, всё равно неизбежно остаются уязвимости в их практической реализации и в обслуживающих сервисах.

На GitHub есть отдельный репозиторий «Кладбище блокчейна» (Blockchain Graveyard), где собирается информация о различных публичных инцидентах, связанных с

криптовалютами и блокчейном. На момент подготовки статьи был описан 51 такой инцидент. Ниже на диаграмме представлена статистика по причинам инцидентов: взлом сервера, уязвимость приложения, действия инсайдера, кража «облачной» учётной записи, неизвестные причины и причины, связанные с применяемыми протоколами.



Не стоит забывать и про человеческий фактор: фишинговые атаки, ненадёжные пароли, социальная инженерия – всё это повсеместно используется в более традиционном финансовом секторе, где отпор злоумышленникам могут дать те же банки. В мире криптовалют, как уже отмечалось выше, в этом смысле царит первобытная анархия – каждый сам за себя. Думаю, никто не назовёт ущерб, который понесли рядовые пользователи по своей собственной вине, потеряв тем или иным способом доступ к своему криптокошельку.

Наконец, несмотря на общую устойчивость и крайне высокую степень продуманности общей архитектуры (что, к слову, вполне может навести на мысли о причастности к процессу спецслужб), существуют потенциальные возможности для компрометации и основополагающих идей того же биткойна.

Так, в докладе исследователей Института инженеров электротехники и электроники (IEEE – Institute of Electrical and Electronics Engineers) отмечается, что существует возможность использовать одни и те же биткойны дважды, применив так называемую атаку баланса, когда злоумышленники задерживают сетевые коммуникации между группами майнеров, чьи компьютеры проверяют транзакции в цепи, добиваясь тем самым при достаточной длительности такой задержки возможности получить два одновременных подтверждения от двух разных получателей их биткойнов и успеть, например, обменять их на реальные доллары.

Понятно, что в любом случае, как и при так называемой атаке 51% (когда кто-то владеет более чем половиной мощности и может создавать две параллельные цепочки транзакций), злоумышленники могут лишь дважды потратить свои собственные биткойны («двойное расходование»), да и технически такая атака пока выглядит сложно реализуемой на практике, но исследования продолжаются и пока нет гарантий, что не будет найден более простой и менее затратный способ.

Вопрос №5
Является ли криптовалюта анонимным средством платежа?

Пожалуй, это один из самых простых вопросов, на который действительно можно дать однозначный ответ: система анонимна, ровно пока пользователь соблюдает свою анонимность.

Согласитесь, трудно считать систему, в которой все транзакции записываются, доступны абсолютно всем и хранятся вечно, полностью анонимной. Строго говоря, вся анонимность держится на том, что никто не знает, кому какой кошелёк принадлежит, но все история операций открыта и прозрачна. Как только пользователь регистрируется на бирже для, например, перевода криптовалюты в реальные деньги, становится участником майнинг пула, указывая свои регистрационные данные, или любым другим способом даёт возможность связать с собой (например, со своим IP-адресом ил адресом электронной почты) какой-либо кошелёк, в тот же момент все его предыдущие транзакции перестанут быть анонимными.

Вопрос №6
Каков правовой статус криптовалют в России?

Завершить статью логично ответом на вопрос о правовом статусе криптовалют в нашей стране. На сегодняшний день такой статус не определён.

Однако на общественном совете при Минфине РФ 28 декабря был представлен законопроект о регулировании цифровых активов в Российской Федерации. В законопроекте даются определения криптовалюте, майнингу и ICO (процедуре первичного размещения токенов). Финальный вариант законопроекта о регулировании криптовалют в РФ, согласно поручению президента Владимира Путина, должен быть подготовлен в первом полугодии 2018 года.

При этом, как сообщил замминистра финансов Алексей Моисеев, Минфин намерен в феврале внести в Госдуму законопроект о криптовалютах (на момент подготовки статьи этого ещё не произошло). В рамках доработки законопроекта в частности предполагается определить перечень площадок, на которых можно будет совершать сделки с криптовалютами.

А пока Минтруд официально разрешил госслужащим не декларировать сведения о наличии виртуальных валют, как сообщило РИА Новости со ссылкой на заявление ведомства: «Формой справки не предусмотрено указание товаров, услуг, полученных в натуральной форме, а также виртуальных валют».

Пока же с юридической точки зрения согласно сттатье 27 Федерального закона от 10 июля 2002 г. №86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и статье 75 Конституции РФ официальной денежной единицей в стране является рубль, а введение других денежных единиц и выпуск денежных суррогатов запрещено, что не позволяет рассматривать никакую криптовалюту как легальное денежное средство.

Официальные позиции по этому вопросу сформулировали ФНС России в письме от 3 октября 2016 г. № ОА-18-17/1027 и Банк России в релизе «Об использовании частных „ виртуальных валют “ (криптовалют)». И налоговики, и банкиры отметили риски выпуска и обращения криптовалют, а ФНС России в своем письме отдельно напомнила о запрете выпуска денежных суррогатов.

Заключение

За рамками статьи остались такие интересные вопросы, как: заменят ли со временем криптовалюты фиатные деньги, действительно ли биткойн является проектом спецслужб, и, пожалуй, ещё два десятка других. На часть из них ответит время, а какие-то, очевидно, так и останутся без ответа – ровно как и те вопросы, что были рассмотрены в данной статье.

Алексей Комаров
автор блога по информационной безопасности www.zlonov.ru

Взаимодействие функционального ключевого носителя (ФКН) и устройств контроля подписи

В отличие от обычных активных носителей, где аутентификация производится простым явным предъявлением PIN-кода по открытому каналу, ФКН для аутентификации и установления защищённого канала используют протокол SESPAKE.

После выполнения протокола между токеном и криптопровайдером устанавливается защищённое соединение, а все данные, которыми они обмениваются, проходят в зашифрованном виде. Нарушитель, прослушивающий канал, не только не может узнать, какие данные подписываются на носителе, но даже понять, команда какого типа посылается криптопровайдером.

Устройство контроля подписи

Однако есть атака, от которой не застрахованы даже ФКН: подмена подписываемых данных до передачи их криптопровайдеру. В этом случае нарушитель находится между пользователем и криптопровайдером, в адресном пространстве пользовательского процесса, и имеет возможность незаметно изменить данные, которые пользователь хочет подписать.

Так как криптопровайдер не показывает пользователю, какие именно данные он отправляет на подпись, подменённая информация успешно подписывается. Поскольку в данном случае речь идёт о нарушителе в адресном пространстве процесса, никакими программными способами, добавленными в криптопровайдер, защититься от него нельзя.

Тут на помощь приходят устройства контроля подписи (УКП), которые отображают на экране подписываемые данные, запрашивающие у пользователя разрешение на подпись (рис. 1). Как правило, они либо представляют собой считыватель, в который может быть вставлен активный носитель, либо сами являются активными носителями с экраном. В любом случае предполагается, что между таким устройством и носителем нарушителя нет. А вот между ним

и криптопровайдером или в одном адресном пространстве с криптопровайдером нарушитель может быть.

Криптопровайдер, получив данные для хэширования, которые потом надо будет подписать, не только сам хэширует их, но и посылает в устройство контроля подписи. В результате хэширования в криптопровайдере получается значение, названное на рисунке ХЭШСР.

УКП имеет экран, на который оно выводит значимую часть подписываемого документа. После отображения документа на экране устройство запрашивает у пользователя разрешение на подпись. Если тот согласился, считается значение хэша документа, которое сохраняется в кэше устройства. На рисунке оно названо ХЭШV.

Когда криптопровайдер посылает носителю, вставленному в УКП, APDU-команду подписи, устройство контроля подписи перехватывает её, выделяет из неё переданный хэш, и последовательно сравнивает со всеми значениями из своего кэша, то есть с теми, на которые получено разрешение пользователя. Если в кэше находится такое же значение, команда подписи пропускается к носителю, в противном случае – отвергается. Таким образом, отвергаются все команды подписи, кроме содержащих хэши от данных, явно одобренных пользователем.

Если нарушитель попытается прямо в канал между криптопровайдером и носителем записать APDU-команду, содержащую некоторый ХЭШХ, эта команда будет отвергнута. Точно так же будет отвергнута команда, содержащая хэш от данных, которые не передавались криптопровайдером устройству контроля подписи, или от данных, не получивших разрешения пользователя (на рисунке — ХЭШ0).

Большим плюсом такого подхода является возможность работы с активным носителем как с помощью обычных считывателей, так и через УКП. Носитель, использовавшийся с устройством контроля подписи, в любой момент времени можно вставить в обычный считыватель и выполнить подпись на том же закрытом ключе.

Фактически, устройство контроля подписи является легальным MITM-нарушителем, фильтрующим обмен сообщениями между носителем и криптопровайдером.

Контроль подписи и ФКН

Кажется, что данная логика входит в противоречие с идеологией ФКН, в рамках которой невозможны даже «легальные нарушители». Защищённый канал, устанавливаемый между криптопровайдером и носителем, скрывает команды подписи, поэтому УКП не может отфильтровать неразрёшенные пользователем хэши. И хотя ФКН защищён от формирования злоумышленником собственной команды в канале между криптопровайдером и носителем, он беззащитен от передачи в криптопровайдер подменённых данных. Это могло бы ограничить возможности использования функциональных носителей, но у данной проблемы есть решение, и мы его здесь представим.

В случае если устройство контроля подписи совмещено с носителем (то есть фактически они — единое целое), то систему фильтра переданных хэшей можно разместить уже после расшифрования команд внутри устройства, так что никакой проблемы нет.

Но если устройство контроля подписи представляет собой только считыватель, в который может быть вставлен один из множества функциональных носителей, решение несколько сложнее, и заключается в переносе кэша разрешённых хэшей в носитель (рис. 2).

Криптопровайдер работает с устройством контроля подписи и с ФКН точно так же, как было описано ранее. Функциональный носитель получает все APDU-команды подписи по защищённому каналу. Но у носителя есть две специальных APDU-команды, разрешённых и по открытому каналу:

- команда, переводящая ФКН в режим работы по белому списку;
- команда, передающая в ФКН одно из значений из белого списка.

Белый список — это, по сути, тот же кэш хэшей, только хранящийся в носителе. После получения первой команды носитель, получив команду подписи, проверяет, есть ли подписываемый хэш в его кэше, и подписывает только те хэши, которые нашёл. Вторая команда передаёт носителю значения хэша, которые тот сохраняет в свой кэш. Не получив первую команду, ФКН подписывает любой переданный ему хэш.

Эти две команды формирует и посылает носителю устройство контроля подписи. Также УКП следит, чтобы носителю не были переданы эти команды со стороны криптопровайдера из канала, в котором может быть нарушитель (это возможно, если защищённый канал ещё не был установлен). А так как между носителем и устройством контроля подписи нарушителя нет (ведь токен или смарт-карта напрямую вставляется в корпус устройства или встроен в УКП), то гарантируется, что кэш носителя будет наполнен только хэшами, переданными устройством контроля подписи.

Первую команду устройство контроля подписи посылает носителю, когда перехватывает APDU-команду аутентификации по SESPAKE (она означает, что криптопровайдер собирается установить защищённый канал с носителем, в котором, возможно, будут проходить команды подписи).

Следом УКП посылает носителю все значения хэшей, разрешённых пользователем в тот момент, а после этого уже пересылает перехваченную команду аутентификации. Также устройство контроля подписи посылает очередной хэш носителю в тот момент, когда пользователь разрешает его подпись.

В итоге

Работающий по такой схеме носитель может быть вставлен и использоваться как с обычным считывателем, так и с УКП.

Устройство контроля подписи не встраивается в защищённый канал, а обменивается данными с криптопровайдером и носителем по открытому каналу.

Криптопровайдер взаимодействует с ФКН, вставленным в УКП, точно так же, как если бы он был вставлен в обычный считыватель.

Достигается основная цель: подписи хэшей данных, отвергнутых пользователем или не передававшихся в устройство контроля подписи, будут отвергнуты носителем (см. на рисунке ситуацию для ХЭШ0).

ХЭШХ, как было сказано выше, будет отфильтрован, потому что команда подписи в ФКН может быть передана только по защищённому каналу.

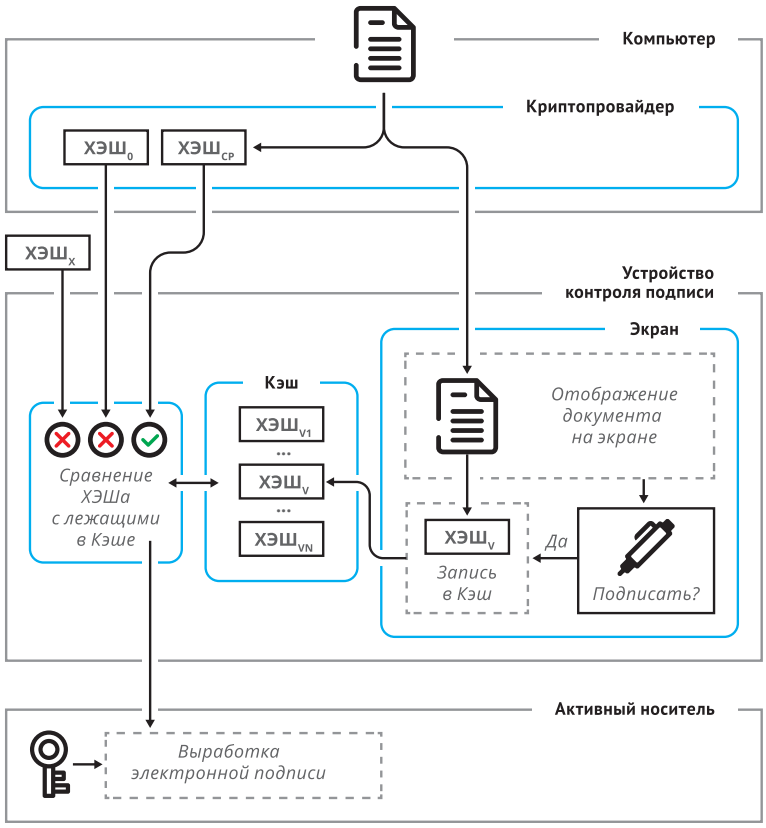


Рисунок 1

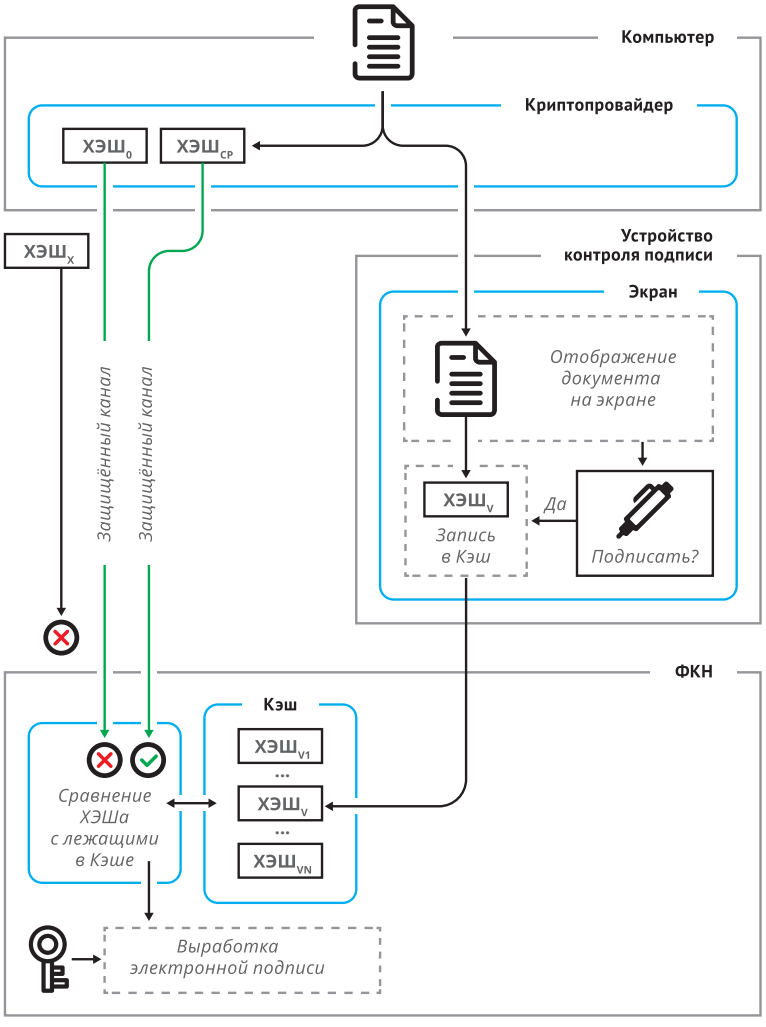


Рисунок 2

Основная опасность данного способа в том, что носителю будет передана команда, записывающая хэш нарушителя в белый список. Но так как, как отмечено выше, нарушителя между устройством контроля подписи и носителем нет, а все команды записи хэша в белый список, полученные УКП снаружи, отфильтровываются, нарушитель не может записать в кэш носителя свой хэш.

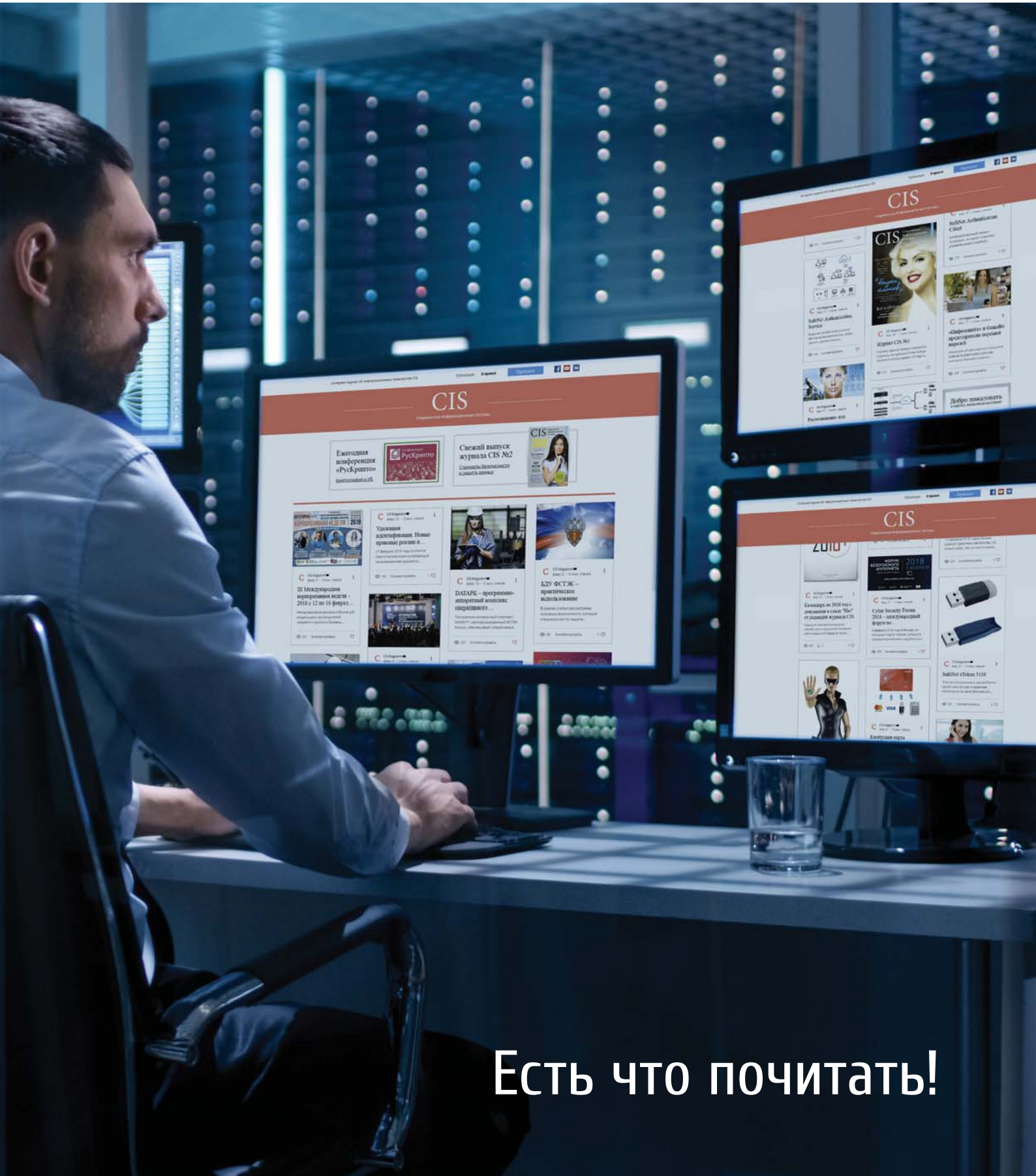
Использование же этих команд без устройства контроля подписи не сможет снизить защищённости ФКН: максимум, можно перевести носитель в режим работы по белому списку, после чего он откажется принимать от криптопровайдера любые команды подписи до ближайшей команды сброса состояния, но это не заставит его ни подписывать хэши, переданные по открытому каналу, ни каким-либо образом раскрыть хранимую на нём закрытую информацию.

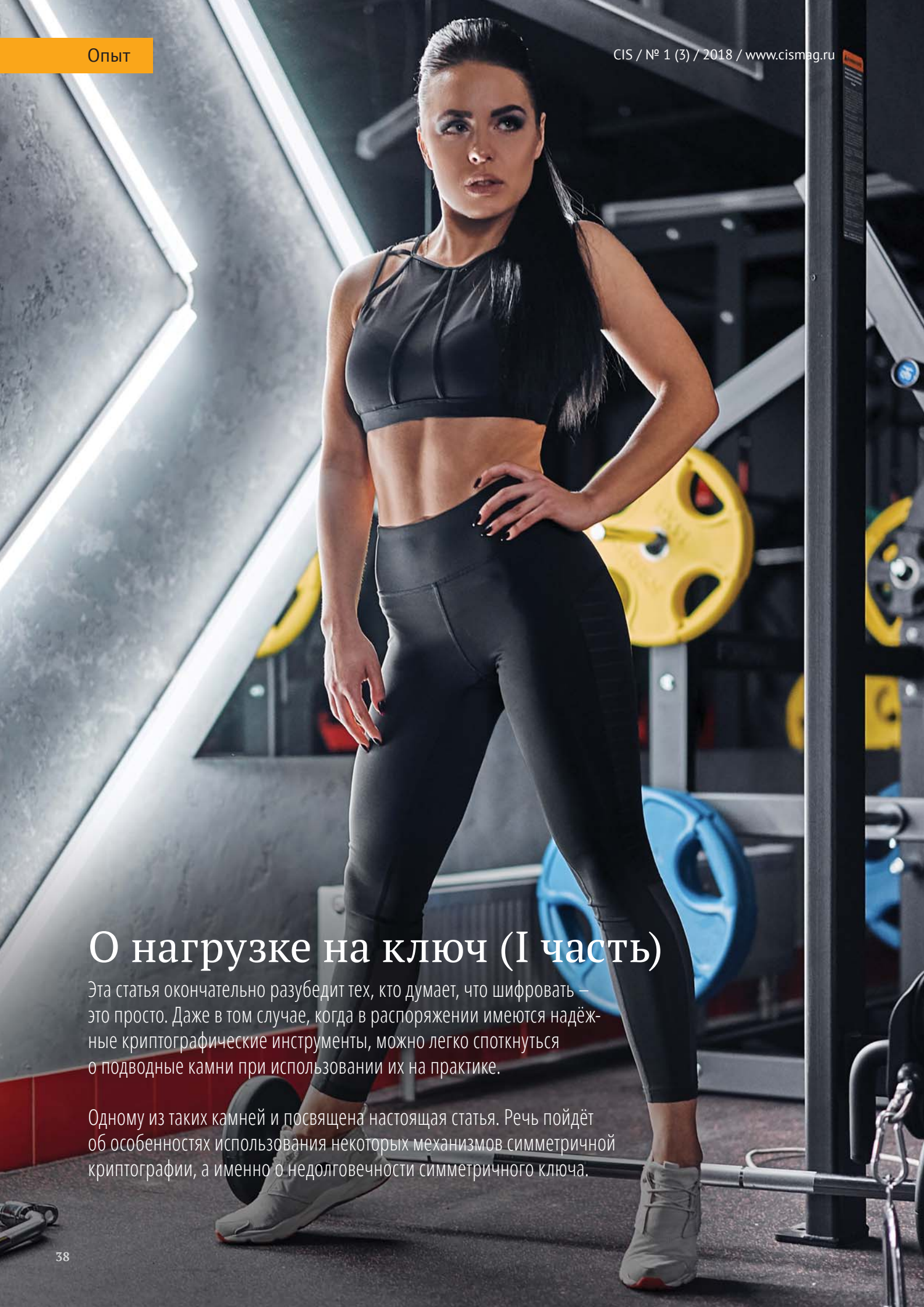
Основным недостатком метода является то, что работать с УКП могут не любые ФКН, а только те, которые поддерживают белые списки. Но поддержка не требует больших затрат ресурсов от носителей: чаще всего между выработкой хэша и его подписью проходит минимальное количество времени, и поэтому можно использовать один кэш для всего ФКН, размером порядка десяти значений, с вытеснением старых хэшей новыми. А операция нахождения в кэше значения, совпадающего с переданным в команде подписи, не является сложной для микропроцессора носителя.

Таким образом, предложенная схема позволяет использовать функциональные ключевые носители вместе с устройствами контроля подписи, что делает их защищёнными от атаки с подменой данных, сохраняя все прочие положительные качества ФКН.

CIS news

www.cismag.news





О нагрузке на ключ (I часть)

Эта статья окончательно разубедит тех, кто думает, что шифровать – это просто. Даже в том случае, когда в распоряжении имеются надёжные криптографические инструменты, можно легко споткнуться о подводные камни при использовании их на практике.

Одному из таких камней и посвящена настоящая статья. Речь пойдёт об особенностях использования некоторых механизмов симметричной криптографии, а именно о недолговечности симметричного ключа.

Существование каких-либо особенностей на практике не означает, что используемые схемы ненадёжны. В теории надёжность или стойкость криптографических схем определяется только в совокупности с условиями, в которых та или иная схема должна функционировать (они определяют возможности потенциального противника). Задача тех, кто данные схемы использует на практике, – сделать реальные условия максимально близкими к «безопасным» теоретическим условиям. Так, априорное существование общих методов и подходов, позволяющих компрометировать ключ или данные при наличии у противника большого объёма информации, приводит к появлению таких важных понятий, как «нагрузка на ключ» и «срок жизни ключа». В настоящей статье мы рассмотрим проблему недолговечности симметричного ключа и расскажем о существующих подходах к её решению.

Что скрывается за «шифрование данных»?

С тех пор как криптография выделилась в самостоятельный раздел науки, её терминологическая база активно расширяется (блочные шифры, режимы работы шифра, нагрузка на ключ, срок жизни ключа, механизм смены ключа), что может вносить путаницу и усложнять понимание. Ситуация в отечественной криптографии усугубляется ещё и неточностью перевода, так как большинство терминов заимствуются из английского языка. В настоящей статье мы будем говорить только о криптографических конструкциях, основанных на блочных шифрах, и далее коротко введём необходимые для этого понятия и поясним связь между ними.

Примитивы — это математические объекты, которые сами по себе не позволяют решать какие-либо прикладные задачи криптографии. Примерами являются хэш-функция, группа точек эллиптической кривой, блочный шифр. Поговорим о последнем. Блочный шифр (или просто шифр) — семейство взаимно однозначных отображений множества двоичных строк некоторой фиксированной длины (блоков) в себя, индексируемое ключом, который тоже является двоичной строкой фиксированной длины. Блочный шифр оперирует исключительно блоками, то есть абстрактной единицей его работы является блок. Примерами блочных шифров являются алгоритмы Магма и Кузнечик, определяемые в ГОСТ Р 34.12-2015.

Утверждение «данные зашифрованы с помощью блочного шифра» не в полной мере описывает состояние дел, потому что зашифровать с помощью любого шифра можно по-разному — стойко и нестойко. Например, шифровать каждый блок по отдельности — плохая идея. В этот момент возникает такое понятие, как режим работы шифра — порядок применения шифра для обработки сообщения, размер которого может не только превышать размер блока, но и не быть кратным ему. Режимы шифрования проектируются таким образом, чтобы минимально зависеть от принципов работы самого шифра (максимум, от размеров блока и ключа). Единицей работы режима является уже не блок, а целое сообщение. Все режимы разрабатываются для решения конкретных прикладных задач — обеспечения конфиденциальности или целостности, причём разные режимы могут решать разные задачи. Например, конфиденциальность информации обеспечивают такие режимы шифрования, как CTR, OFB, CFB, CBC. В свою очередь, для обеспечения целостности используются режимы выработки кода аутентификации OMAC, TMAC, CBC-MAC. Также существуют режимы, решающие одновременно обе задачи: GCM, CCM (так называемые режимы аутентифицированного шифрования – AEAD). Описание некоторых из этих режимов можно найти в ГОСТ Р 34.13-2015.

Теперь о криптографических свойствах описанных объектов. Понятие стойкости определяется в рамках модели противника и не существует отдельно от понятия угрозы. Чтобы не нагружать читателя введением сложных определений, не нужных для понимания основной идеи статьи, под стойкостью будем подразумевать отсутствие у противника какой-либо возможности компрометировать ключ или данные.

Итак, фундамент заложен и можно переходить к обсуждению основной темы статьи.

Может ли ключ «жить» вечно?

Рассмотрим следующую прикладную задачу. Пусть нам необходимо на протяжении многих лет обмениваться с кем-то информацией, каждый фрагмент которой после передачи месяц хранится в секрете, после чего публикуется.

Для начала согласуем общий закрытый ключ, например, при личной встрече в защищённом от прослушивания подземном бункере. Насколько длинным он должен быть? Всем известно, что ключ можно найти с помощью полного перебора, но перебрать, например, 2^{256} возможных значений 256-битного ключа даже за 1000 лет невозможно. Таким образом, 256 бит должно хватить на очень долгое время. Далее выбираем стойкий блочный шифр с соответствующей длиной ключа, а также стойкий режим шифрования.

Можно начинать работу. Данные передаются, всё идёт хорошо.

По прошествии всего нескольких месяцев мы понимаем, что кто-то явно читает нашу переписку, при этом в совокупности нами было передано чуть больше 5 терабайт данных. В чём может быть причина? А причина в том, что мы не обратили внимания на размер блока используемого шифра, который оказался слишком мал – всего 40 битов (240 значений блоков * 5 байтов в блоке = 5 терабайтов). Противник терпеливо собирал передаваемые по каналу зашифрованные данные и соответствующие им открытые тексты, которые публиковались через месяц после передачи. С помощью собранных данных он в конце концов узнал результаты применения используемого блочного шифра ко всем возможным блокам и сохранил эти результаты в таблицу. Таким образом, с её помощью он смог расшифровывать любые данные, не зная ключ.

Этот простой пример демонстрирует важность условий, в которых функционирует система защиты информации, а именно важность учёта так называемой нагрузки на ключ. Нагрузка на ключ — это объём данных, обработанных на одном ключе. В рамках настоящей статьи будем считать, что нагрузка на ключ измеряется в блоках.

Практика показывает, что обработка большого количества сообщений на одном ключе может привести к потере стойкости (к компрометации ключа, дешифрованию конфиденциальных сообщений). В примере, описанном выше, противник использовал фундаментальное свойство

блочного шифра — взаимную однозначность отображений, приводящую к тривиальному ограничению нагрузки на ключ порядка 2n, где n – длина блока. Однако существуют другие не столь очевидные классы методов, необходимым условием работы которых также является наличие у противника большого объёма данных:

Методы анализа, основанные на свойствах используемого шифра

Наиболее распространёнными методами этого типа являются линейный и дифференциальный методы. Для «хороших» блочных шифров данные методы требуют наличия материала, объём которого по порядку соответствует тривиальному ограничению 2n. В данной статье мы исходим из того, что используемый шифр стойкий, и поэтому не будем далее учитывать эти ограничения.

Методы анализа, основанные на комбинаторных свойствах используемого режима работы шифра

Как уже было сказано ранее, комбинаторные свойства режимов минимально зависят от особенностей внутреннего строения используемого блочного шифра. Эти свойства начинают проявляться при обработке большого количества данных и могут привести к появлению реальных угроз. Ярким примером метода, осуществляющего такие угрозы, является атака Sweet32 на TLS, приводящая к частичному дешифрованию трафика. Ограничения, обусловленные методами этого типа, будем для краткости называть комбинаторными ограничениями (для большинства режимов по порядку они равны 2n/2).

Методы, основанные на информации, полученной по побочным каналам

При функционировании криптографических систем на практике у противника появляются возможности, которых нет на бумаге, — он может получать информацию о секретных параметрах системы с помощью так называемых побочных каналов. К ним можно отнести энергопотребление, электромагнитное излучение, акустический шум, время работы алгоритма. При обработке большого количества сообщений «опасная» информация, полученная по побочным каналам, накапливается, что может привести к осуществлению реальных угроз, например, вскрытию ключа. Примером метода, осуществляющего такие угрозы, является атака TEMPEST. Ограничения, обусловленные методами такого рода, будем называть ограничениями по побочным каналам.

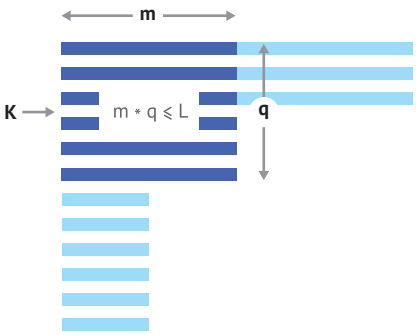
Ограничения, соответствующие методам анализа из пункта 1, близки к тривиальному 2n (в силу стойкости блочного шифра) и далее не рассматриваются. Также в рамках данной статьи будем считать, что ограничения по побочным каналам гораздо более сильные, чем комбинаторные (что обычно соответствует реальному положению дел).

Итак, после рассмотрения такого обилия различных методов становится очевидно, что ограничивать нагрузку на ключ не только желательно, но и необходимо. Отсюда возникает такое понятие как допустимая нагрузка на ключ или срок жизни ключа (в английском языке используется термин «key lifetime») — объём данных, который можно «безопасно» обработать на одном ключе. Здесь под словом «безопасно» также будем понимать отсутствие у противника возможности компрометировать любую конфиденциальную информацию.

Что если данных очень много?

Конкретное значение допустимой нагрузки на ключ определяется протоколом, в рамках которого используется тот или иной шифр и режим шифрования, с учётом описанных выше методов анализа и необходимого уровня стойкости.

Рассмотрим такой протокол. Исходя из необходимого уровня стойкости протокола фиксируется допустимая нагрузка на ключ L. Предположим, что на одном ключе обрабатывается q сообщений. Для упрощения понимания будем предполагать, что все сообщения имеют одинаковую длину m блоков. Параметры q и m должны выбираться так, чтобы суммарный размер этих сообщений не превосходил допустимую нагрузку на ключ, т. е. $q*m \leqslant L$. Графически это можно изобразить следующим образом: допустимая нагрузка на ключ L ограничивает площадь прямоугольника высоты q и длины m.



Следовательно, если хочется обрабатывать сообщения большей длины, придётся обрабатывать меньшее количество сообщений, и, напротив, при обработке большого числа сообщений все они должны быть небольшого размера. На практике часто бывает, что допустимая нагрузка на ключ оказывается слишком мала и с помощью одного ключа удаётся обработать очень небольшое число сообщений ограниченной длины. Но что делать, если нужно обрабатывать больше данных, не теряя стойкости?

Естественным решением проблемы «безопасной» обработки большого объёма данных, которое первым приходит в голову, является замена ключа на новый по истечении срока его жизни. Казалось бы, всё просто: шифруем максимально возможный объём данных, заменяем старый ключ на новый и продолжаем в том же духе. Такая замена в протоколах обычно называется пересогласованием ключа. Однако у такого подхода есть существенный недостаток: низкая эффективность. В большинстве протоколов пересогласование ключа приведёт к прекращению передачи прикладных данных, пересылкам ряда служебных сообщений, работе датчика случайных чисел и вообще уйме дополнительных вычислений, а в некоторых случаях придётся задействовать крайне ресурсоёмкую асимметричную криптографию.

Неужели не существует эффективного способа решения данной проблемы? К счастью, такой способ есть, и известен он под названием «rekeying» (преобразование ключа). О нём, его особенностях и разновидностях будет рассказано в следующей части нашей статьи.

О нагрузке на ключ (II часть)

В первой части статьи мы ввели такие понятия, как шифр, режимы работы шифра, а также немного рассказали о нагрузке на ключ, оставив открытым вопрос о том, как именно решать проблему эффективной обработки данных, объём которых выходит за рамки ограничений по нагрузке на ключ.

Естественным решением проблемы «безопасной» обработки большого объёма данных, которое первым приходит в голову, является замена ключа на новый по истечении срока его жизни. Казалось бы, все просто: шифруем максимально возможный объём данных, заменяем старый ключ на новый, и продолжаем в том же духе.

Такая замена в протоколах обычно называется пересогласованием ключа. Однако у такого подхода есть существенный недостаток: низкая эффективность. В большинстве протоколов пересогласование ключа приведёт к прекращению передачи прикладных данных, пересылкам ряда служебных сообщений, работе датчика случайных чисел и вообще уйме дополнительных вычислений, а в некоторых случаях придётся задействовать крайне ресурсоёмкую асимметричную криптографию.

Неужели не существует эффективного способа решения данной проблемы? К счастью, такой способ есть, и известен он под названием re-keying (преобразование ключа). О нём, его особенностях и разновидностях будет рассказано в следующей части статьи.

Промежуточный итог

Итак, если каждый раз пересогласовывать ключ вы не хотите, преобразование ключа re-keying спешит вам на помощь! Re-keying – подход, основная идея которого заключается в следующем: непосредственная обработка данных производится с помощью последовательности ключей, получаемых из первоначально согласованного ключа (будем называть его начальным) путём применения специально подобранных детерминированных преобразований. Эти преобразования позволяют считать выработанные ключи почти случайными и независимыми.

Будем выделять два типа подходов к re-keying: external (внешний) и internal (внутренний). Рассмотрим каждый из них подробно.

Internal re-keying

Подход internal re-keying заключается в модификации какого-то конкретного режима работы блочного шифра таким образом, чтобы ключ, с помощью которого происходит непосредственное преобразование данных, периодически изменялся по ходу обработки одного сообщения. Применение подхода internal re-keying приводит к изменению порядка обработки единицы работы режима.

Таким образом, данный подход не предполагает рассмотрение режима работы шифра как черного ящика, а затрагивает внутренние особенности его строения (отсюда термин «internal»). В результате применения подхода internal re-keying образуется новый класс расширенных режимов с внутренним преобразованием ключа (internally re-keyed mode of operation), причем конкретный вид преобразования зависит от используемого базового режима. Пожалуй, первый режим работы блочного шифра с использованием internal re-keying был описан в документе RFC 4357, хотя в то время такого понятия как internal re-keying не существовало, как и открытых работ, посвящённых исследованию криптографических свойств описанных режимов.

Понятие «internal re-keying» неразделимо с понятием «секция». Секция – это подстрока сообщения, обрабатываемая на одном ключе до его преобразования, при этом такой ключ будем называть секционным. Размер секции является параметром расширенного режима работы шифра. Он должен фиксироваться с учетом требований к уровню стойкости и эффективности. Сложность выбора состоит в сохранении баланса: чем чаще меняется ключ по ходу обработки одного сообщения, тем выше уровень стойкости, но меньше скорость.

Основную идею механизма internal re-keying можно проиллюстрировать как представлено на рисунке 1.

Здесь каждое отдельное сообщение делится на секции длины N блоков каждая. Первая секция каждого сообщения обрабатывается на начальном ключе K. Перед обработкой каждой следующей секции текущий секционный ключ преобразуется по некоторому определенному алгоритму.

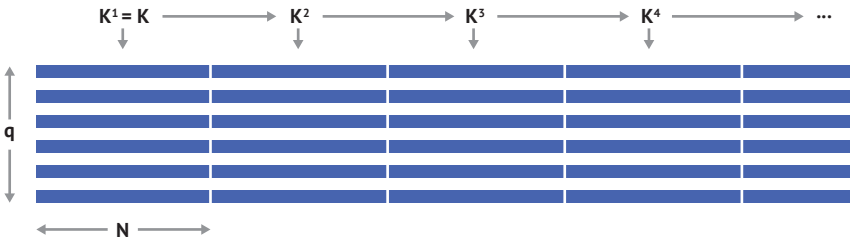


Рисунок 1

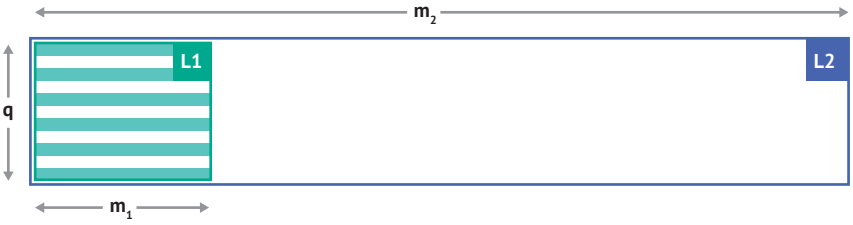


Рисунок 2

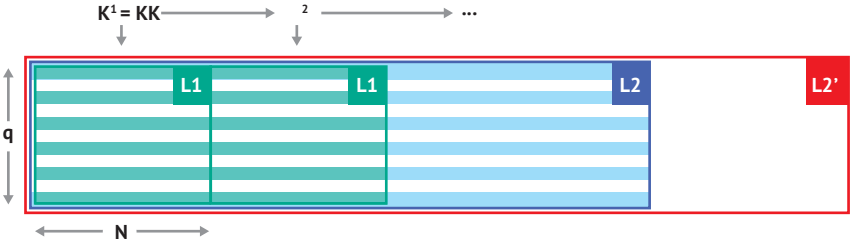


Рисунок 3

Примечание: вообще говоря, на начальном ключе K шифрование может и не осуществляться. Он может использоваться лишь для порождения последовательности секционных ключей. В таком случае его называют мастер-ключом.

С основной идеей internal re-keying мы ознакомились. Но действительно ли он решает поставленную нами выше проблему эффективной и «безопасной» обработки большого количества данных?

Сравним некоторый расширенный режим с его режимом-прообразом — тем же режимом, но без использования internal re-keying, на предмет ограничений по нагрузке на ключ.

Для начала рассмотрим режим-прообраз. Предположим, что допустимая нагрузка на ключ L1, соответствующая ограничениям по побочным каналам, позволяет обрабатывать q сообщений длины m1 блоков. В то же время допустимая нагрузка на ключ L2, соответствующая комбинаторным ограничениям, при том же количестве сообщений q позволяет обрабатывать сообщения длины m2. Таким образом, для режима-прообраза итоговая допустимая нагрузка на ключ соответствует самому строгому из ограничений L1, а максимальная длина сообщения равна m1 (рис. 2).

Теперь рассмотрим расширенный режим с внутренним преобразованием ключа (рис. 3).

Информация, получаемая по побочным каналам, имеет отношение только к ключу, на котором непосредственно обрабатывается сообщение. Если используется такой алгоритм преобразования ключа, что секционные ключи для противника являются «почти» случайными и независимыми, то каждое изменение ключа приводит к тому, что информация о предыдущем ключе к противнику больше не поступает. Поэтому, выбрав размер секции N таким образом, что $q \cdot N \leqslant L1$, можно больше не думать об ограничениях по побочным каналам и сфокусироваться только на комбинаторных ограничениях. Как правило, комбинаторные свойства новых режимов с использованием подхода

internal re-keying только улучшаются, что должно подтверждаться строгими доказательствами (см., к примеру, [1]). Следовательно, при том же уровне стойкости новая допустимая нагрузка на ключ L2', соответствующая комбинаторным ограничениям, в разы увеличивается в сравнении со старой допустимой нагрузкой L2.

Для наглядности рассмотрим пример. Пусть для некоторого режима-прообраза в протоколе P зафиксированы следующие нагрузки на ключ: L1 = 128 МБ, L2 = 1 ТБ. Тогда, если мы хотим обработать, к примеру, 128 сообщений, их длина не должна превышать L1/128 = 1 МБ. Если же расширить этот режим с помощью internal re-keying с размером секции N = 1 МБ, то при том же общем числе сообщений длина каждого сообщения может быть увеличена до нескольких терабайтов.

Но что же это за «определенный алгоритм», по которому преобразуется ключ? Как уже было сказано ранее, этот алгоритм зависит от базового режима, поэтому в качестве примера рассмотрим алгоритм преобразования ключа ACPKM («ACPKM» = «Advanced Cryptographic Prolongation of Key Material»), который применяется к режиму шифрования CTR.

Сообщение разбивается на секции, и в качестве ключа первой секции используется начальный ключ K. Для зашифрования (i+1) секции значение (i+1)-ого секционного ключа вычисляется с помощью i-ого ключа следующим образом (на примере блочного шифра Кузнечик):

Ki+1 = EKi(W1) | EKi(W2),

где W1 и W2 – некоторые константные строки, а операция «|» – конкатенация. То есть для получения нового ключа достаточно преобразования двух блоков на предыдущем ключе. Согласитесь, это гораздо проще, чем заново согласовывать ключ.

Таким образом, internal re-keying позволяет в разы увеличить допустимую нагрузку на ключ, практически не снижая эффективности.

Internal re-keying более всего подходит для использования в протоколах, где обрабатываются сообщения большого размера, например, CMS-сообщения, так как он позволяет достичь существенный выигрыш именно в длине сообщений, а не в количестве.

Если вас интересует существенное увеличение именно количества сообщений, читайте следующий раздел.

Внешнее преобразование ключа external re-keying

Основным отличием external re-keying от определённого выше подхода internal re-keying является то, что ключ меняется не в процессе обработки одного сообщения, а после обработки некоторого количества целых сообщений. Применение данного подхода не влияет на внутреннее строение режима и не меняет порядка обработки отдельных сообщений – тех самых «единиц» работы режима. То есть external re-keying может рассматриваться в качестве «режима использования режима» (режим с точки зрения external re-keying – это чёрный ящик).

Следствием этого является безусловный плюс данного подхода – конкретные алгоритмы преобразований ключа, применяемые в рамках external re-keying, могут использоваться совместно с любыми режимами работы шифра.

Впервые криптографические свойства данных конструкций были исследованы в работе Абдалы и Белларе, в которой совокупность алгоритма преобразования ключа и режима работы шифра в рамках подхода external re-keying рассматривается, как расширенный режим с внешним преобразованием ключа (по аналогии, externally re-keyed mode of operation). Такая точка зрения вполне оправдана – задачи, решаемые классическим и расширенным режимами, одинаковы.

Основная идея механизма external re-keying проиллюстрирована на рисунке 4.

Из начального ключа K по некоторому определённому алгоритму вырабатывается последовательность подключей K^i – ключей, с помощью которых будут непосредственно обрабатываться сообщения. Аналогом понятия «секция» для расширенного режима с внешним преобразованием ключа является количество сообщений, которое можно обрабатывать на одном подключе. Для упрощения понимания будем считать, что каждый из подключей K^i может применяться для обработки максимум h сообщений длины m блоков.

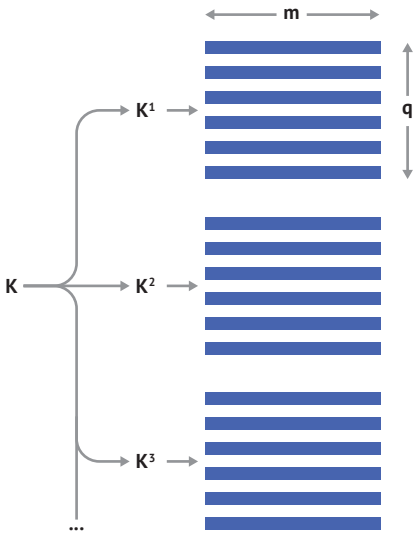


Рисунок 4

Примечание: выделяют несколько способов получения ключей обработки данных из начального ключа: с мастер-ключом, который никогда не используется непосредственно для обработки данных, и без него, параллельный и последовательный способы.

По аналогии с подходом internal re-keying убедимся в том, что external re-keying также решает проблему эффективной и «безопасной» обработки большого количества данных.

Ситуация, при которой мы просто шифруем данные, не пользуясь подходом external re-keying, представлена на рисунке 5.

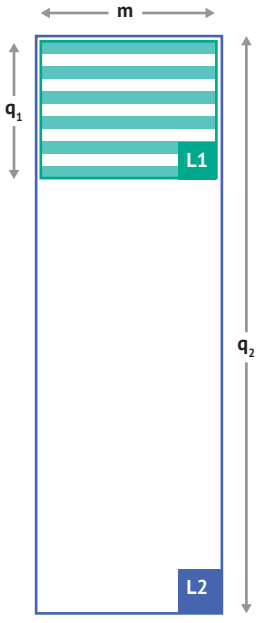


Рисунок 5

Здесь L1 и L2 — допустимые нагрузки, соответствующие ограничениям по побочным каналам и комбинаторным ограничениям соответственно, а q1 и q2 — количества сообщений длины m, которые мы можем безопасно обработать при данных допустимых нагрузках. Таким образом, итоговая допустимая нагрузка на ключ без использования external re-keying равна L1, а обработать мы можем лишь q1 сообщений.

Теперь применим подход external re-keying (рис. 6).

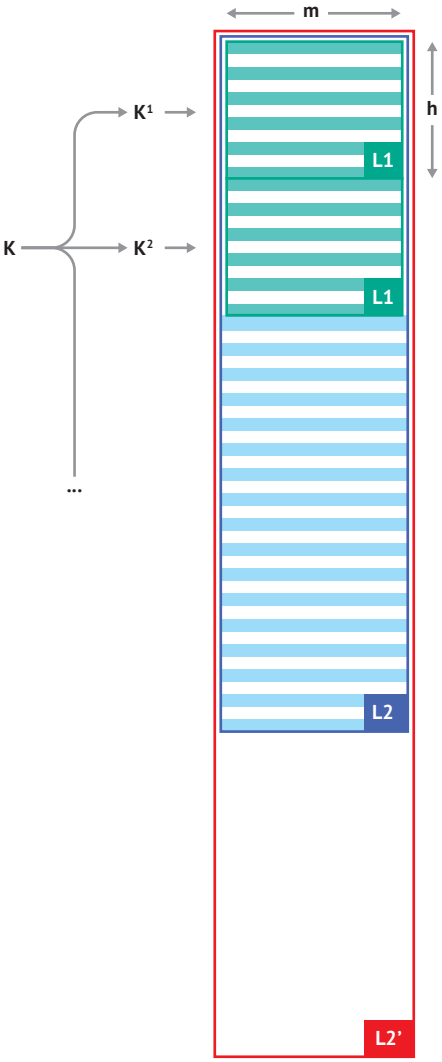


Рисунок 6

Приведённые выше рассуждения об информации, получаемой по побочным каналам, справедливы и для подхода external re-keying. Поэтому, выбирая параметр h таким образом, что h • m ⩽ L1, можно учитывать только допустимую нагрузку L2›, соответствующую комбинаторным ограничениям. Согласно все той же работе Абдалы и Беллареа нагрузка L2› в разы увеличивается в сравнении с допустимой нагрузкой L2.

Для наглядности рассмотрим пример. Пусть для некоторого режима в протоколе P зафиксированы следующие нагрузки на ключ: L1 = 128 МБ, L2 = 1 ТБ. Если мы хотим обработать сообщения длины 1 МБ каждое, их количество не должно превышать 128. Если же расширить этот режим с помощью external re-keying, то при той же длине количество сообщений может быть увеличено в десятки тысяч раз.

Так как алгоритмы преобразования ключа, разрабатываемые в рамках подхода external re-keying, могут применяться с любыми режимами работы шифра, мы можем их рассматривать без привязки к последним. Приведем пример конкретного алгоритма получения t ключей обработки из начального ключа K для шифра Кузнечик:

K1 | K2... | Kt = EK([0]) | EK([1]) | ...|EK([2t-1]),

где [i] — строка длины 128 бит, которая является двоичным представлением числа i. Таким образом, для получения t ключей надо зашифровать всего лишь 2t констант.

Преобразование ключа в рамках подхода external re-keying планируется к применению в протоколе TLS 1.3 (к примеру, в процедуре Key Update), который служит для передачи большого числа сообщений небольшой длины.

В теории все хорошо, а что на практике?

Итак, мы рассмотрели два подхода re-keying: внутреннее и внешнее преобразования ключа. Так как internal re-keying порождает новый класс режимов шифрования, а external re-keying определяет порядок их использования, выделяется и третий подход, объединяющий в себе достоинства последних.

Таким образом, можно прийти к следующей структуре взаимодействия блочного шифра, режимов его работы и подходов к преобразованию ключа (рис. 7).

Несмотря на то, что понятия external re-keying и internal re-keying сформировались относительно недавно, оба подхода уже давно успешно применяются на практике. Так сложилось, что в зарубежной криптографии практикуют преобразование ключей в рамках подхода external re-keying (например, протокол TLS 1.3), в то

Рисунок 7

время как у нас в стране широко распространено применение расширенных режимов с внутренним преобразованием ключа (internal re-keying).

Напомним, что в отечественном варианте протокола TLS 1.0 используется подход internal re-keying, а в разрабатываемой новой версии TLS 1.2 планируется совместное применение двух подходов. Более того, использование подхода internal re-keying совместно с ключевым деревом в качестве механизма external re-keying используется в российской версии протокола IPsec.

Разработка специалистами нашей компании нового поколения расширенных режимов с внутренним преобразованием ключа послужила толчком не только к созданию документа новых методических рекомендаций ТК 26, но и к началу работы над документом, который бы, наконец, ввёл понятную классификацию и стал единой базой существующих «безопасных» подходов преобразования ключа. Объединив свои усилия вместе с зарубежными коллегами, мы начали разработку проекта RFC, в котором можно будет найти описание всего спектра механизмов преобразования ключа, а также полезные рекомендации по их применению.

Информационные технологии и коммуникационные системы

Компания ИнфоТеКС – признанный лидер рынка информационной безопасности России. Уже на протяжении 25 лет компания успешно решает амбициозные и сложные задачи в сфере защиты данных. Основана в 1991 году.

ИнфоТеКС входит в ТОП-5 крупнейших компаний России в сфере защиты информации (согласно рейтингу CNews).

Флагманской разработкой компании является технология ViPNet — гибкое VPN-решение для безопасной передачи данных в защищ`нной сети. Сегодня ViPNet — самое масштабируемое и над`жное решение на российском рынке информационной безопасности.

Торговая марка ViPNet объединяет целый ряд продуктов и сетевых решений для крупного, среднего и малого бизнеса и включает::

- программные и программно-аппаратные средства организации виртуальных частных сетей (VPN) и инфраструктуры открытых ключей (PKI);
- средства межсетевого экранирования и персональные сетевые экраны;
- средства шифрования данных, которые хранятся и обрабатываются на компьютерах и в сети;
- системы централизованного управления и мониторинга СЗИ;
- средства криптографической защиты информации для встраивания в прикладные системы сторонних разработчиков (системы юридически значимого документооборота, порталы и т. п.);
- программно-аппаратные комплексы (или самостоятельные сетевые устройства) обнаружения компьютерных атак ViPNet IDS.

В ГК ИнфоТеКС входит 4 компании: «ИнфоТеКС Интернет Траст» (услуги защиты информации, в том числе в области систем электронного документооборота); «Перспективный мониторинг»; ООО «Системы практической безопасности» и НОЧУ ДПО «Учебный центр ИнфоТеКС», который сотрудничает с ведущими вузами страны. Совокупный оборот компании превышает 4 млрд рублей, количество сотрудников – более 1000 человек.

Система менеджмента качества ИнфоТеКС сертифицирована по международному стандарту ISO 9001:2008. Продукты ИнфоТеКС регулярно проходят сертификацию в ФСБ России и ФСТЭК России, а также в отраслевых системах сертификации.

infotecs®

«ИнфоТеКС» www.infotecs.ru

Календарь мероприятий

28 марта
Москва • Конференция
**BIG DATA 2018
VII Всероссийский форум**

29 марта
Киев • Конференция
Blockchain & Bitcoin Conference Kyiv

29 марта
Москва • Конференция
Epic Growth Conference

30–31 марта
Киев • Конференция
JS Fest

30 марта
Санкт-Петербург • Конференция
Digital Spring 2018

31 марта –1 апреля
Москва • Фестиваль
MosCode Festival

31 марта –1 апреля
Санкт-Петербург • Тренинг
Методы, технологии и инструменты обучения персонала в технических, продуктовых и IT-компаниях

5 апреля
Бишкек • Конференция
ИТ-форум BIT-2018

6–7 апреля
Москва • Конференция
Java-конференция JPoint 2018

11 апреля
Санкт-Петербург • Конференция
ИТ-форум BIT-2018

14 апреля
Санкт-Петербург • Конференция
ProfsoUX 2018

14–15 апреля
Санкт-Петербург • Тренинг
«Руководство проектами в IT»: Управление требованиями 9

17 апреля
Санкт-Петербург • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

18–20 апреля
Санкт-Петербург • Конференция
X Общероссийская молодежная научно-техническая конференция «Молодежь. Техника. Космос»

18–20 апреля
Горки-10 • Форум
РИФ 2018

19 апреля
Нижний Новгород • Курс
Семинар о новых возможностях TrueConf Server 4.3.9

23–27 апреля
Санкт-Петербург • Конференция
Системный и бизнес анализ в разработке ПО. Интенсивный курс

24 апреля
Москва • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

26 апреля
Киев • Конференция
Blockchain Summit Kyiv 2018

26 апреля
Санкт-Петербург • Конференция
CPA Life 2018 — 5-ая юбилейная конференция по Интернет-рекламе и партнерскому маркетингу

11–12 мая
Санкт-Петербург • Конференция
Конференция HR API 2.0

12–13 мая
Санкт-Петербург • Тренинг
«Руководство проектами в IT»: Составление плана проекта. Ведение проекта

13–18 мая
Санкт-Петербург • Курс
Семинар по системной биологии

15 мая
Ростов-на-Дону • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

17–18 мая
Москва • Конференция
DevGAMM Moscow 2018

17 мая
Краснодар • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

23–24 мая
Москва • Выставка
ECOM Expo 2018 — крупнейшая в Восточной Европе выставка ecommerce-технологий

24–25 мая
Казань • Конференция
IT&SECURITY FORUM

26 мая
Минск • Конференция
Voxxed Days Minsk

2 июня
Санкт-Петербург • Турнир
Турнир по картингу «IT Race #5»

5–6 июня
Санкт-Петербург • Выставка
Выставка-форум «Передовые Технологии Автоматизации. ПТА — Санкт-Петербург 2018»

16–17 июня
Санкт-Петербург • Тренинг
«Руководство проектами в IT»: Управление рисками проекта

30 июня
Санкт-Петербург • Турнир
Voxxed Days Minsk Турнир по кикеру «IT's KICKER #5»

14–15 июля
Санкт-Петербург• Тренинг
«Руководство в проектами IT»: Завершение проекта. Проведение ретроспективы проекта

8 сентября
Санкт-Петербург • Турнир
Велотурнир «IT Bike Fest #5»

18 сентября
Екатеринбург • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

20 сентября
Челябинск • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9k

22 сентября
Санкт-Петербург • Турнир
Беговая эстафета «IT Run #3»

25 сентября
Тюмень • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

27 сентября
Ханты-Мансийск • Тренинг
Семинар о новых возможностях TrueConf Server 4.3.9

13 октября
Санкт-Петербург • Турнир
Турнир по шахматам «IT Chess #5»

18 октября
Москва • Конференция
Видео+Конференция 2018

24 ноября
Санкт-Петербург • Турнир
Турнир по мини-футболу «IT Goal #5»

27–29 ноября
Екатеринбург • Выставка
Выставки по автоматизации и электронике «ПТА-Урал 2018» и «Электроника-Урал 2018»

КРИПТОПРО

Сервер электронной подписи (СЭП) КриптоПро DSS для интернет-банкинга

обеспечивает удобный «облачный» сервис создания электронной подписи в интересах пользователей

Нет необходимости установки средства ЭП на каждое рабочее место пользователя

Существенное снижение совокупной стоимости владения (TCO) инфраструктурой ЭП

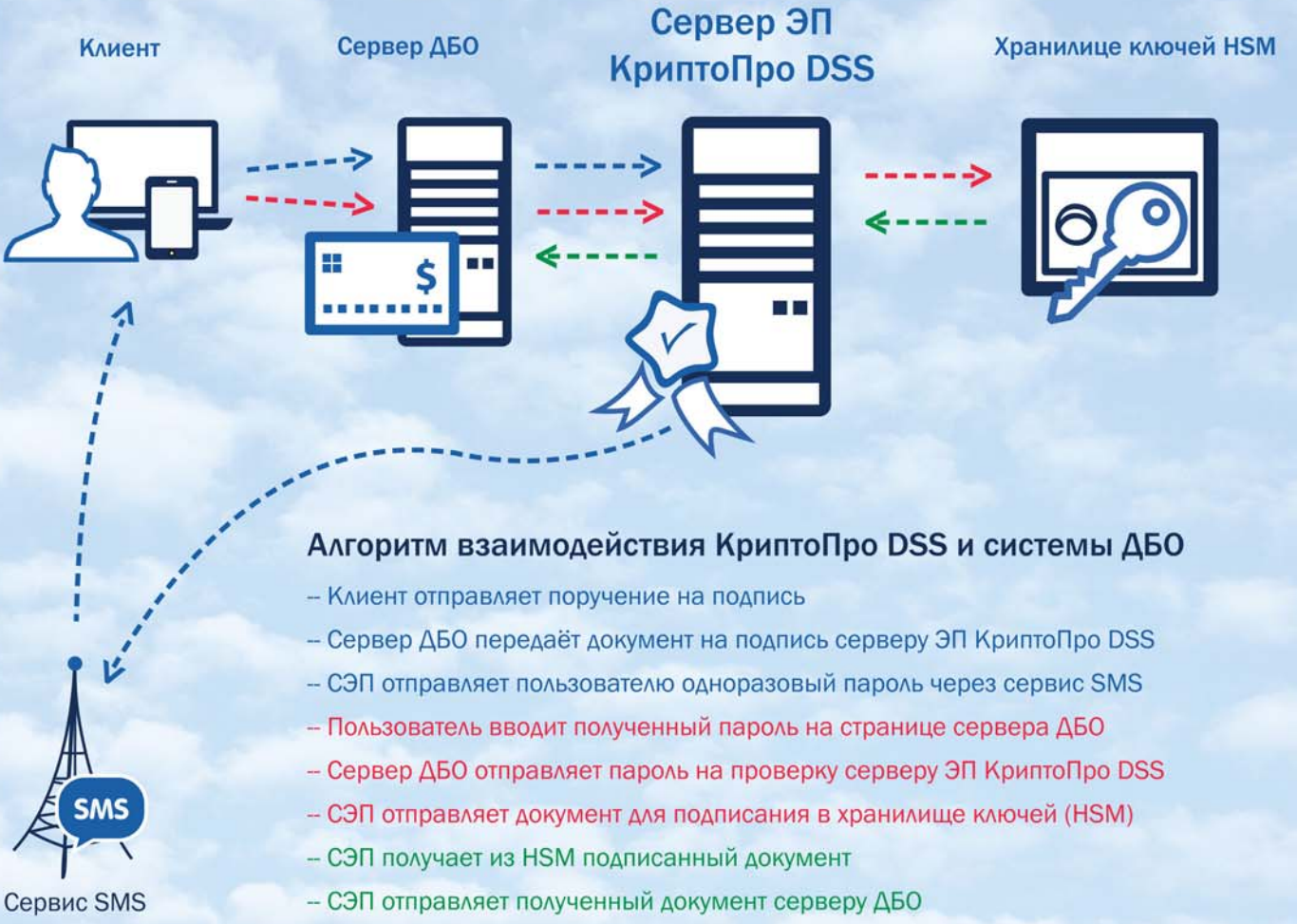
СЭП КриптоПро DSS поддерживает

Любые устройства

Любые платформы

Любые браузеры

Различные схемы аутентификации



Алгоритм взаимодействия КриптоПро DSS и системы ДБО

-- Клиент отправляет поручение на подпись
-- Сервер ДБО передаёт документ на подпись серверу ЭП КриптоПро DSS
-- СЭП отправляет пользователю одноразовый пароль через сервис SMS
-- Пользователь вводит полученный пароль на странице сервера ДБО
-- Сервер ДБО отправляет пароль на проверку серверу ЭП КриптоПро DSS
-- СЭП отправляет документ для подписания в хранилище ключей (HSM)
-- СЭП получает из HSM подписанный документ
-- СЭП отправляет полученный документ серверу ДБО

+7 (495) 995-48-20 info@cryptopro.ru www.cryptopro.ru