Аладдин

Аутентификация - от паролей к 2ФА, биометрии, адаптивной МФА

Ответы на заданные и присланные вопросы

О документе

15.05.2025 в рамках Aladdin Security Day прошёл вебинар на тему "Аутентификация - от паролей к 2ФА, биометрии, адаптивной МФА".

В процессе вебинара и после него было задано достаточно большое количество вопросов, на которые мы постарались ответить ниже.

Некоторые заданные вопросы нам пришлось немного переформулировать, чтобы был лучше понятен контекст.

Авторам этих вопросов приносим свои извинения, а всем, кто был активен и задал нам эти вопросы - ещё раз отдельная благодарность!

Все вопросы мы сгруппировали по нескольким группам:

1. Аутентификация
2. Биометрия
3. Удалённый доступ
4. Нормативные требования (для идентификации и аутентификации).

Дополнительные материалы:

- Презентация (скачать) - "Аутентификация - от паролей к 2ФА, биометрии, адаптивной МФА"
- Запись вебинара "Аутентификация - от паролей к 2ФА, биометрии, адаптивной МФА"
- FAQ - "Аутентификация - от паролей к 2ФА, биометрии, адаптивной МФА"

1. Аутентификация

Внедрение адаптивной МФА с технологической точки зрения не является сложным. Сложность возникает при формировании правил, составлении модели рисков. Как определить минимально необходимые, достаточные и разумные критерии факторов для адаптивной МФА, чтобы не закончилось полным запретом, преследуя концепцию zero trust?

Вопрос абсолютно правильный - основная сложность возникает при формировании и РЕАЛИЗАЦИИ правил, модели рисков, матрицы доступа и пр. Как раз на этом все и обламываются ;-)

Мы предложили более простую модель, основанную на ролевом разделении, сценариях работы и выборе определённого типа средства 2ФА, компенсирующего основные риски:

- Сотрудники в офисе - USB-токен или смарт-карта для 2ФА
- Сотрудники на удалёнке (смешанный режим работы)
  - надо добавить доп. способ подтверждения личности (push, OTP или SMS) и геолокацию для определения места (можно или нельзя подключаться из этого региона?) -к токену добавляется использование мобильного телефона - Aladdin 2ФА
- Привилегированные пользователи:
  - Администраторы - им необходимо дать возможность безопасно делать свою работу с любого подручного компьютера (домашнего, в отеле, где-то…), для этого надо компенсировать (убрать) риски, возникающие при работе из недоверенной среды (трояны, вирусы, удалённое управление и пр.). Для этого мы предлагаем использовать специализированное средство для безопасной дистанционной работы - Aladdin LiveOffice, позволяющее запустить с защищённой флешки преднастроенную доверенную ОС, установить защищённое соединение со своим служебным компьютером или виртуальным (VDI) и безопасно работать из недоверенной среды. Подробнее здесь. Если администратор работает на служебном ноутбуке и подключается удалённо, то проблема недоверенной среды уходит, и остаётся лишь дополнительно подтвердить его личность с помощью биометрии - для это у него вместо обычного токена должен быть токен с биометрией (JaCarta SecurBIO).
  - ВИП-пользователи, руководители - всё то же, пусть у них будет в кармане лежать специализированное USB-устройство (Aladdin LiveOffice), с помощью которого они могут безопасно подключаться с любого подручного недоверенного компьютера и работать в ИС, в том числе со всеми служебными документами, относящимися к служебной тайне и с информацией ограниченного доступа (ДСП), не опасаясь утечек и атак через его подключение на ИС.
- Сотрудники подрядных организаций, обслуживающие или поддерживающие ИС (удалённо) - в зависимости от сегмента ИС, куда их пускают, должны использовать строгую или усиленную 2ФА.
- Внешние пользователи публичных сервисов ИС могут аутентифицироваться с использованием своих мобильных телефонов, используя их в качестве аппаратного средства 2ФА, установив на них специальное приложение - Aladdin 2ФА (push, генерация/получение OTP, SMS) или виртуальный токен - функциональный аналог аппаратного токена JaCarta PKI.

То есть делим всех пользователей нашей ИС на группы в зависимости от сценария работы, роли, сегмента ИС, куда они получают доступ, среды и места из которой подключаются удалённо, и выдаём им соответствующее средство 2ФА, компенсирующее возникающие риски и угрозы ИБ.

Такая модель гораздо проще в понимании, планировании и реализации, а эффективность её не сильно ниже классической схемы адаптивной МФА (которая, как я сказал, мало у кого прижилась).

Откуда взято требование про усиленную аутентификацию для ИС со средним уровнем доверия и что такое средний уровень доверия? (Слайд 7)

Основные понятия, определения, требования доверия к идентификации и аутентификации описаны в национальных стандартах РФ (ГОСТах), разработанных, кстати, нашей компанией (Аладдин), 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.

Их стоит изучить и начать применять.

PS. Они не списаны с зарубежных стандартов, как наши многих ГОСТы, а сделаны на базе лучших практик и рекомендаций, что называется, выстраданы и "написаны кровью", как правила дорожного движения.

Достоверность результатов аутентификации сильно зависит от:

- Достоверности идентификации (степени связанности идентификатора с объектом ИС или субъектом - пользователем)
- Количества одновременно применяемых атрибутов идентификации и факторов аутентификации
- Протоколов аутентификации
- Организации обмена аутентификационной информацией - односторонняя или взаимная
- Среды выполнения (замкнутая доверенная или недоверенная среда, внутри или вне защищённого периметра)
- Типа аутентификации.

При организации доступа в ИС должен использоваться один из трёх видов аутентификации, соответствующий или превышающий уровень доверия самой ИС:

Вид аутентификации	Уровень доверия
Простая	Низкий
Усиленная	Средний
Строгая	Высокий

Вид аутентификации в ИС должен определяться:

- по уровню значимости информации
- по риску возникновения недопустимого события ИБ и размеру возможного ущерба в случае взлома и утечки.

Каким образом происходит интеграция PKI и систем двухфакторной аутентификации? Где в системе 2ФА можно использовать Enterprise CA?

Давайте начнём с PKI и целей её внедрения:

- В открытых ИС (публичных сервисах для неограниченного круга лиц - сервисы ФНС, портал госуслуг и др.)
  - Для аутентификации Web-сайтов и защиты сессий (SSL, TLS-сертификаты)
  - Для организации юридически значимого электронного документооборота с использованием квалифицированной электронной подписи (ЭП)
- В закрытых корпоративных системах
  - Для обеспечения доверенного взаимодействия всех элементов корпоративной ИТ-инфраструктуры - используемого оборудования, программного обеспечения (ПО), пользователей
  - Для строгой аутентификации пользователей при доступе в корпоративную ИС
  - Для корпоративного электронного документооборота с использованием усиленной неквалифицированной ЭП
  - Для защиты данных.

Т.е. PKI - это инфраструктура для обеспечения доверия в ИС и строгой взаимной аутентификации всех её элементов (оборудования, ПО, пользователей).
В MS Windows все необходимые компоненты PKI и строгой аутентификации уже есть - MS CA (Центр сертификации), MS Smartcard Logon - PKI-клиент с поддержкой 2ФА, Active Directory - служба каталога и контроллер домена, обеспечивающий строгую доменную аутентификацию (для работы в сети).

В Linux всё сильно хуже, там нет полноценного PKI Enterprise-класса.

Упоминаемые FreeIPA и др. не обеспечивают нужного уровня масшабируемости, отказоустойчивости и др. требований к продуктам класса Enterprise.
Поэтому, чтобы вытянуть Linux на уровень MS Windows (Enterprise), и обеспечить возможность безопасного доверенного взаимодействия всех компонентов ИТ-инфраструктуры (оборудования, ПО/сервисов/шлюзов, пользователей) - их строгую аутентификацию, мы разработали и сертифицировали несколько важнейших (ключевых) компонент для построения полноценного PKI - Aladdin Enterprise CA (для замены точки отказа в инфраструктуре - MS CA), Aladdin SecurLogon (аналог MS Smartcard Logon).
Эти компоненты и обеспечивают реализацию (поддержку) строгой 2ФА в Linux и дают возможность параллельно работать и с унаследованной экосистемой Windows и жить "на два дома".
Получается не сложнее, чем в Windows.

Есть ли примеры внедрения данных продуктов (в частности JMS, JAS и Аладдин 2ФА) в рамках отказоустойчивой (катастрофоустойчивой) и георазпределённой архитектуры? Каким образом при такой архитектуре происходит балансировка и копирование данных между ЦОД? Особенно данных для Аладдин 2ФА, который находится в DMZ? Есть ли примеры схем и бестпрактисы?

Да, у нас есть ряд таких примеров успешных внедрений и эксплуатации ИС под 100К пользователей, с отработанными решениями по построению отказоустойчивой, георазпределённой катастрофоустойчивой архитектуры. Свяжитесь с нашими специалистами из команды пресейла - projects@aladdin.ru - поделимся примерами и рекомендациями
Если захотите, мы попробуем организовать reference-визиты к нашим крупным заказчикам, у кого это внедрено и работает.

Насколько Ваша система управления жизненным циклом PKI может обеспечить требования 152 приказа ФАПСИ?

В JMS (система централизованного управления жизненным циклом средств аутентификации/ЭП и сертификатов) реализован поэкземплярный учёт СКЗИ в соответствии с требованиями приказа ФАПСИ от 13 июня 2001 г. N152.

Если подробнее, то в JMS реализовано:

- регистрация в базе данных подлежащих учёту дистрибутивов, документации, лицензий СКЗИ, аппаратных модулей СКЗИ и носителей ключевой информации (электронные ключи JaCarta, eToken, Рутокен, ESMART, сертифицированные ФСБ России как СКЗИ, КриптоПро CSP, ViPNet CSP)
- экземпляров СКЗИ (электронные ключи JaCarta, eToken, Рутокен, ESMART, сертифицированные ФСБ России как СКЗИ КриптоПро CSP, ViPNet CSP и т.п.), документации
- установка программных СКЗИ (КриптоПро CSP, ViPNet CSP) и лицензий на автоматизированные рабочие места (АРМ) пользователей
- обнаружение и регистрация ранее установленных на АРМ пользователей КриптоПро CSP 3.6, 3.9, 4.0, 5.0, ViPNet CSP 4.2, 4.4 и лицензий на эти СКЗИ при наличии сетевого соединения между серверным компонентом программного комплекса, АРМ пользователя и наличии запущенного клиентского компонента программного комплекса на АРМ пользователя
- автоматическое создание в электронном журнале учёта СКЗИ событий, относящихся к регистрации, передаче пользователю, введению в эксплуатацию, выводу из эксплуатации, уничтожению экземпляров СКЗИ
- ведение электронного журнала учёта ключевых документов и автоматическое создание в нем событий, относящихся к регистрации, передаче пользователю, введению в эксплуатацию, выводу из эксплуатации, уничтожению ключевых документов
- формирование отчёта по учитываемым СКЗИ – электронные ключи JaCarta, eToken, Рутокен, ESMART, сертифицированные ФСБ России как СКЗИ, КриптоПро CSP 3.6, 3.9, 4.0, 5.0; ViPNet CSP 4.2, 4.4 и ключевым документам в форме, соответствующей требованиям приказа ФАПСИ №152 от 13.06.2001
- экспорт отчёта в распространённые форматы.

Как в случае взаимной аутентификации (строгой) ИС докажет пользователю, что она подлинная?

При строгой аутентификации производится взаимная проверка и доказательство (подтверждение) подлинности сторон - что каждая из них является тем, за кого себя выдаёт (очень схематично):

- пользователь доказывает ИС (серверу), что он тот, за кого себя выдаёт, с помощью предъявляемого им цифрового сертификата и подписанного с помощью контролируемого им (принадлежащего ему) закрытого ключа некого технологического сообщения (дайджеста).
- сервер проверяет цифровую подпись под дайджестом с помощью открытого ключа пользователя, проверяет валидность его цифрового сертификата (обратившись к Центру валидации - CA), и, если всё нормально, даёт разрешение на вход данного пользователя в ИС.
- сервер (перед тем как пустить пользователя) предъявляет ему свой цифровой сертификат (содержащий его открытый ключ) и посылает некое сообщение, подписанное его закрытым ключом.

- пользователь (клиентское ПО с поддержкой PKI), чтобы убедиться в том, что он попал именно на тот ресурс, куда и был должен попасть, и что этот ресурс ему не подменили в результате фишинга, проверяет на открытом ключе подпись под сообщением, полученным от сервера (ИС), затем запрашивает у Центра сертификации (CA - корпоративный "нотариус") проверку валидности цифрового сертификата
- если у каждой из сторон с проверками всё нормально, происходит подключение пользователя к ресурсу (ИС).

Таким образом, каждая из сторон доказала свою подлинность с помощью третьей доверенной стороны - корпоративного ЦЕНТРА СЕРТИФИКАЦИИ (CA), цифровых сертификатов и протоколов аутентификации (Kerberos, TLS и др.). И при этом - никто из сторон (участников обмена) никому не доверяет, кроме Центра сертификации (CA).

Является ли сеть сотового оператора (для SMS) другой средой, где обладание (SIM картой) является фактором?

Можно конкретизировать, в случае использования телефона как 2-го фактора, в качестве устройства подразумевается именно телефон или сим-карта (в случае если телефон имеет 2 слота для сим-карт разных операторов, возможно ли использовать его и для удаленного доступа и в качестве 2-го фактора идентификации, если канал предоставления удаленного доступа и канал передачи второго фактора будут идти через разные сим-карты).

Нет, не является. В контексте вашего вопроса - это лишь способ доставки SMS. Обладание SIM-картой не может считаться фактором (в данном случае фактором ОБЛАДАНИЯ) - SIM-карта вставлена в телефон (или припаяна - eSIM, или вообще виртуальная/программная), т.е. является практически от него неотчуждаемой. Поэтому SIM-карту и телефон правильнее рассматривать как одно целое. Более того, SIM-карт в одном телефоне может быть несколько.

Приложение на смартфоне, SMS на другой телефон. Надежно?

Нет.

У многих пользователей уже есть ЭПЦ, многие сервисы, например, сайт ФНС аутентифицируют пользователей по этой ЭЦП (УКЭП), так почему бы не использовать её для 2ФА в свои ИС?

Использовать УКЭП (ЭП) для целей аутентификации в ИС категорически недопустимо.

Те, кто это делал и делает, в том числе для наших федеральных ИС, и считает это допустимым - крайне невежественные “специалисты”, которые занимают чужое место.
Для аутентификации и доступа пользователей в ИС должны использоваться цифровые сертификаты доступа (и отдельные ключи), выдаваемые корпоративными Центрами сертификации (CA), а для ЭП документов и систем ЭДО (эл. документооборота) - электронные подписи и сертификаты, выдаваемые УЦ (Удостоверяющими центрами) согласно 63-ФЗ.

USB-токен пользователя может выполнять сразу две функции - быть средством строгой 2ФА, и одновременно - средством УКЭП. Это реализовано в наших токенах и смарт-картах - JaCarta PKI/ГОСТ.

Каким образом сотрудник сможет пройти удаленную идентификацию для случая необходимости выпуска виртуального токена при нахождении в командировке и отсутствии аппаратного токена?

Хороший вопрос, спасибо за него.

Идентификация всегда имеет два этапа - первичная и вторичная.
На этапе первичной идентификации пользователь предоставляет дополнительные сведения о номере своего мобильного телефона, который регистрируется в ИС.

Далее он может установить приложение JaCarta Virtual Token сразу (или перед своей командировкой) и выпустить для него цифровой сертификат доступа в ИС, как альтернативный аппаратному токену, но, желательно с рядом ограничений, например по времени использования, поскольку мобильный телефон менее защищён, чем аппаратный токен.

Либо сделать это позже, например, уже находясь в командировке, подтверждая свою личность несколькими, описанными в правилах и политиках ИБ организации, способами. Например, связавшись с администратором голосом, по ВКС или другим способом. При этом, упомянутые дипфейки и бесконтактный способ биометрической идентификации здесь работают не очень, поскольку номер мобильного телефона уже заведен в систему, а сертификат (и ключи) будут привязаны к номеру абонента и аппарата, и подменить их будет весьма проблематично.

Криптографическая беспарольная аутентификация выглядит на текущий момент как идеальная замена двухфакторной и биометрической аутентификации (хотя биометрическая может применяться для разблокировки ключа, хотя я считаю, что безопаснее всё-таки разблокировать персональный ключ паролем, который знаешь только ты).

Как вы думаете, возможно ли применение в России создание аналога или возможности использования протокола WebAuthn, разработанного альянсом FIDO, с применением отечественной криптографии? Есть ли наработки в этой части, и ведется ли проработка вопросов криптографической аутентификации с использованием отечественных постквантовых криптографических алгоритмов?

1. Если используется криптография, то обязательна аутентификация пользователя (владельца криптографического ключа), например, с использованием фактора ЗНАНИЯ (пароля) и/или БИОМЕТРИИ. В нашем БИО-токене (SecurBIO) так и сделано - пользователь с помощью отпечатка пальца подтверждает свою личность (и владение криптографическим ключом) и может использовать палец вместо пароля.

2. По поводу FIDO - это стандарт для аутентификации с использованием криптографии. Но без PKI. Некоторые мои коллеги называют это PKI без необходимости построения PKI и развертывания CA (Центра сертификации). Согласитесь, звучит как-то натянуто и немного глупо.
Эта технология неприменима для корпоративных ИС.
Почему? Потому что там нет роли администратора, и пользователь сам прописывает свое устройство в разные ИС. Это для консьюмерского рынка, не для ГИС и не для корпоративного рынка.

Теперь вопрос - а тогда зачем там российская криптография, если использовать его на регулируемом рынке (гос. ИС, Enterprise) нельзя? И тем более с использованием отечественных постквантовых криптографических алгоритмов…
Не думаю, что кто-то у нас готов тратить на это свои деньги и время.

Адаптивная МФА предполагает под собой элемент авторизации? Если пользователь подтвердил (с необходимым набором факторов) на даже рабочем ноутбуке свою личность, то при попытке получить доступ к ИС, например из-за границы, происходит не только аутентификация устройства, но и его авторизация по ряду определённых факторов, в т.ч. из какой именно страны осуществляется подключение. В данном случае ИС авторизует устройство и пользователя, чтобы определить какое количество факторов и какие из них необходимо требовать для аутентификации пользователя или в при.

Получается, чтобы получить доступ к аутентификации - необходимо пройти первичную авторизацию на основе среды выполнения аутентификации? И как вариант в принципе запретить доступ к аутентификации.

Давайте разбираться - как должен быть организован процесс доступа в ИС?
Он производится в 4 этапа, которые идут в строгом порядке:

1. **Идентификация**

   - Первичная - однократный процесс - предоставление документов (свидетельств), их проверка, получение подтверждений об их подлинности, заведение в ИС учётной (-х) записи (-й), выдача пользователю физического средства 2ФА
   - Вторичная - многократно повторяющийся процесс - опознавание пользователя (сравнение предъявленного им идентификатора с зарегистрированным в ИС).

2. **Аутентификация** - это процесс (способ) подтверждения идентификационных данных - 3 базовых типа (а всего из 8):

   - Локальная
   - Доменная (для входа в сеть)
   - Браузерная

И 3 возможных фактора - ВЛАДЕНИЕ, ЗНАНИЕ и БИОМЕТРИЯ. Всё остальное, что иногда называют факторами аутентификации - заблуждение.

3. **Авторизация** - проверка ИС прав доступа (что разрешено делать, куда разрешен доступ?)

4. **Предоставление доступа в ИС.**

Процесс работает именно так, и нарушать его, меняя очередность или придумывая что-то своё, нельзя.

Интересует совместимость VPN UG и JMS+JAS+A2FA. (в части продуктов на Linux)
Есть ли практика успешной реализации данного кейса? Если имеется, прошу оказать содействие в данном вопросе.

Совместимость обеспечена, на сайте есть информация. Есть практические внедрения.
Напишите нам на projects@aladdin.ru

2. Биометрия

Не считаете ли Вы использование биометрии при аутентификации вредной практикой? Биометрию при утечке пользователь не сможет сменить!

Отпечаток пальца или снимок сосудов пальца утекает так же достаточно просто как и фотография, но поменять палец пользователь не сможет!

Поменять скомпрометированную биометрию пользователь, как например токен, не сможет, придется менять пользователя? А если это VIP пользователь?

Дьявол в деталях, в выбранной технологии и в реализации.
Для начала, надо определить, о какой технологии (биометрии) мы говорим?
Если об отпечатках пальцев (о которой я рассказывал), то ключевой вопрос в технологии - что и откуда может утечь:

1. Куда и как подключен сканер отпечатков пальцев?

   - Если напрямую к компьютеру, то утечка неизбежна. Плохо.
   - Если сканер интегрирован в устройство и результаты сканирования (фото отпечатков) не попадают в компьютер (в ИС), то надо смотреть дальше…

2. Где производится обработка изображения отпечатка пальцев, полученных со сканера?

   - Если в компьютере (в ИС), то утечка неизбежна. Плохо.
   - Если внутри устройства (используется технология Match-On-Device), то надо смотреть дальше…

3. Где хранятся отпечатки пальцев (их образы, обработанные шаблоны)?

   - Если в базе данных, то как ружьё, висящее на стене - в конце спектакля оно обязано выстрелить, так и здесь - база, даже если декларируется, что она надёжно защищена, всё равно рано или поздно утечет. Плохо.
   - Если внутри устройства, без общей базы данных, то вопрос в надёжности такого устройства к взлому. И к тому, а зачем его ломать, если нужный отпечаток пальца проще снять, например, со стакана, из которого только что пили?

В нашем BIO-токене (SecurBIO) полупроводниковый емкостной сканер встроен в само устройство (1), отпечатки пальцев не попадают ни в компьютер, ни в ИС (кстати, поэтому владелец ИС не становится оператором персональных биометрических данных!), у нас нет общей базы данных, хранящей, обрабатывающей и передающей (кому-то и куда-то) эти данные.

Следовательно, особо утекать нечему, и "менять свою биометрию" не придётся ;-)

Небольшой комментарий по поводу сосудов пальца - не совсем корректная формулировка, правильнее говорить об отпечатке пальца. Он основан на особенностях папиллярного узора пальца - это специфический и практически уникальный рисунок, образованный линиями (гребешками) кожи на подушечках пальцев, не меняется в течении жизни человека.

Вероятность повторения (совпадения) папиллярного узора или невозможности его снятия в силу особенностей кожи человека - порядка 10^{-5} (1:100,000).

Теперь про компрометацию биометрических данных - действительно, поменять свои данные, как например, токен (точнее данные в нем), пользователь не сможет.

Что такое Match-On-Device / Match-On-Card?

Это технология, при которой хранение, обработка и сравнение образов отпечатков пальцев, полученных со встроенного в устройство сканера отпечатков пальцев, принятие решения о совпадении или несовпадении происходит внутри устройства.

При этом критически важная информация (цифровой образ отпечатка пальца, полученных из него шаблон) проходит полный цикл обработки непосредственно в самом устройстве, и не передается ни на рабочую станцию пользователя, ни на сервер, ни в базу данных с отпечатками пальцев или шаблонами на их основе.

Это безопасная технология распознавания отпечатков пальцев внутри устройства или смарт-карты.

Какое количество шаблонов отпечатков пальцев может храниться в памяти JaCarta SecurBIO?

В памяти устройства SecurBIO можно сохранить до 20 шаблонов отпечатков пальцев:

- До 10 шаблонов отпечатков пальцев для Пользователя
- До 10 шаблонов отпечатков пальцев для Администратора (для альтернативного доступа к функциям SecurBIO-токена).

Нужно ли устанавливать какое-либо дополнительное ПО для работы с SecurBIO-токеном?

Для администрирования и регистрации отпечатков пальцев пользователя необходим Единый клиент JaCarta версии 3.3 и выше (для Linux и Windows, бесплатен, можно скачать с нашего сайта).

Драйвера устройства устанавливать не надо - под всеми ОС (вкл. macOS) работает "из коробки".

Для 2ФА/3ФА на Windows - работает через штатное ПО - Windows Smartcard Logon, для Linux - необходимо дополнительное ПО, включающее поддержку PKI и 2ФА/3ФА - Aladdin SecurLogon (платное).

Поддерживает ли JaCarta SecurBIO работу с удаленным рабочем столом?

Да, поддерживает

Насколько реально реализовать двухфакторную аутентификацию, полностью исключающую участие пользователя — например, на основе поведенческой биометрии и анализа окружения?

Какие риски и перспективы у такой модели безопасности?

1. Если исключаем участие пользователя, то откуда возьмём второй фактор? Есть только один - биометрия.
2. Если исключаем участие пользователя, то такой вид биометрии относится к бесконтактной (фото/видео, голос, поведение).
3. Бесконтактная биометрия предназначена немного для других целей - выявление определенных личностей в толпе (лицо, поведение/походка), идентификация по голосу - т.е. больше для целей криминалистики и общественной безопасности. Использовать бесконтактную биометрию для целей идентификации и аутентификации пользователей в ИС и для прохода на объекты КИИ категорически не рекомендуется.

Почему? Дипфейки, генеративный ИИ, способный на лету генерировать нужное изображение (лицо, мимику и пр.), голос.

Настоятельно рекомендую прочитать (или хотя бы пролистать) "Руководство по биометрии" (Р.М. Болл, 2004 г.) - ещё в 2004 г. авторы написали там большими буквами - настоятельно не рекомендуем использовать бесконтактную биометрию для аутентификации в ИС, поскольку считаем, что ИИ за 10 лет разовьётся настолько, что на лету сможет генерировать фейковые видео и голос любого нужного пользователя.

Как в воду глядели… Так что риски, на сегодняшний день, недопустимые.

Бесконтактная биометрия с использованием ToF-камер (камер глубины) тоже не безопасна?

Ключевое слово - бесконтактная. Тоже крайне не безопасна по описанным выше причинам.

Насколько надежной вы считаете фактор биометрии, с учетом того, что для изображений/голоса используются не только дипфейки, но и сами системы распознавания имеют процент расхождения с эталоном, чтобы пользователь проходил аутентификацию, если освещение не так падает или сам пользователь немного не так смотрит, не так говорит.

Любую бесконтактную биометрию, используемую не по её прямому назначению, считаю ненадёжной и недопустимой для использования в целях идентификации и аутентификации пользователей в ИС.

Разве контактную [биометрическую] аутентификацию нельзя подменить, как и бесконтактную? Нет принципиальной разницы при отсутствии непосредственного контроля.

Как написал выше, если говорить абстрактно и вообще, то, конечно же, можно (теоретически). Но если попытаться разобраться в используемой технологии и реализации, то подменить практически оказывается крайне сложно.

Но здесь опять встаёт риторический вопрос (а вы же и задали свой вопрос как риторический) - а кто и как сможет подтвердить ту самую практическую сложность или невозможность подмены? Для это проводится сертификация.

Свой SecurBIO мы сертифицировали в ФСБ России, сейчас он на сертификации во ФСТЭКе (по УД-4 - для конфиденциалки), далее планируем сертификацию для гостайны (до СС вкл.).

Это и есть подтверждение невозможности, кстати, с разными степенями доверия к результатам (сертификации).

В чем принципиальная разница между контактным и бесконтактным факторов? Подмена возможна в обоих случаях, если данные вводятся не под непосредственным контролем.
При возможности подмены отпечаток пальца становится фактором владения "отпечатком"

Про разницу между контактной и бесконтактной биометрией и возможности подмены см. выше. Называть это факторами не совсем корректно.
Контактная биометрия - отпечатки пальцев (сокращу список, ибо это самая доступная, недорогая, компактная, удобная и безопасная для человека технология).

- Отпечатки одного или нескольких пальцев регистрируются в устройстве (а оно персональное, выдаётся пользователя как обычный USB-токен) только в режиме и **под контролем администратора**. Сам пользователь (бесконтрольно) зарегистрировать или поменять/добавить/удалить отпечатки не может!

Сейчас с помощью ЕБС можно получить УКЭП (63-ФЗ) дистанционно.
С помощью биометрии открывается доступ к механизму получения УКЭП.
Насколько хорошо защищен данный механизм получения УКЭП ?

ЕБС основана на использовании бесконтактной биометрии, про неё ответил выше.
Считаю использование ЕБС для целей дистанционной идентификации и аутентификации пользователей в ИС, дистанционного получения УКЭП, прохода в метро по лицу и пр. большой технологической ошибкой, основанной на вере в надёжности защиты базы данных, алгоритмов, процедур и пр.

3. Удалённый доступ

Как обеспечить контролируемую зону в домашних условиях? 152-ю инструкцию никто не отменял...

Контролируемая зона должна обеспечиваться самим пользователем, на него возложена обязанность по сохранению сведений и данных при исполнении им своих функций и должностных обязанностей, в том числе и при дистанционной работе.
Правила обеспечения контролируемой зоны должны устанавливаться самой организацией в своих организационно-распорядительных документах по защите информации, в т.ч. при дистанционной работе.
Дистанционная работа должна рассматриваться как привилегия, как возможность поработать дома, не тратить время на дорогу, не ехать в офис, если заболел, плохо себя чувствуешь, если нужно срочно что-то сделать по работе и при этом не срываться на работу с дачи, из дома.
Это право сотрудника – работать дистанционно.
Но с возникновением прав появляются и обязательства, и ответственность. Так вот вместе с правом работать дистанционно появляется обязанность и ответственность обеспечить вокруг себя и контролируемую зону.
В частности, при дистанционной работе сотрудник должен обеспечить такой режим работы, чтобы никто из посторонних не мог видеть информацию на экране компьютера, не мог следить и считывать надираемый на клавиатуре текст и т.д.

Не можешь обеспечить такие условия при дистанционной работе – не подключайся.

Рекомендуется сделать памятку для пользователей по обеспечению безопасности при дистанционной работе (как, например, сделали в ФНС России).

- Настоятельно рекомендую посмотреть запись прямого эфира AM-Live на эту тему с участием Д.Н. Шевцова (ФСТЭК) и М. Судакова (ФНС России), который всё это физически внедрял в ФНС и сталкивался с такими же проблемами.

Очень сомневаюсь, что при дистанционной работе вообще можно как-то сделать контролируемую зону?..
В случае удаленной работы каким образом пользователь сможет обеспечить контролируемую зону?

Сотрудник должен самостоятельно обеспечить для себя такой режим работы, чтобы никто из посторонних не смог бы подсматривать за его работой с экрана компьютера – что и как он делает, не смог бы считывать нажатия клавиш на клавиатуре.

Для этого достаточно уединиться в отдельной комнате дома, в номере гостиницы, в купе поезда...

Каким образом орган по аттестации будет проверять контролируемую зону, обеспеченную пользователем?

Орган по аттестации проверяет контролируемую зону в ГИС.
Личный компьютер пользователя, используемый вместе с сертифицированным средством безопасной дистанционной работы, не входит в информационную систему организации, но должен быть учтён как СВТ, с которого допускается дистанционная работа при использовании такого-то сертифицированного средства.

Контролируемая зона должна обеспечиваться самим пользователем согласно разработанным организационно-распорядительным документам по защите информации.

Орган по аттестации контролируемую зону в таком случае не проверяет.

Сотрудник на удалёнке – он является ВНУТРЕННИМ НАРУШИТЕЛЕМ? Если ДА, то почему? Он же наш сотрудник – лояльный, честно делающий свою работу, только не на работе, а дома? Такое отношение к удаленному сотруднику (что его записали во внутреннего нарушителя) не обижает сотрудников?

Сотрудник, работающий дистанционно, считается потенциальным внутренним нарушителем.

Поэтому к обеспечению безопасной дистанционной работы и к средствам обеспечения безопасной дистанционной работы предъявляются повышенные требования, призванные снизить потенциальные риски и возможности кражи информации, утечки чувствительных служебных данных (аккаунты, пароли, настройки СЗИ и пр.), каналы и возможности для атаки на ИС организацию.

Повышенные меры безопасности, особенно в текущих условиях, не должны никого обижать.

Накладывает ли удалённая работа из-за границы какие-либо дополнительные требования ИБ со стороны Регуляторов? Или это недопустимо?

В Требования ФСТЭК России к средствам безопасной дистанционной работы каких-либо ограничений или запретов на дистанционную работу из-за границы нет.

Очевидно, что подобные ограничения могут вводится самими организациями из-за специфики и особенностей их деятельности, необходимости и обоснованности такой работы из-за границы, например, во время загранкомандировки или отпуска, при наличии служебной необходимости.
Если надо, то специализированной сертифицированное средство позволяет это сделать.
Ограничения на дистанционную работу могут и должны быть наложены внутренними нормативными документами организации.

В качестве примера – в ФНС России дистанционная работа из-за границы запрещена внутренними организационно-распорядительными документами.

В новых Требованиях ФСТЭК России к защите информации в ГИС
(на замену 17-му Приказу ФСТЭК) запрет на удалённое подключение к ГИС появился.

Какие ещё средства сертифицированы ФСТЭК России на соответствие Требованиям по безопасности информации к средствам обеспечения безопасной дистанционной работы?

На данный момент пока единственным сертифицированным решением является Aladdin LiveOffice от компании "Аладдин".

Почему при работе на недоверенном железе (домашнем компьютере, кишащем вирусами и троянами) ФСТЭК считает, что можно обеспечить безопасность обработки персональных данных и служебной тайны? Звучит так, как пытаться вытащить себя за волосы из болота?

Общая идея решения, которая и обеспечила возможность безопасной дистанционной работы с подключением к государственным информационным системам и др. и работу со всеми видами служебной тайны и ДСП-информации, выглядит так: на недоверенном (личном) компьютере с внешнего защищённого носителя загружается преднастроенная замкнутая доверенная программная среда, из которой производится подключение и работа на служебном компьютере пользователя (или на виртуальном, если в организации развёрнута VDI).

При этом все задачи и все конфиденциальные документы обрабатываются внутри организации, не покидая его периметра, а на личный компьютер по защищённому каналу «прилетают» лишь отрисованные картинки экрана, а обратно "улетают" лишь скан-коды нажимаемых клавиш и координаты указателя мыши.
Пользователь, при этом, удалённо работает на своём рабочем компьютере, но – в терминальном режиме, в привычной для него среде (Windows, Linux). Все документы на своих привычных местах, доступ в ГИС, АСУ ТП, ИБС, ИСПДн и др., выход в Интернет (если разрешён), переучиваться не надо.

При этом локальные ресурсы его личного компьютера – жёсткие диски, NAS, флешки, принтеры и пр. – которые могут быть использованы в качестве канала утечки служебной информации, либо для организации атаки на ресурсы организации – в этом режиме заблокированы и недоступны. Использовать Aladdin LiveOffice можно ТОЛЬКО на авторизованных компьютера ("привязанных" к устройству), так что если устройство попало к злоумышленнику, и он знает от него пароль, то на незнакомом компьютере устройство не заработает, и подключиться к ИС организации злоумышленник не сможет.

Более того, пользователь не знает, а следовательно и не сможет дискредитировать, свой логин и пароль для удалённого подключения, адрес шлюза, настройки VPN и др. Пользователь также не сможет ни модифицировать преднастроенную программную среду, ни изменить её настройки, ни установить какое-то своё приложение, ни сохранить у себя, ни распечатать на локальный принтер служебный документ.

Ещё раз – вся работа производится на удалённом рабочем компьютере, в ИС организации. Мы считаем такой режим работы достаточно безопасным, никакой мистики.

Если сотрудник потеряет свою флешку Aladdin LiveOffice и её попробует использовать злоумышленник? Что будет, какие угрозы и риски для всех ИС организации?

Рисков практически нет, т.к. злоумышленник не сможет получить доступ к функционалу носителя и информации. В том числе за счёт использования жёсткой привязки админом компьютеров пользователя к устройству.

Много лет нам продвигалась тема BYOD (принеси и используй для работы свой девайс), многие активно это используют. Решение, которое сделал и сертифицировал Аладдин (Aladdin LiveOffice), использует технологию LiveUSB – загрузка замкнутой преднастроенной доверенной программной среды с недоверенного (домашнего – ЛИЧНОГО) компьютера сотрудника. Это, в каком-то смысле, тоже развитие технологии BYOD… Так в чём же принципиальные различия?
Почему смартфон нельзя, а личный домашний ПК, на котором играют дети, установлено чёрти что, могут сидеть трояны, вирусы – можно?

Смартфон использовать нельзя, потому что он не подходит в качестве средства вычислительной техники, используемого для подключения защищенного носителя, в соответствии с требованиями ФСТЭК.

4. Нормативные требования (идентификация и аутентификация)

Есть общепринятые понятия (термины) - парольная аутентификация, двухфакторная, многофакторная, биометрическая. Вы в своей презентации вводите новые, свои - простая, усиленная, строгая. Зачем?

Основные понятия, термины, определения, уровни доверия к идентификации и аутентификации, что для каких ИС надо применять - всё то, о чём я рассказывал, описано в российских национальных стандартах (ГОСТах), которые, кстати, разрабатывала наша компания (Аладдин).

В них есть понятия и определения и парольной аутентификации, и двухфакторной, и многофакторной, и биометрической, и допустимые сценарии их применения в ИС.

Действующие стандарты:

- **ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения**
- **ГОСТ Р 70262.1-2022 Защита информации. Идентификация и аутентификация. Уровни доверия идентификации**
- ГОСТ Р 59381-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции
- ГОСТ ISO/IEC 24760-2-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования.
- ГОСТ Р 59382-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 3. Практические приемы
- ГОСТ Р 59383-2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом
- ГОСТ Р 59515-2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности

Проекты стандартов (в стадии оформления и согласования, поэтому пока без номеров):

- **Защита информации. Идентификация и аутентификация. Уровни доверия аутентификации**
- Защита информации. Идентификация и аутентификация. Управления идентификацией и аутентификацией
- Защита информации. Идентификация и аутентификация. Типовые угрозы и уязвимости идентификации и аутентификации
- Защита информации. Идентификация и аутентификация. Рекомендации по управлению идентификацией и аутентификацией.

При проектировании ГИС и аутентификации для них следует ориентироваться на эти ГОСТы, а не на "научно-популярные" статьи из интернета.

Какой нормативной базой следует руководствоваться при организации удалённого доступа (аутентификации) сотрудников и контрагентов в ГИС?

Понятие государственных информационных систем (ГИС) определено в Федеральном законе от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

Согласно закону государственными информационными системами являются федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

За защиту информации в ГИС отвечает оператор такой системы.

Помимо понятия ГИС, федеральным законом №149-ФЗ вводится понятие "муниципальная информационная система" (ИС, созданная на основании решения органа местного самоуправления).

С точки зрения защиты информации государственные и муниципальные информационные системы – идентичны.

Нормативная база по защите информации в ГИС включает в себя:

- Федеральный закон "Об информации, информационных технологиях и о защите информации"
- "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (утверждены приказом ФСТЭК России № 17 от 11 февраля 2013 года)
- "Меры защиты информации в государственных информационных системах" (утверждены ФСТЭК России от 11 февраля 2014 года) – достаточно объёмный и подробный документ - 176 страниц
- Новые требования ФСТЭК России к защите информации в ГИС (проект).

Требования по обязательному применению сертифицированных средств для обеспечения безопасной дистанционной работы в ГИС регламентированы:

- Федеральным законом "Об информации, информационных технологиях и о защите информации" от 27.07.2006.
- Приказом ФСТЭК России от 11 февраля 2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
- Постановлением Правительства Российской Федерации от № 330.
- "Требований ФСТЭК России к средствам дистанционной работы" (ДСП), утверждены Приказом ФСТЭК №32.

Кроме того, для защиты информации, содержащейся и обрабатываемой в ГИС, в т.ч. при дистанционной работе, также действуют Требования ФСБ России, утверждённые приказом №524 от 24.10.2022 "О защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств", в т.ч. в части:

- защиты каналов связи (передачи информации)
- защиты (шифрования) данных на носителях информации
- обеспечения юридической значимости электронных документов и защиты от их подделки.

+7 (495) 223-00-01
aladdin@aladdin.ru
www.aladdin.ru