АУТЕНТИФИКАЦИЯ

ОТ ПАРОЛЕЙ К АДАПТИВНОЙ МФА

Сергей ГРУЗДЕВ
генеральный директор «Аладдин Р.Д.»

МЕНЯЕТСЯ МИР, МЕНЯЮТСЯ ТРЕБОВАНИЯ

После начала СВО Россия столкнулась с беспрецедентным ростом атак на информационные системы (ИС) организаций – как государственных, так и бизнеса.

Что обычно происходит после успешной атаки (инцидента ИБ)? Начинается борьба с её последствиями, выделение денег на закупку и внедрение новых систем мониторинга, антивирусов, DLP, ИИ и других модных продуктов и технологий, а не устранение причин, приведших к инциденту.

Причины же большинства инцидентов банальны – слабая, неправильно реализованная система идентификации и аутентификации в ИС.

Увы, этот сегмент ИБ – самый консервативный, нормативная база здесь не менялась десятилетиями.

ПАРОЛИ

Существующая нормативная база предписывает использование для аутентификации пользователей в ИС паролей – не менее 6-ти символов при мощности алфавита 30 символов для ИС 4-го класса защищённости, не менее 8-ми символов при мощности алфавита не менее 70 символов для ИС 1-го класса защищённости, а также смену пароля через каждые 6 мес. и 1 мес. соответственно.

Насколько это надёжно сегодня? Оценки времени, затрачиваемого на прямую атаку – прямой перебор всех возможных вариантов пароля (brute force) при использовании домашнего компьютера с 12-ю графическими картами RTX 5090, приведены в таблице 1[1].

Из таблицы видно, что использование пароля менее 8-ми символов, набранного без использования цифр и/или служебных символов недопустимо. Таким образом, действующие тре-

[1] По материалам https://www.hivesystems.com/blog/are-your-passwords-in-the-green.

бования к паролю для ИС 4-го класса защищённости безнадёжно устарели в случае, если имеется возможность машинного перебора.

А если увеличить мощность вычислительного ресурса и использовать облачный ресурс, например, Amazon (AWS) или ChatGPT-4?

8-ми символьный пароль с использованием прописных, заглавных букв, цифр и спецсимволов ломается за 5 часов.

Становится очевидно – от паролей надо отказываться, либо значительно усиливать требования к ним, увеличивая их длину (не менее 11-ти символов) и мощность алфавита (количество используемых букв в разных регистрах, цифр и символов).

А теперь давайте вспомним 2020–2021 гг., когда мы сидели на удалёнке. С чем мы столкнулись? С тем, что пользователи, выучив свой сложный пароль для доступа в корпоративную ИС, не сильно задумываясь о последствиях вводили его при заказе пиццы, в различных сервисах и соцсетях. Потом эти чужие сервисы ломали, пароли массово утекали в сеть, а затем уже попадали в объединённые базы типа Collection #2–5 (25 млрд учётных записей и паролей к ним). В результате там оказывалось до 7–10% наших сотрудников со своими актуальными паролями к корпоративным ресурсам.

Тот самый пресловутый человеческий фактор...

«Честными» – правильными и действительно стойкими паролями (выбранными случайно равновероятно из слов заданной длины используемого алфавита) практически никто не пользуется, запомнить их нереально, поэтому люди пользуются парольными фразами или составными паролями на основе легко запоминаемых слов.

Но, если пароль содержит слово или большую его часть из словаря паролей, или такой пароль когда-то ранее был использован кем-то, учётная запись с этим паролем была взломана или украдена, то оценки времени взлома/подбора пароля выглядят уже совсем по-другому (Таблица 2).

Кол-во символов пароля	Только цифры	Прописные буквы (текст)	Прописные и заглавные буквы	Прописные и заглавные буквы + цифры	Прописные и заглавные буквы + цифры и спецсимволы
4	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
5	Мгновенно	Мгновенно	57 мин.	2 часа	4 часа
6	Мгновенно	46 мин.	2 дня	6 дней	2 недели
7	Мгновенно	20 часов	4 мес.	1 год	2 года
8	Мгновенно	3 недели	15 лет	62 года	164 года
9	2 часа	2 года	791 год	3K лет	11K лет
10	1 день	40 лет	41K лет	238K лет	803K лет

Таблица 1.

K-во символов пароля	Только цифры	Прописные буквы (текст)	Прописные и заглавные буквы	Прописные и заглавные буквы + цифры	Прописные и заглавные буквы + цифры + спецсимволы
...	...	...	...	...	...
17	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно
18	Мгновенно	Мгновенно	Мгновенно	Мгновенно	Мгновенно

Таблица 2.

Резюме:

◆ Надёжность защиты ИС с помощью правильных 8-ми символьных паролей типа *t~pbE#0u* (как предписывают нам нормативные требования)– это иллюзия, такая защита ломается примерно за 5 часов при стоимости аренды ресурсов ~$20.

◆ ***Про использование паролей для аутентификации в корпоративных ИС следует забыть и использовать более надёжную аутентификацию – усиленную или строгую.***

Теперь, чтобы двигаться дальше, нужно сделать шаг назад и обновить свои знания в области аутентификации.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Основные понятия идентификации и аутентификации и требования к их реализации определены в российских национальных стандартах, основные из них:

◆ ГОСТ Р 58833–2020 (Идентификация и аутентификация. Общие положения).

◆ ГОСТ Р 70262.1–2022 (Идентификация и аутентификация. Уровни доверия идентификации).

◆ ГОСТ Р 70262.2–2025 (Идентификация и аутентификация. Уровни доверия аутентификации).

Это основа, фундамент ИБ организации. Их нужно хорошо знать и руководствоваться именно ими, а не статьями из Интернет и рекомендациями новомодных систем ИИ, частенько выдающими откровенную чушь.

Идентификация. Идентификация пользователя – это процесс и способ установления и подтверждения личности пользователя – физического лица.

Идентификация всегда производится в два этапа: первичная и вторичная.

Во время первичной идентификации пользователя производится установление (распознавание) и подтверждение его личности, присваивание ему уникального идентификатора, регистрация в ИС, а также хранение и поддержание идентификационной информации в актуальном состоянии.

Во время вторичной идентификации пользователя в ИС осуществляется опознавание пользователя путем проверки предъявленного пользователем идентификатора. При положительном результате проверки производится переход к его аутентификации.

Вторичная идентификация является многократно повторяющимся процессом, осуществляющимся каждый раз при новом запросе пользователя на доступ к ресурсам ИС.

Уровни доверия идентификации определяют степень уверенности в правильности определения личности пользователя:

◆ Низкий (некоторая уверенность).

◆ Средний (достаточно высокая уверенность).

◆ Высокий (очень высокая уверенность).

Аутентификация пользователя – это процесс подтверждения (доказательства) подлинности пользователя и принадлежности ему предъявленного идентификатора.

Идентификация и аутентификация всегда неразрывны и используются вместе. Надёжность одного процесса существенно влияет (определяет) надёжность (уровень доверия) другого.

Цели аутентификации пользователей в ИС

1) Подтверждение личности пользователя (по предъявленному им идентификатору);

2) Установление доверительных отношений между участниками (сторонами) обмена:

◆ Аутентификация одной стороны (например, источника данных) – односторонняя аутентификация,

◆ Аутентификация обеих сторон (например, элементов ИТ-инфраструктуры) – взаимная аутентификация);

3) Предоставление доступа в ИТ-инфраструктуру или в ИС только «подлинным» пользователям;

4) Подтверждение личности и правомочности владельца ключа ЭП для проверки наличия полномочий на право создания электронной подписи и фиксации неотказуемости при выполнении процедуры создания электронной подписи электронного документа.

Достоверность результатов идентификации и аутентификации и уровень доверия ИС

Достоверность (корректность, правильность) результатов идентификации и аутентификации и уровень доверия ИС зависят от ряда параметров:

1) От уровня доверия первичной идентификации – полноты, качества предоставленных документов, подтверждений корректности и подлинности представленных документов и степени их связанности с личностью пользователя.

2) От уровня доверия аутентификации, определяемого видом аутентификации, характеризуемого:

◆ количеством одновременно применяемых факторов аутентификации (одно-, двух- или трёхфакторная аутентификация),

◆ используемыми протоколами аутентификации,

◆ организацией обмена аутентификационной информацией и доказательствами (односторонняя или взаимная аутентификация),

◆ используемыми средствами аутентификации.

3) От способов реализации аутентификации в ИТ-инфраструктуре и самой ИС (всего их 8 – локальная, прямая, доменная, иерархическая, распределённая сетевая, мостовая, браузерная и браузерная с трансляцией доверия).

4) От среды функционирования и места выполнения (замкнутая доверенная или недоверенная среда, внутри или вне защищённого периметра).

Уровень доверия ИС определяется достигнутым уровнем доверия идентификации и аутентификации и не может быть выше него. При этом определяющим является используемый вид аутентификации.

Их три (см. таблицу 3).

Простая аутентификация. Простая аутентификация может применяться в ИС с низким уровнем значимости информации и несущественным размером возможного ущерба в случае возникновения инцидента ИБ.

Особенности и примеры:

- ◆ Однофакторная
  - Пароль – запоминаемый и вводимый вручную (фактор знания общего с ИС секрета);
  - Одноразовый код доступа, присылаемый из ИС на зарегистрированное в ИС устройство пользователя;
  - Электронный идентификатор, не требующий ввода PIN-кода (фактор владения).
  - ***Использование биометрии в качестве единственного фактора аутентификации не допускается (например, лицо, голос или отпечаток пальца, снятый сканером, встроенным в компьютер пользователя).***
- ◆ Односторонняя – передача аутентификационной информации осуществляется в одном направлении – от пользователя к объекту доступа (ресурс ИС), при этом пользователь не может быть уверен, что получает доступ в нужную ему ИС, что её не подменили.

Усиленная аутентификация. Усиленная аутентификация должна применяться в ИС со средним уровнем значимости информации и существенным размером возможного ущерба.

Существенными условиями и отличиями от простой аутентификации являются:

- ◆ Использование двух факторов аутентификации (2ФА) – владения аппаратным устройством и знание пароля (секрета) или
- ◆ Использование двухэтапной проверки[2] – подтверждение личности пользователя с использованием фактора знания (долговременного пароля) и одноразового пароля (кода доступа), присылаемого пользователю на его зарегистрированный в ИС мобильный телефон SMS, push-уведомление, либо
- ◆ Одноразовый пароль (OTP), сгенерированный в приложении, установленном на мобильном телефоне пользователя на основе общего с ИС секретного ключа. Секретный ключ может быть загружен в приложение при инициализации, при сканировании QR-кода или другим способом. Технически сложной является задача безопасной передачи секрета в приложение, у многих она не решена, что сводит на нет всю безопасность.

Примеры:

- ◆ Google Authenticator (его использование противоречит российскому законодательству).
- ◆ Яндекс Ключ.
- ◆ Aladdin 2FA + корпоративный высокопроизводительный сервер аутентификации JAS (решена проблема безопасной передачи секрета на устройство пользователя).
- ◆ Аппаратные OTP-токены, U2F-токены (FIDO/FIDO-2), USB-токены, в защищённую память которых загружен файл-контейнер или сертификат, содержащий пользовательский идентификатор.
- ◆ Приложение на смартфоне, генерирующее и обслуживающее OTP-токены и др.

Опасность и особенности:

- ◆ Мобильный телефон, независимо от установленной ОС, является недоверенным и небезопасным.
- ◆ Один OTP-токен позволяет подключаться только к одной ИС, для работы с OTP-токенами на стороне ИС требуется сервер аутентификации.
- ◆ ***Перехват кодов доступа, извлечение из телефона секретного ключа для генерации OTP способно дискредитировать всю ИС и дать злоумышленникам доступ в неё под видом легальных пользователей (как в своё время было со взломом RSA SecurID).***

Уровень доверия ИС	Уровень доверия идентификации	Вид аутентификации
Низкий	Низкий	Простая
Средний	Средний	Усиленная
Высокий	Высокий	Строгая

Таблица 3.

Строгая аутентификация. Строгая аутентификация пользователей обязательна для применения в ИС с доменной архитектурой с высоким уровнем значимости информации и значительным размером возможного ущерба – для всех пользователей в ГИС класса защищённости К1, для привилегированных, удалённых пользователей, мобильных пользователей переносных устройств (ноутбуков), при обработке в ИС информации ограниченного доступа, для сотрудников подрядных организаций и их ИС, подключающихся к обслуживаемой ИС[3].

При строгой аутентификации должна применяться двух- или трёхфакторная взаимная аутентификация (2ФА/3ФА) с организацией двухстороннего обмена аутентификационной информацией между пользователем и объектом доступа, либо многостороннего обмена при использовании третьей доверенной стороны (корпоративного Центра Сертификации, выполняющего функции корпоративного «нотариуса»).

В процессе строгой аутентификации должны использоваться криптографические алгоритмы и протоколы аутентификации (например, Kerberos, TLS).

Третья доверенная сторона (Центр Сертификации) выполняет функции проверяющей стороны (Центр Валидации), и может не являться прямым участником обмена между пользователями и ИС, но может обеспечивать их данными, необходимыми для аутентификации (напри-

[2] Двухэтапную проверку часто путают с двухфакторной аутентификацией. При двухэтапной проверке допускается совмещение среды функционирования в одном устройстве, т.е. со своего смартфона пользователь может работать в ИС и получать на него push, OTP или SMS для доступа в эту ИС. При двухфакторной аутентификации среда функционирования ИС и среда функционирования второго фактора аутентификации пользователя (его аппаратного средства аутентификации) должны быть разными.

[3] Из новых Требований 117-го приказа ФСТЭК России о защите информации в государственных ИС (ГИС) и иных ИС и содержащейся в них информации.

мер, Ticket Kerberos для аутентификации в домене).

Необходимые компоненты для построения корпоративной PKI, обеспечения ДОВЕРИЯ и строгой аутентификации в ИС:

1. Корпоративный Центр Сертификации (ЦС, CA – Certificate Authority)[4]

◆ Это ключевой компонент, основа системы обеспечения доверенного взаимодействия всех объектов (сетевого, компьютерного оборудования, ПО, сервисов в ИТ-инфраструктуре), субъектов (пользователей) в ИС, основа корпоративной PKI.

◆ Центр Сертификации должен быть доверенным, ему должны безусловно доверять все элементы ИС и все участники обмена для реализации концепции ZeroTrust (нулевое доверие), когда никто в ИС никому не верит, но все доверяют корпоративному «нотариусу» (CA), который всех идентифицировал, проверил и по запросу подтвердил подлинность. И это не должен быть Microsoft CA (CS) – бесплатный сыр в мышеловке и единая точка отказа в большинстве наших ИТ-инфраструктур.

◆ Центр Сертификации должен быть сертифицирован ФСТЭК России – его безопасность, корректность функционирования и уровень доверия должны быть проверены и доказаны в процессе сертификации.

2. Служба каталога с контроллером домена (для ИС с доменной архитектурой)

◆ Примеры реализации: Windows – Active Directory, Linux – ALD Pro, РЕД АДМ, Альт Домен, Samba DC, FreeIPA и др.

3. USB-токены, смарт-карты, BIO-токены/ридеры со встроенным сканером отпечатков пальцев– это пользовательские аппаратные средства 2ФА/3ФА (фактор владения). Требования к ним:

◆ Устойчивость к взлому и клонированию, уникальность (для однозначной идентификации устройства).

◆ Аппаратная реализация криптографических преобразований с неизвлекаемым закрытым ключом, обеспечивающих необходимый уровень стойкости или имеющих гарантированную стойкость[5].

◆ Энергонезависимая память, достаточная для хранения как минимум двух цифровых сертификатов формата X.509.

◆ ПИН-код устройства (фактор знания), позволяющий пользователю разблокировать доступ к закрытому ключу и операциям с ним.

◆ Для средств 3ФА/2ФА – встроенный сканер отпечатков пальцев и математика для верификации полученного со сканера отпечатка с хранящимся в памяти токена эталоном – цифровым шаблоном (биометрический фактор, подтверждающий личность пользователя и его право получить доступ к функциональности токена или смарт-карты).

4. Клиентское ПО, обеспечивающее поддержку устройств аутентификации, работу с цифровыми сертификатами и PKI.

◆ В MS Windows таким штатным клиентским ПО является Windows Smartcard Logon.

◆ В Linux (и всех российских ОС на базе Linux) штатной поддержки PKI и средств 2ФА/3ФА нет.

Это серьёзная проблема, поскольку именно PKI обеспечивает безопасное доверенное взаимодействие всех со всеми в корпоративных сетях и инфраструктурах Enterprise-класса.

5. Система централизованного управления жизненным циклом сертификатов и средств 2ФА/3ФА.

При разворачивании корпоративной PKI и внедрении строгой аутентификации возникает необходимость автоматического отслеживания срока действия цифровых сертификатов пользователей, оборудования, вовремя их обновлять, перевыпускать, учитывать выданные пользователям средства 2ФА/3ФА, вовремя блокировать их и пр., а также существенно снижать рутинную нагрузку на администраторов.

ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

Что нужно для внедрения строгой аутентификации и повышения живучести наших ИС?

Пока мы жили в экосистеме Windows и доверяли всему, что нам давали, мы успели привыкнуть ко всему хорошему, что там есть – удобству, встроенной безопасности, построенной на базе PKI, к уровню Enterprise.

Как только началась СВО, нам послали первое предупреждение – отозвали сертификаты для межсайтового взаимодействия, и половина Интернет-сайтов в стране «легла», точнее, не смогла обеспечить то самое доверенное взаимодействие.

Инструменты обеспечения доверия стали использоваться как инструменты давления, шантажа, как серьёзное оружие, призванное и способное парализовать ИТ-инфраструктуру гос. организаций, органов власти, организаций КИИ, экономику страны.

Давайте зададим себе вопрос, а что будет, если вдруг перестанет работать корпоративный Центр Сертификации? Перестанет выдавать новые сертификаты? Не страшно.

А если перестанет работать корневой CA (который до поры до времени находился в оффлайне, а вам надо перевыпустить сертификаты для подчинённых CA, срок действия которых заканчивается) или Центр Валидации, который и проверяет предъявляемые всеми участниками обмена сертификаты?

Вот тут и начнётся страшный сон – наши ИТ-инфраструктуры («железо», сервисы, ПО) рискуют развалиться за сутки, все компоненты перестанут доверять друг другу и взаимодействовать друг с другом. Почему сутки? Это срок жизни тикета Kerberos.

Так что же происходит при миграции на Linux? Почему там всё не так? А всё достаточно просто – в Linux нет полноценного PKI корпоративного уровня, а без него – это всё консьюмерская история, не Enterprise, к которому мы все так привыкли.

[4] Не путать с УЦ (Удостоверяющим Центром), обеспечивающим выпуск и обслуживание сертификатов открытого ключа электронной подписи (по 63-ФЗ) для юридически значимого электронного документооборота

[5] Зарубежные криптоалгоритмы RSA, ECDSA с декларируемой стойкостью, российские ГОСТы с известной/гарантированной стойкостью.

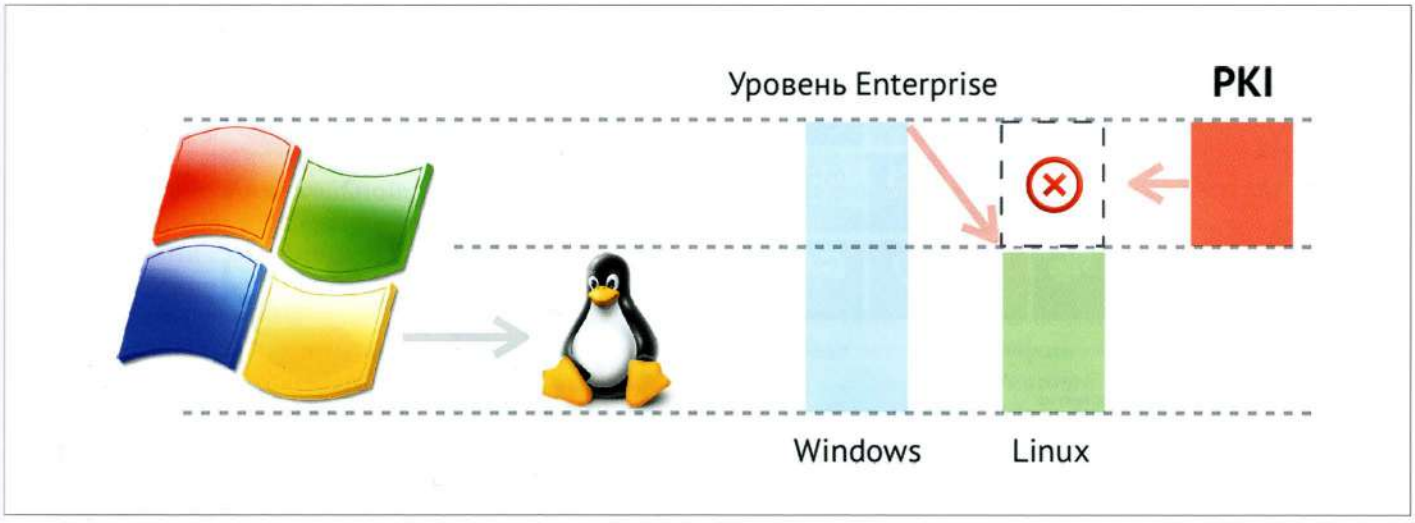

Рисунок 1.

И Open Source нам здесь, увы, не помощник – «поляна» хорошенько зачищена, поскольку это стратегическая технология, и как мне в своё время объяснили, цитирую: «Продать Enterprise PKI в Россию, это хуже, чем поставить ядерные технологии в Иран» (рис. 1).

Резюме.

Чтобы «вытянуть» Linux на уровень Enterprise, обеспечив при этом сквозную безопасность от ИТ-инфраструктуры до пользователей, реализовать доверенное взаимодействие, необходимо:

1. Внедрить корпоративную PKI – доверенный CA под Linux, который заменит MS CA – единую точку отказа, обеспечив бесшовный переход без остановки работы всех сервисов. Это обеспечит возможность «жить на два дома» – одновременно пользоваться ресурсами и из мира Windows, и новыми, из мира Linux.

2. Внедрить (поддержать с использованием нового доверенного CA) строгую аутентификацию всего используемого оборудования в ИТ-инфраструктуре.

3. Внедрить строгую аутентификацию пользователей (с использованием клиента PKI и 2ФА под Linux, обеспечивающего возможность «ходить налево» – в Windows). И не забыть про систему централизованного управления.

Ключевые различия двух экосистем (рис. 2).

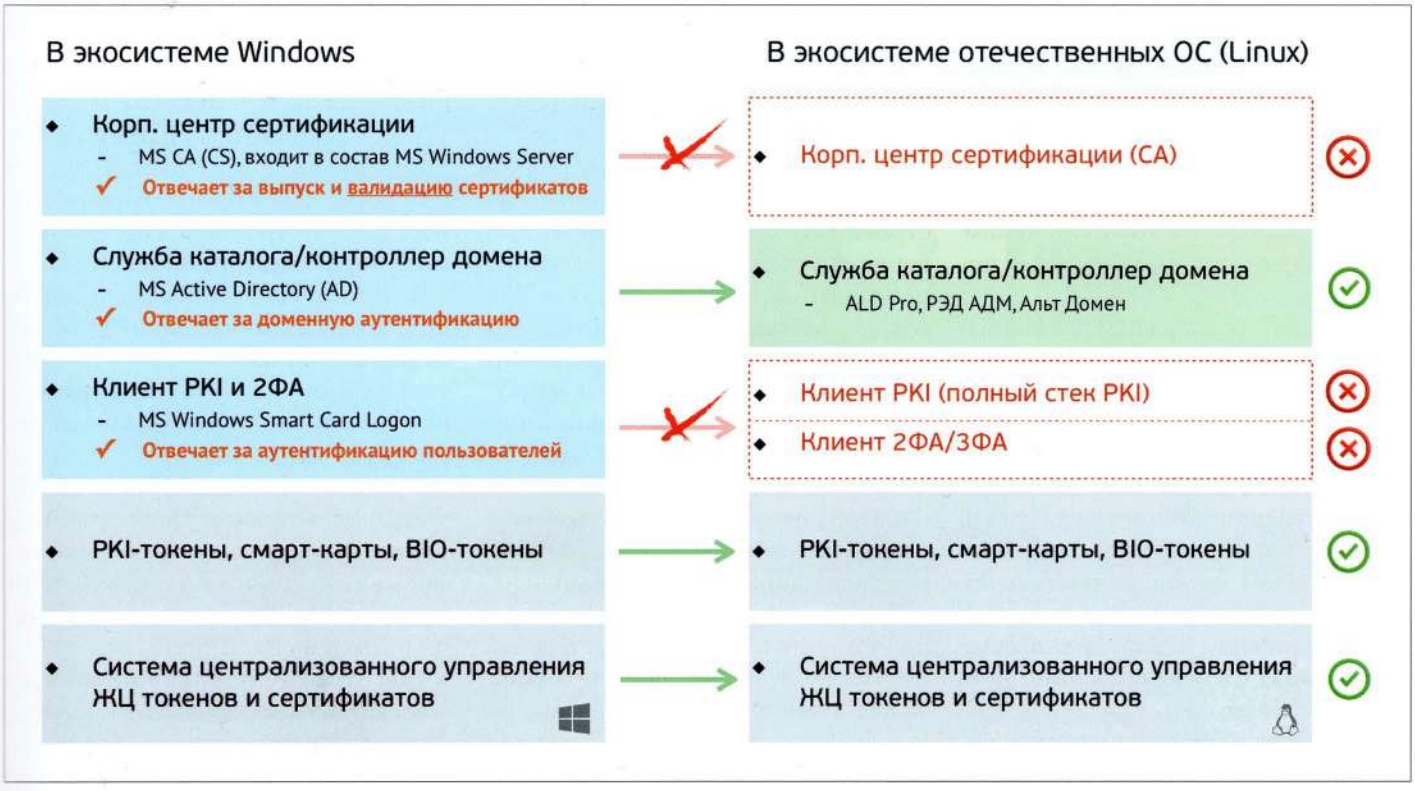

Рисунок 2.

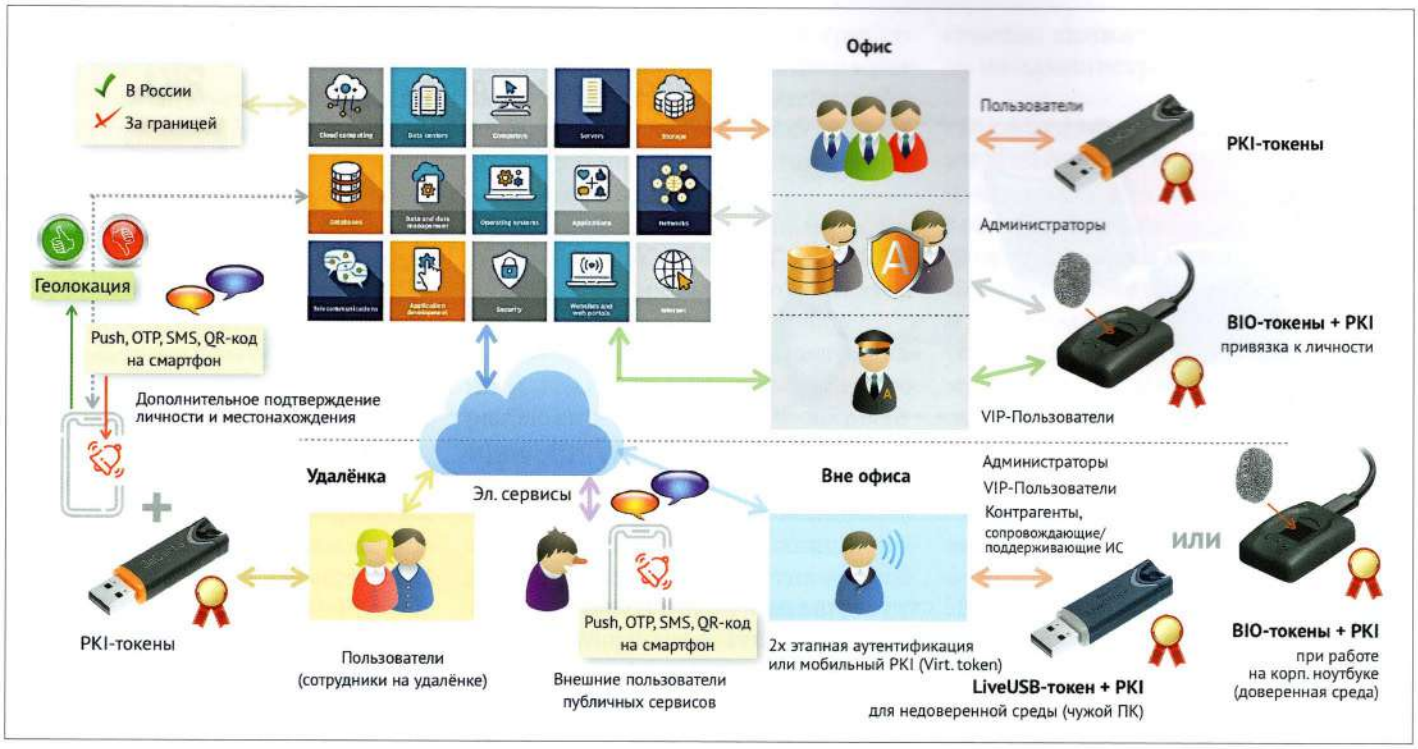

Рисунок 3.

Адаптивная многофакторная аутентификация. Самое время вспомнить про наши ИС: они не монолитны, имеют несколько сегментов, в которых хранится и обрабатывается информация разного уровня значимости. И про сотрудников, которые имеют разные уровни доступа в ИС, разные полномочия (ТОПы, ВИПы, админы), работают в разных условиях – кто-то в офисе, кто-то удалённо, из дома или с дачи, а кто-то релоцировался и работает из-за рубежа, кто-то работает на корпоративном ноутбуке, а кто-то на своём – домашнем.

А раз оно так, то разве можно подходить ко всем с одними правилами и требованиями по аутентификации? Нет, нельзя.

Для разных сегментов ИС, условий работы пользователей, для разных сред функционирования (в т.ч. средств 2ФА) должен быть определён РАЗНЫЙ набор факторов, дополнительных средств и способов подтверждения идентификационных данных и их связи с личностью пользователя.

Чем выше риск возможной атаки на систему и больше вариантов ее исполнения – тем должно быть больше дополнительных факторов, средств, способов и компенсационных мер для подтверждения личности пользователя.

Это и есть адаптивная многофакторная аутентификация (МФА), реализовать и поддерживать которую достаточно просто.

Попробуем показать и объяснить это с использованием рисунка 3.

1. Сотрудник работает в офисе

Контролируемый периметр объекта (здания, офиса), правильно настроенный корпоративный ПК, доверенная среда функционирования используемого ПО, развёрнута PKI, сотрудник работает с чувствительной информацией (CRM, ERP, персональные данные клиентов и пр.).

Для строгой аутентификации можно использовать USB-токены, смарт-карты с поддержкой PKI.

2. Привилегированные пользователи (администраторы, ВИПы, ТОПы) с корпоративными ноутбуками

Пользователи имеют расширенные полномочия и практически полный доступ ко всем ресурсам и сегментам ИС, мобильны, часто работают и в офисе, и вне его, подключаются к ИС удалённо, но со своего корпоративного ноутбука (контролируемого службой ИТ, с доверенной средой функционирования), голова забита более важными глобальными задачами и проблемами, чем непосредственно вопросы ИБ... Отсюда следствие, часто забывают ПИН-код от своего токена.

Для строгой аутентификации желательно использовать BIO-токены (отпечаток пальца вместо ПИН-кода и/или в дополнение к ПИН-коду для компенсации возникающих рисков при работе такого привилегированного пользователя вне контролируемого периметра организации).

3. Привилегированные пользователи (+ сотрудники подрядных организаций, поддерживающие ИС, внедряющие новое ПО и пр.), работающие из недоверенной среды (личный ноутбук, «чужой» ПК)

При работе из недоверенной среды для ИС возникают недопустимые риски – кража чувствительной информации, «подсаживание» специализированного трояна, организация атаки на ИС и т.п.

Для устранения этих рисков необходимо использовать специализированное средство, обеспечивающее безопасную дистанционную работу и строгую 2ФА пользова-

теля, работающего из недоверенной среды[6].

4. Сотрудники на удалёнке (с корпоративными ноутбуками – в доверенной среде функционирования).

Работают с чувствительной информацией (CRM, ERP, с персональными данными клиентов), им было дано разрешение работать удалённо, подключаясь из дома или работая на даче (где относительно безопасно).

Вопрос – а как отследить и убедиться, что сотрудник действительно работает из дома или на даче, а не уехал за границу и не работает оттуда?

Для многих организаций это недопустимый риск.

Чтобы получить геолокацию, понадобится зарегистрированный в ИС номер мобильного телефона такого сотрудника и дополнительные средства, обеспечивающие дополнительную (усиленную) аутентификацию с отправкой на него push, SMS, OTP сообщений и обработку данных геолокации по базовым станциям (увы, GPS/ГЛОНАСС теперь могут увести далеко не туда). И это в дополнение к его штатному USB-токену. Телефон нужен как «второй» фактор с возможностью получения геолокации, позволяющий осуществлять блокирование доступа из-за границы.

5. Сотрудники подрядных организаций, внешние пользователи некритичных сервисов ИС.

Сотрудники не подключаются к сегментам ИС, содержащим чувствительную информацию.

В этом случае достаточно использовать усиленную или двухэтапную аутентификацию (когда на смартфон пользователя посылается код доступа или установленное в нём приложение генерирует одноразовый пароль).

6. Внешние пользователи открытых публичных сервисов.

Являются потребителями информационных сервисов, подключаются к публичным ресурсам ИС.

Для доступа в Личный кабинет или для отправки в ИС сообщений часто требуется авторизация пользователей в ИС и их аутентификация. Если в организации уже развернут сервер для усиленной аутентификации, то имеет смысл использовать его и для аутентификации внешних пользователей с использованием push- или SMS-сообщений на его мобильный телефон.

Резюме.

Внедрение адаптивной аутентификации позволит кардинально решить проблему и устранить большое количество потенциальных проблем и инцидентов, поскольку устраняет одну из главных ПРИЧИН атак на ИС – слабую аутентификацию, обеспечит гибкость в выборе средств, методов и способов аутентификации, позволит правильно и эффективно распределить бюджет на ИБ.

Правильная система аутентификации в ИС – залог её безопасности.

[6] Требование 117-го Приказа ФСТЭК России, а также лучшие практики ИБ