АУТЕНТИФИКАЦИЯ И ЭП С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИИ

Сергей ГРУЗДЕВ
генеральный директор «Аладдин Р.Д.»

Данная статья является продолжением материала «Аутентификация – от паролей к адаптивной МФА», опубликованного в BIS Journal № 3 (58) за 2025 год, и рассматривает особенности применения биометрических технологий для аутентификации и ЭП пользователей.

ПАРОЛИ

Использование паролей в качестве единственного фактора не позволяет обеспечить надежную аутентификацию пользователей информационных систем (ИС). Дополнительные риски связаны с новыми возможностями генеративного искусственного интеллекта, который (в частности, ChatGPT-4) собрал (и продолжает собирать) все возможные пароли, которые когда-либо были использованы для доступа к информационным сервисам и ресурсам, а учётная запись была взломана или украдена.

Теперь ИИ способен при определенных условиях практически мгновенно выдать[1] нужное значение, независимо от длины пароля или парольной фразы и мощности алфавита (количества используемых букв в разных регистрах, цифр и символов).

Организации, использующие только пароли (простую аутентификацию), не контролируют свой периметр и являются первейшими кандидатами на взлом и утечки.

СРЕДСТВА 2ФА (ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ)

В отличие от пароля (единственного фактора – запоминаемого секрета), здесь добавляется второй фактор – владение аппаратным устройством (USB или OTP-токеном, смарт-картой). При этом пароль (или PIN-код) является способом подтверждения факта владения данным устройством.

Долгое время считалось, что этого вполне достаточно, и средства 2ФА обеспечивают должный уровень безопасности при аутентификации пользователей и использовании ими электронной подписи (ЭП, квалифицированной ЭП, усиленной квалифицированной ЭП).

Что видим на практике, какие проблемы и риски безопасности для ИС?

1. Пресловутый «человеческий фактор»:

- Пользователи частенько передают свои средства 2ФА другим, а те подключаются и работают в ИС от их имени (нет привязки средства 2ФА к личности его владельца).
- Пользователи частенько забывают свой PIN-код, несколько раз подряд вводят его неправильно и устройство блокируется – возрастает простой и нагрузка на администраторов.
- Использование PIN-кода, установленного по умолчанию (вопиющие ошибки администрирования) – как следствие, теряется фактор знания – «секрета» для разблокирования аппаратного средства.

2. Удалённая работа, в т.ч. из недоверенной среды:

- Многие пользователи работают удалённо, в т.ч. подключаются к ИС с домашних/личных компьютеров, которые могут скрытно управляться злоумышленниками, на которые могут быть подсажены специализированные трояны, в т.ч. реализующие атаки с подменой подписываемых документов.

Первая проблема – обычные средства 2ФА и ЭП (USB-токены и смарт-карты) не защищают от таких рисков и подобных атак.

Для защиты от них следует использовать специализированные средства обеспечения безопасной дистанционной работы пользователей из недоверенной среды, соответствующие требованиям 32-го Приказа ФСТЭК России, например, Aladdin LiveOffice[2].

Такие же требования к организации удалённого доступа для пользователей организации, её контрагентов и подрядных организаций содержатся и новом 117-м Приказе ФСТЭК России.

Вторая проблема, возникающая при удалённой работе, особенно для администраторов и привилегированных пользователей, имеющих расширенный доступ к ИС организации и расширенные полномочия (а как следствие – повышенные риски причинить существенный ущерб) – это подтверждение личности пользователя.

Помним, что чем больше риск, тем больше методов и способов для подтверждения личности пользователя следует применять[3].

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

[2] См. описание продукта https://www.aladdin-rd.ru/catalog/liveoffice/

[3] См. ГОСТ Р 70262.2-2025 (Идентификация и аутентификация. Уровни доверия аутентификации), разработчик «Аладдин Р.Д.».

Средства 2ФА являются обязательными и надёжными при работе пользователей в офисе, в доверенной среде исполнения (на администрируемых организацией средствах вычислительной техники (СВТ)).

Однако они не обеспечивают требуемого уровня информационной безопасности (ИБ) при дистанционной работе и работе из недоверенной среды (личные СВТ, не контролируемые и не администрируемые организацией).

БИОМЕТРИЯ

Для подтверждения личности пользователя с учётом упомянутого «человеческого фактора» применяется биометрия. В сфере ИТ и ИБ она стала применяться относительно недавно, и ей, естественно, свойственны многие «детские» болезни — неправильное применение, ошибки реализации и пр.

Давайте разбираться подробнее. Начнём с основ и сфокусируемся на применении биометрии для решения задач аутентификации, ЭП и прохода (доступа) на объекты критической информационной инфраструктуры (КИИ).

Основы биометрии. Краткие выжимки из учебного пособия[4].

Биометрия делится:

- На контактную и бесконтактную.
- По месту и способу хранения биометрических данных — с единой централизованной базой и без неё, с использованием так называемого «распределённого» хранения данных.

Контактная биометрия — к ней относится технология распознавания по отпечаткам пальцев, ладоней и пр.

Бесконтактная биометрия — технология распознавания по лицу, голосу и пр. (лежит в основе ЕБС).

И сразу по тексту книги предупреждение, большими буквами:

Категорически не допускается использование бесконтактной биометрии для целей идентификации и аутентификации пользователей в ИС и для доступа на объекты КИИ.

Почему? Да потому что авторы книги, настоящие профессионалы, еще в 2003–2004 гг. прекрасно понимали и предсказывали, что за 10 лет генеративный ИИ разовьётся до такого уровня, что на лету сможет генерировать нужный для обмана системы голос и видео.

Что мы сегодня и наблюдаем — расцвет дипфейков и доступность инструментов для их создания. Эта первая и самая важная проблема.

Вторая существенная проблема — централизованное хранение собираемых персональных биометрических данных. Защитить такую базу практически невозможно[5], следовательно, будут утечки. В отличие от паролей или средств 2ФА, которые можно оперативно перевыпустить, с биометрией такой фокус не проходит. Разве что массово делать пластические операции?

Третья проблема — при правильной реализации это достаточно дорого (защита среды исполнения, канала, базы данных и пр.).

То, что нам продолжают навязывать использование ЕБС для целей аутентификации в ИС и доступа на объекты КИИ — это просто опасно.

Контактная биометрия. Лидером здесь является технологии распознавания по отпечаткам пальцев (Fingerprint). Что важно и оказывает существенное влияние на надёжность и безопасность её использования?

1. Используемая технология:
   - идентификация (один отпечаток ко многим из базы данных);
   - верификация (один к одному — сравнение предъявленного отпечатка с эталоном).
2. Место хранения биометрических данных (эталонных шаблонов с привязкой к персональным данным пользователя):
   - централизованное хранение (база данных);
   - распределённое хранение эталонных шаблонов (без единой базы данных):

   a) в защищённой среде — в персональном аппаратном устройстве пользователя — токене, смарт-карте;

   b) в незащищённой среде (например, в компьютере пользователя или в общем терминале доступа).
3. Тип сканера отпечатков пальцев и его расположение:
   - оптический или полупроводниковый;
   - внешний или встроенный в персональное устройство или в терминал доступа.

Оптический сканер делает фото отпечатка пальца. А дальше передает его в терминал или в компьютер для обработки и отправки на сравнение с эталоном. Эталон может находиться в базе данных или в персональном устройстве (токене, смарт-карте).

Недорогой сканер можно достаточно просто обмануть, подсунув ему отпечаток, снятый, например, с использованного стакана. Хороший оптический сканер значительно дороже и существенно больше — с собой его носить уже накладно и неудобно.

Основная проблема — передача отпечатков пальцев в ИС. Это делает её владельца оператором персональных биометрических данных со всеми вытекающими...

Полупроводниковые сканеры, как правило, емкостные, существенно дешевле, надёжнее и компактнее, что позволяет размещать их «на борту» специализированных устройств аутентификации и ЭП, не передавать снятые отпечатки пальцев в ИС, а обрабатывать их и производить сравнение с шаблоном (верификацию 1:1) внутри аппаратного устройства.

Различают два типа полупроводниковых сканеров — протяжные (щелевые — когда палец нужно аккуратно протащить через неё), и прижимные, когда палец нужно прижать к сенсору.

Протяжные сканеры снимают с движущегося пальца серию отпечатков (полосок), а далее с помощью специального программного обеспечения (ПО) склеивают их в единое изображение. Качество получающегося изображения плохое, надежность, как правило, не превышает 1:10 — 1:100. Дешевая никчёмная игрушка.

Прижимные сканеры сразу дают полноценную «картинку» и обеспечивают надёжность на уровне от 1:10,000 до 1:100,000.

[4] Настоятельно рекомендую прочитать книгу «Руководство по биометрии», Р.М. Болл, Дж.Х. Коннел, изд. Техносфера, 2007

[5] Знаю это не понаслышке, наша компания занимается этим более 20 лет

Рисунок 1. Персональный BIO-токен и Aladdin SecurBIO Reader

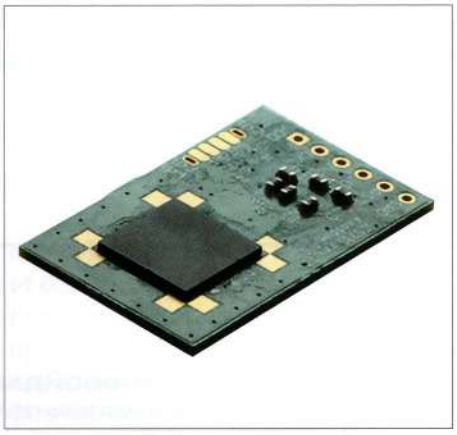

Рисунок 2. OEM-модуль для встраивания в оборудование

Для контактной биометрии это предел. Почему? Потому что на планете Земля с вероятностью 1:100,000 у каждого из нас существует «биологический двойник» с такими же отпечатками. Доказанный факт.

Обмануть полупроводниковый сканер с оставленным на стакане жировым отпечатком не получится.

Что ещё важно знать? Практически все полупроводниковые сканеры поставляются на рынок (производителям электроники) в виде сборок – сенсор + чип.

В чипе реализована необходимая математика, и при сравнении предъявленного отпечатка с сохранённым в чипе шаблоном, на выходе получаем 0 (отказ) или 1 (совпадение) – такой вот простейший тумблер – «свой/чужой». Элементарное изменение в схемотехнике – и ты всегда «свой».

Увы, но многие производители электроники и средств защиты информации (СЗИ) с использованием биометрии допускают эту детскую ошибку, обнуляя их безопасность.

ALADDIN SecurBIO

Под этим названием компания «Аладдин» недавно выпустила три новых продукта:

- Персональный BIO-токен.
- Смарт-карт ридер со встроенным сканером отпечатков пальцев и смарт-карты для безопасного хранения шаблонов.
- OEM-модуль на базе BIO-токена для встраивания в оборудование (для производителей терминалов, компьютеров и пр.).

Персональный BIO-токен. Обеспечивает «привязку» личности пользователя к физическому носителю (USB-токену с встроенным прижимным полупроводниковым сенсором) и невозможность его передачи и использования посторонними (рис. 1).

Для начала работы с BIO-токеном его необходимо разблокировать, приложив к сканеру палец. После снятия отпечатка внутри BIO-токена производится его оцифровка и получение шаблона – аналога однонаправленной хеш-функции, и далее – сравнение с ранее сохранённым в чипе BIO-токена эталонным шаблоном. При совпадении с заданной вероятностью[6] предъявляемого шаблона с эталоном все необходимые функции BIO-токена разблокируются, и он «превращается» в привычный USB-токен JaCarta PKI/ГОСТ – средство строгой или усиленной аутентификации и ЭП.

Важно: отпечатки пальцев не попадают ни в компьютер, ни в ИС, а владелец ИС не становится оператором персональных биометрических данных (в отличие от ЕБС).

СМАРТ-КАРТ РИДЕРЫ И СМАРТ-КАРТЫ С ПОДДЕРЖКОЙ БИОМЕТРИИ

Aladdin SecurBIO Reader – семейство профессиональных смарт-карт ридеров Enterprise-класса с встроенным прижимным полупроводниковым сканером отпечатков пальцев (рис. 1):

- JCR761 – смарт-карт ридер с горизонтальной загрузкой смарт-карты.
- JCR781 – смарт-карт ридер с вертикальной загрузкой смарт-карты.

Рекомендуется для организации совместной или сменной работы пользователей за одним рабочим местом (один ридер и у каждого своя смарт-карта с загруженными в неё эталонными шаблонами отпечатков пальцев), при использовании одной смарт-карты (с RFID) для доступа на объект/в помещения, для интеграции со средствами контроля и управления доступом (СКУД).

Преимущества. BIO-токены/ридеры и смарт-карты позволяют реализовать как трёхфакторную аутентификацию (3ФА), так и 2ФА, отказавшись от использования паролей (PIN-кодов), и убрать тот самый пресловутый «человеческий фактор». При этом останется фактор владения физическим устройством и биометрический фактор – разблокировать и использовать устройство сможет только его владелец.

РЕЗЮМЕ

Внедрение аутентификации и ЭП с использованием биометрии позволит отказаться от использования паролей и кардинально решить проблему «человеческого фактора», правильно и эффективно распределить бюджет на ИБ.

Надёжная система аутентификации в ИС – основа и залог её безопасности.

[6] FAR и FRR можно настраивать, добиваясь значений 1:10,000 – 1:100,000