ЗАМЕЩЕНИЕ ГОРЫ

WINDOWS НЕЗАМЕНИМ, НО ЗАМЕНЯТЬ НАДО. КАК?

Сергей ШАЛИМОВ
руководитель направления по работе с технологическими партнерами «Аладдин Р.Д.»

Традиционно банки ориентировались на лидеров мирового рынка и самые высокотехнологичные решения. Сейчас сложилась непростая ситуация: уход с рынка вендоров, отказ в техподдержке и обновлениях, с одной стороны; с другой стороны, как следствие этого возникли ограничения со стороны регулятора — объявлено о приостановке ряда сертификатов ФСТЭК России. При этом банковские системы оказались между двух огней. Рассмотрим варианты оперативного выхода из таких непростых и недружественных условий.

ЕЩЁ НЕ ОДИН ГОД...

Многие эксперты дают оценки, что в России более 90% ИС построены на продуктах семейства Windows.

Чаще всего сервис генерации и управления цифровыми сертификатами (сертификаты доступа, PKI-инфраструктура) базируется на Windows Active Directory (далее AD), глубоко интегрированным с AD центром сертификатов Microsoft Certification Authority. Широко используются веб-серверы IIS и базы данных Microsoft SQL или Oracle. Подавляющее количество приложений написано под Windows. Такая ситуация не является благоприятной для экстренной миграции на открытую платформу на базе ядра Linux, на которой базируется большинство отечественных решений.

Ещё не один год в период поэтапного перехода банковские ИС будут содержать два корпоративных домена — один под управлением сервера Windows и второй под управлением сервера Linux. Для увязывания и обеспечения непрерывности работы ИС нужны рабочие инструменты и плавный (так называемый «бесшовный») переход на платформу Linux.

Компания «Аладдин Р. Д.» в сотрудничестве с отечественными разработчиками операционных систем и баз данных уже несколько лет работает над комплексной экосистемой безопасных продуктов. Коллеги сфокусировались на импортозамещении AD и СУБД такими решениями, как Samba DC или FreeIPA (Astra Linux ALD Pro), СУБД Postgres Pro или Jatoba, при этом достаточно успешно решают задачи работоспособности сервисов и доступности информационных активов. Мы, взаимодействуя на этапах проектирования и разработки российских дистрибутивов на Linux и отечественных СУБД, интегрируем в них наши компоненты ИБ. В настоящее время разработан уже целый пул продуктов и методик внедрения плавной бесшовной миграции всех ресурсов на отечественные «рельсы».

ЧЕМ ЗАМЕНИТЬ MICROSOFT CA?

Одна из основных задач при организации доверенной внутрикорпоративной среды — создание домена доверия, функционально не уступающего импортному, как правило, Microsoft.

В отличие от домена на базе Microsoft AD DS, в отечественных решениях для построения доменов нет встроенного центра сертификатов, такого как Microsoft CS. Разработчики компании «Аладдин Р.Д.» сосредоточились на замещении средств аутентификации, инфраструктуры PKI и организации единого входа (SSO). Эта работа велась на уровне проектирования и разработки решений, т.е. так же, как и у Microsoft, мы ставили задачу тесной интеграции служб организации домена и центра сертификации. В итоге разработали одно из возможных решений для импортозамещения –отечественный корпоративный центр выдачи и обслуживания сертификатов доступа Aladdin Enterprise Certificate Authority (Aladdin eCA), способный заменить импортный Microsoft CS. Aladdin Enterprise Certificate Authority (Aladdin eCA) — сервер на базе отечественных ОС, обеспечивающий управление цифровыми сертификатами (ЦС) пользователей и техническими средствами информационной системы (выпуск, распространение, аннулирование, приостановка, возобновление).

Aladdin Enterprise Certificate Authority (Aladdin eCA) — сервер на базе отечественных ОС, обеспечивающий управление цифровыми сертификатами (ЦС) пользователей и техническими средствами информационной системы (выпуск,

Одна из основных задач при организации доверенной внутрикорпоративной среды — создание домена доверия, функционально не уступающего импортному

распространение, аннулирование, приостановка, возобновление).

Aladdin eCA, основанный на технологии открытых ключей (PKI), — это решение «из коробки», с которым легко разворачивать домены безопасности и обслуживать цифровые сертификаты контроллеров доменов, серверов, сетевого оборудования и АРМ пользователей. Aladdin eCA глубоко интегрирован со службами глобальных каталогов, что позволяет обеспечить непрерывность и связанность сервисов при миграции.

Aladdin eCA может обеспечить замену Microsoft CA в корпоративных и государственных информационных системах. Он может применяться в ГИС до 1-го класса защищённости включительно, ИСПДн до 1-й категории включительно, на объектах КИИ до 1-й категории включительно, а также в АСУ ТП на критически важных объектах, потенциально опасных объектах до 1-го класса защищённости включительно.

ПРО ОТЕЧЕСТВЕННУЮ PKI

В банковской сфере обслуживание клиентов тесно связано с удалённым доступом к информационным ресурсам, в котором применяется не менее чем двухфакторная усиленная аутентификация, а в расширенном пакете услуг — квалифицированная электронная подпись, строгая аутентификация с применением различных факторов аутентификации, в том числе и биометрических.

На рынке аутентификации наблюдается приостановка деятельности, а также не исключён и потенциальный уход с российского рынка ряда крупнейших западных вендоров (Vasco, Yubico, Thales, EMC и др.). Что можно использовать взамен?

Представим одно из возможных решений. Это отечественный продукт, разработанный «Аладдин Р. Д.», — высокопроизводительный сервер аутентификации JAS (JaCarta Authentication Server) с поддержкой как аппаратных OTP- и U2F-токенов, так и программных OTP/PUSH/SMS-аутентификаторов. JAS поддерживает генерацию программных OTP с помощью приложения на смартфоне, передачи через СМС или Push, а также поддерживает все известные «железные» токены-брелоки с кнопкой или экраном для генерации OTP по стандартам RFC4226 (HOTP) и RFC6238 (TOTP), USB-токены, например JaCarta WebPass, любые U2F-токены, например JaCarta U2F из достаточно широкого семейства JaCarta.

На рынке аутентификации наблюдается приостановка деятельности, а также не исключён и потенциальный уход с российского рынка ряда крупнейших западных вендоров (Vasco, Yubico, Thales, EMC и др.). Что можно использовать взамен?

JAS обеспечивает безопасный механизм передачи секрета для инициализации генератора OTP в приложении Aladdin 2FA, при этом позволяет работать и с любыми другими приложениями типа Google Authenticator, «Яндекс. Ключ» в стандартном режиме.

Основные преимущества JAS — это простота внедрения, поддержка самых распространённых прикладных сервисов, удобный и понятный личный кабинет для пользователя, универсальное мобильное приложение Aladdin 2FA.

Также JAS сертифицирован ФСТЭК России на соответствие уже новым требованиям на УД-4, что позволяет использовать его для защиты информации в ИСПДн до 1 уровня включительно и при создании автоматизированных ИС до класса защищённости 1Г включительно.

БЕЗОПАСНАЯ РАБОТА С БД

Безопасная работа с базой данных (БД) — это краеугольный камень безопасности любой ИС. В банковской сфере невозможно оставаться в современном состоянии, когда самые распространённые продукты MS SQL и Oracle оказались под прицелом недружественных отношений с вендорами, а утечка данных может стать невосполнимой потерей. Основная отечественная платформа замещения СУБД представлена продуктами PostgreSQL и PostgresPro.

Для защиты баз данных от возможных утечек при миграции с MS SQL и Oracle на отечественные СУБД используется система «Крипто БД». Даже если переезд, например, с Oracle невозможен, как в случае с большими базами данных, «Крипто БД» позволяет остаться на этой платформе, заменяя встроенные в Oracle средства защиты сертифицированными российскими. Система также изолирует обрабатываемые данные от самой СУБД, предотвращая их утечку.

«Крипто БД» поддерживает сразу несколько платформ баз данных, что позволяет защитить информацию в исходной СУБД (например, Oracle или MS SQL) и одновременно в новой, строящейся (например, Postgres Pro или PostgreSQL).

Защитные механизмы «Крипто БД» основаны на стойких отечественных криптоалгоритмах, в БД защищаются таблицы или отдельные

столбцы, реализованы методы «прозрачного» шифрования. Продукт соответствует всем требованиям ФСБ России к СКЗИ, что подтверждено соответствующими заключениями ФСБ России по классам КС1, КС2 и КС3. Это позволяет системе защиты обеспечивать противодействие наиболее критичным угрозам — нарушению целостности и конфиденциальности информации. Чаще всего в банках это персональные данные сотрудников и клиентов.

Основные сценарии применения «Крипто БД» могут реализовать такие задачи, как защита конфиденциальной информации в СУБД при взломах информационных систем, предотвращение доступа со стороны привилегированных пользователей, разграничение прав доступа пользователей к защищаемой информации, маскирование и деперсонализация информации в СУБД, предотвращение возможности восстановления удалённой информации, аудит фактов доступа пользователей к защищаемой информации и другие.

ПРО БЕЗОПАСНОСТЬ РАБОЧИХ МЕСТ

Перевод автоматизированных рабочих мест (АРМ) сотрудников на отечественное ПО с использованием платформы Linux также сопряжён с вопросами информационной безопасности. Одно из возможных решений для данной задачи — клиентское ПО SecurLogon, которое позволяет добавить недостающие компоненты на клиентские ОС и автоматически сконфигурировать клиентские АРМ для задач единого входа в различных вариантах построения доменов — Samba DC, FreeIPA, Microsoft AD, что максимально соответствует политике сохранения разных доменов в период миграции.

Aladdin SecurLogon также позволяет реализовать двухфакторную аутентификацию в разных инфраструктурах, добавить аутентификацию по цифровым сертификатам в такие распространённые протоколы и сервисы, как SSH, RDP, почтовые клиенты, браузеры, подпись и доступ в СЭД. Для больших инсталляций остро стоит задача автоматической централизованной конфигурации клиентских АРМ, так как привычных групповых политик в Linux пока ещё нет. С помощью Aladdin SecurLogon можно автоматизировать настройку АРМ и организовать до 1000 АРМ за 20 минут.

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Для защиты данных на дисках в Windows многие используют встроенную функцию шифрования BitLocker, рискуя полностью потерять к ним доступ. Оперативно обезопасить информацию на дисках рабочих станций и серверов способны продукты линейки Secret Disk — система прозрачного шифрования данных для Windows и Linux. Эти отечественные разработки развиваются в течение всего периода действия программы импортозамещения. Основа ПО — крипто-ядро SDCE, сертифицированное ФСБ России (КС1, КС2), код механизмов защиты не содержит чужеродные включения.

Aladdin SecurLogon также позволяет реализовать двухфакторную аутентификацию в разных инфраструктурах, добавить аутентификацию по цифровым сертификатам в такие распространённые протоколы и сервисы, как SSH, RDP, почтовые клиенты, браузеры, подпись и доступ в СЭД

Оперативная замена импортных средств шифрования отечественным Secret Disk для ОС Windows (Secret Disk 5) снимет остроту проблемы защиты данных, поскольку его внедрение занимает считанные минуты. Это позволит сохранить данные от утечки по техническим каналам встроенными механизмами Microsoft. В случае перехода на ОС на базе ядра Linux защиту обеспечит продукт Secret Disk Linux.

Новый продукт Secret Disk Linux поддерживает лидирующие отечественные ОС — Astra Linux SE1.7, РЕД ОС 7.3 и 7.3.1. Он обеспечивает шифрование виртуальных дисков, прозрачное шифрование информации, двухфакторную аутентификацию пользователей на базе алгоритма ЭП ГОСТ Р 34.10–2018, разграничение прав доступа.

При таком способе перехода применяются единые технологии защиты в ОС Windows/Linux, что поддерживает бесшовную интеграцию разнородных систем и возможность использования единой системы управления в гетерогенной среде.

ЗАКЛЮЧЕНИЕ

Представленные в статье решения помогут оперативно организовать безопасную среду для корпоративной информационной системы, обеспечить переход на доверенные средства аутентификации, безопасную работу СУБД как отечественных, так и иностранных поставщиков, а также поэтапно осуществить бесшовный перевод пользователей на отечественные продукты, обеспечив надёжную защиту информации.