УЧИТЫВАТЬ ПРИ ВЫБОРЕ

ПОМОЩЬ ТЕОРИИ ПРИ ИМПОРТОЗАМЕЩЕНИИ СРЕДСТВ АУТЕНТИФИКАЦИИ

Алексей САБАНОВ
доктор технических наук, профессор кафедры защиты информации МГТУ им. Н.Э. Баумана, заместитель генерального директора АО «Аладдин Р.Д.»

В связи с приостановлением работы и ухода ряда крупных западных поставщиков средств аутентификации с российского рынка перед банками встала срочная задача быстрого выбора адекватного отечественного решения. В данной статье обсуждаются некоторые существенные проблемы, сопутствующие такому выбору, а также аспекты, которые надо учитывать в первую очередь, чтобы не потерять имеющийся уровень защищённости доступа к информационным ресурсам. Значительная часть изложенного ниже материала опирается на обзоры международных стандартов и зарубежной нормативной базы [1–3], основной международный стандарт по аутентификации [4], принятые национальные стандарты по идентификации и аутентификации [5–9] и находящиеся на разных стадиях принятия проекты стандартов, в которых аутентификация рассматривается с точки зрения уверенности в получаемых результатах. Также в статье используются основные положения научных статей, в которых рассмотрены наиболее используемые процессы [10] и методы формирования уровней доверия к результатам аутентификации [11], подробно исследованы методы двухфакторной аутентификации [12], выявлены риски идентификации [13,14] и аутентификации [15], рассмотрены национальные рекомендации по идентификации и аутентификации США [16] и Канады [17], а также сформированы качественные [18, 19] и количественные показатели уровня рисков ошибочной аутентификации [20].

НЕКОТОРЫЕ ПРОБЛЕМЫ ИМПОРТОЗАМЕЩЕНИЯ

О необходимости применения идентификации и аутентификации (ИА) указывается во многих федеральных законах и подзаконных актах, однако практически нигде не указано, КАК должна строиться система ИА. В работах [1–3] сделан вывод о том, что нормативная база в части регулирования ИА недостаточно развита, о чём можно судить по весьма скромному по полноте и качеству содержания отечественной базы технических спецификаций (стандартов, методик, руководств), методов, протоколов и технологий ИА. В условиях нуждающейся в совершенствовании нормативно-правовой базы и недостатка утверждённых методических рекомендаций уполномоченных органов выбор методов и средств ИА отдан на откуп владельцам или операторам ИС. В таких условиях для построения эффективных систем ИА одним из путей решения является опора на научную базу.

Интернет полон статей «специалистов» по ИА с подчас сомнительными советами по использованию средств ИА. Средний уровень (аналог «средней температуры по больнице») таких «советов» часто можно оценить как низкий.

Одной из традиционных задач безопасности является поиск компромисса между безопасностью и удобством пользователей. Зачастую в погоне за удобством теряется защищённость и обоснованность выбора методов и средств ИА.

Чтобы корректно решать указанные проблемы, углубимся в интенсивно развивающуюся теорию доверия к результатам аутентификации. Кратко рассмотрим общую теорию, виды и средства аутентификации, а также типовые ошибки при выборе вида и средств аутентификации.

ВИДЫ И СРЕДСТВА АУТЕНТИФИКАЦИИ

В соответствии с [5] при организации доступа должен использоваться один из видов аутентификации: простая, усиленная или строгая. При простой аутентификации применяется однофакторная односторонняя аутентификация с организацией передачи аутентификатора от субъекта доступа к объекту доступа. При усиленной аутентификации применяется многофакторная односторонняя аутентификация или многофакторная взаимная аутентификация с организацией обмена аутентификационной информацией между субъектом доступа и объектом доступа. При строгой аутентификации должна применяться многофакторная взаимная аутентификация с организацией двухстороннего, между субъектом доступа и объектом доступа, или многостороннего (при использовании третьей доверенной стороны) обмена аутентификационной информацией. В процессе перечисленных видов аутентификации должны использоваться криптографические протоколы аутентификации, соответствующие виду организации обмена сообщениями между участниками процесса аутентификации. При аутентификации могут использоваться следующие средства аутентификации:

- Запоминаемый секрет (например, пароль). При аутентификации с помощью данного средства аутентификации используется фактор знания — подтверждается знание секрета.
- Поисковый секрет (например, одноразовый пароль). Представляет собой физическую или электронную запись, в которой хранится совокупность секретов, формируемых для субъекта доступа регистрирующей стороной. При аутентификации с помощью данного средства аутентификации используется фактор владения (подтверждается обладание и контроль над аутентификатором).
- Внеполосный аутентификатор («второй канал», например смартфон). Представляет собой зарегистрированное устройство, которое является уникально адресуемым и может взаимодействовать с доверяющей стороной по отдельному каналу связи, называемому вторым каналом. При аутентификации с помощью данного средства аутентификации используется фактор владения (обладание и контроль над аутентификатором). Внеполосный аутентификатор, как правило, применяется совместно с другими аутентификаторами.
- Однофакторный генератор одноразовых паролей (OTP — One Time Password). При аутентификации используется фактор владения (обладание и контроль над аутентификатором).
- Многофакторный генератор одноразовых паролей. Используется фактор владения (обладание и контроль над аутентификатором) совместно с фактором знания и/или с биометрическим фактором.
- Однофакторное криптографическое программное средство аутентификации. Представляет собой криптографические ключи и программу, осуществляющую криптографические операции, которые хранятся на носителе, входящем в состав СВТ или аналогичного устройства. При аутентификации используется фактор владения (обладание и контроль над криптографическими ключами).
- Однофакторное криптографическое техническое средство аутентификации. Осуществляет хранение выработанных и/или импортированных в него криптографических ключей, а также выполняет криптографические операции с их использованием и представляет результаты через непосредственное соединение с СВТ. При аутентификации используется фактор владения (подтверждается обладание и контроль над криптографическими ключами).
- Многофакторное криптографическое программное средство аутентификации. Доступ к криптографическим ключам осуществляется с использованием второго фактора аутентификации, представляющего собой информацию, полученную с клавиатуры СВТ (пароль, PIN-код и т.п.) или биометрического считывающего устройства. Используется фактор владения (обладание и контроль над криптографическими ключами) совместно с фактором знания и/или с биометрическим фактором.
- Многофакторное криптографическое техническое средство аутентификации. Устройство аутентификации осуществляет хранение самостоятельно выработанных и/или импортированных в него криптографических ключей, а также выполняет криптографические операции с их использованием. Доступ к криптографическим ключам и/или результатам криптографических операций осуществляется с использованием второго фактора аутентификации. Используется фактор владения (обладание и контроль над криптографическими ключами) совместно с фактором знания и/или с биометрическим фактором.
- Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом. Устройство аутентификации вырабатывает закрытые неизвлекаемые криптографические ключи, а также выполняет криптографические операции с их использованием и представляет результаты через непосредственное соединение с СВТ. Использование криптографических ключей и/или результатов криптографических операций осуществляется после активации второго фактора аутентификации. Используется фактор владения (обладание и контроль над криптографическими ключами) совместно с фактором знания и/или с биометрическим фактором.

УРОВНИ ДОВЕРИЯ

Уровень доверия аутентификации определяет достигнутую уверенность в том, что субъект доступа действительно является тем **зарегистрированным** субъектом доступа, за кого себя выдаёт предъявленным идентификатором. Уровень доверия аутентификации определяет необходимые к применению вид аутентификации и средства аутентификации. Устанавливаются три уровня доверия аутентификации: низкий уровень доверия (некоторая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом, за кого себя выдаёт предъявленным идентификатором доступа), обеспечиваемый простой аутентификацией; средний уровень доверия (умеренная уверенность), обеспечиваемый усиленной аутентификацией; высокий уровень доверия (значительная уверенность в том, что субъект доступа действительно является зарегистрированным субъектом, за кого себя выдаёт предъявленным идентификатором), обеспечиваемый применением строгой

Уровень доверия аутентификации	**Уверенность в результатах аутентификации**	**Необходимые**		**Допустимые**	
		виды аутентификации	средства аутентификации	виды аутентификации	средства аутентификации
1	2	3	4	5	6
Низкий	Некоторая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа	Простая	Запоминаемый секрет, поисковый секрет, однофакторный генератор одноразовых паролей	Простая, усиленная, строгая	Многофакторный генератор OTP, однофакторное криптографическое программное средство, однофакторное криптографическое техническое средство, многофакторное криптографическое программное средство, многофакторное криптографическое техническое средство, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
Средний	Умеренная уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа	Усиленная	Многофакторный генератор OTP или совместно с запоминаемым секретом должны использоваться поисковый секрет, или внеполосное устройство, или однофакторный генератор OTP, или однофакторное криптографическое ПО аутентификации, или однофакторное криптографическое техническое средство аутентификации	Усиленная, строгая	Многофакторное криптографическое программное средство, многофакторное криптографическое техническое средство, многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
Высокий	Высокая уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа при условии, что субъект доступа знает, обладает и контролирует используемые средства аутентификации	Строгая	Многофакторное криптографическое техническое средство, или однофакторное криптографическое техническое средство совместно с запоминаемым секретом, или многофакторный генератор OTP совместно с однофакторным криптографическим техническим средством, или однофакторный технический генератор OTP совместно с многофакторным криптографическим программным средством, или однофакторный технический генератор OTP совместно однофакторным криптографическим программным средством аутентификации и запоминаемым секретом	Строгая	Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом
Очень высокий	Максимальная уверенность в том, что субъект доступа действительно является тем зарегистрированным субъектом доступа, за кого себя выдаёт предъявленным идентификатором доступа	Строгая	Многофакторное криптографическое техническое средство аутентификации с неизвлекаемым ключом	–	–

Таблица 1. Уровни доверия аутентификации

аутентификации. Допускается использование строгой или усиленной аутентификации для обеспечения требуемого в конкретной среде функционирования низкого уровня доверия, а также использование строгой аутентификации для обеспечения требуемого среднего уровня доверия. Результаты такого рассмотрения сведены в таблицу 1.

Из анализа таблицы видно, что с низкого по высокий уровни доверия могут достигаться разными комбинациями видов и средств аутентификации, а очень высокий уровень доверия — с применением только одного средства аутентификации с неизвлекаемым ключом. Согласно результатам работ [4, 13,15] выбор метода аутентификации должен определяться результатами анализа рисков доступа к конкретной транзакции или проникновения к информационному ресурсу злоумышленника под видом легального пользователя.

НЕКОТОРЫЕ ТИПОВЫЕ ОШИБКИ

К сожалению, в большинстве случаев двухфакторной аутентификацией часто называют совсем не те виды и средства аутентификации, которые были рассмотрены в предыдущем разделе. Так, последовательное (не одновременное) применение одного или различных однофакторных методов аутентификации не является 2ФА. Такая аутентификация согласно [5] называется многошаговой. Более того, надёжность такой аутентификации определяется надёжностью самого слабого звена. Типичным примером такой аутентификации является последовательная аутентификация сначала к СВТ, затем к компьютерной сети, затем к информационному ресурсу или прикладной программе. Защищённость такой последовательной аутентификации определяется защищённостью самого слабого шага. Например, если при этом на каждом шаге применяются пароли, то аутентификация является однофакторной, а оценка защищённости всей цепочки шагов определяется самым слабым паролем.

Второй наиболее распространённой в последнее время ошибкой является отнесение аутентификации к 2ФА при использовании двух или более биометрических характеристик (например, лицо и голос). Строго говоря, такой процесс должен называться не аутентификацией, а идентификацией. Статья 7.7 стандарта [5] говорит о том, что «применение фактора биометрического в качестве единственного фактора при однофакторной аутентификации не допускается», а в рассматриваемом случае дважды используется именно биометрический фактор.

Ещё одной ошибкой является отнесение аутентификации к 2ФА при использовании только вероятностных (не детерминированных) характеристик, примером которых является определение местоположения, имеющего погрешности обсервации, обусловленные точностью позиционирования. В качестве второго примера можно привести применение биометрии, характеристики которой всегда содержат ошибки первого и второго рода.

ЗАКЛЮЧЕНИЕ

Показано, что «результирующая» уверенность в результатах аутентификации зависит не только от применяемого вида, но и от используемых при этом средств аутентификации. Существенную роль при этом играют методы и результаты первичной идентификации субъекта доступа, а также способ хранения секрета, используемого в качестве аутентификационной информации. Чем выше уровень доверия первичной идентификации, способ хранения секрета и применяемые вид и средства аутентификации, соответствующий данному уровню доверия, тем к более высокорисковым транзакциям можно допускать субъекта после успешной аутентификации. При этом уровни доверия всех трёх составляющих (первичная идентификация, вид и средства аутентификации, способ хранения секрета) должны соответствовать друг другу. Предлагается учитывать вышеизложенное при выборе импортозамещающих вида и средств аутентификации.

ЛИТЕРАТУРА

1. *Кузьмин А. С.*, *Сабанов А. Г.* Анализ зарубежной нормативной базы по идентификации и аутентификации. Инженерный журнал: наука и инновации. 2013. Вып. 11 (23). С. 1–13.
2. *Сабанов А. Г.* Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 1 // Инсайд. Защита информации. Часть 1. 2016. № 2 (68). С. 84–87.
3. *Сабанов А. Г.* Общий анализ международных стандартов по идентификации и аутентификации при доступе к информации. Часть 2 // Инсайд. Защита информации. 2016. № 3. С. 70–74.
4. ISO/IEC29115:2013 «Information technology — Security techniques — Entity authentication assurance framework» https://www.iso.org/standard/45138.html
5. ГОСТ Р 58833–2020 Защита информации. Идентификация и аутентификация. Общие положения. https://docs.cntd.ru/document/1200172576
6. ГОСТ Р 59383–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом. https://docs.cntd.ru/document/1200179662
7. ГОСТ Р 59515–2021 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности. https://docs.cntd.ru/document/1200179667
8. ГОСТ Р 59381–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции. https://docs.cntd.ru/document/1200179660
9. ГОСТ ISO/IEC24760–2–2021 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 2. Базовая архитектура и требования. https://docs.cntd.ru/document/1200180228
10. *Сабанов А. Г.* Классификация процессов аутентификации // Вопросы защиты информации. 2013. № 3 С. 46–52.
11. *Сабанов А. Г.* Уровни доверия к результатам идентификации и аутентификации субъекта доступа в период цифровой трансформации // Вопросы кибербезопасности. 2019. № 5 (33). С. 19–25.
12. *Сабанов А. Г.* Методы двухфакторной аутентификации // Инсайд. Защита информации. 2021. № 6. С. 52–56.
13. *Сабанов А. Г.* Концепция предварительного анализа рисков первичной идентификации субъектов доступа // Инсайд. Защита информации. 2020. № 2. С. 74–79.
14. *Сабанов А. Г.*, *Шубинский И. Б.* Метод анализа технологических рисков первичной идентификации субъектов доступа// Инсайд. Защита информации. 2020. № 3. С. 57–61.
15. *Сабанов А. Г.* О применимости методов управления рисками к процессам аутентификации при удаленном электронном взаимодействии // Электросвязь 2014. № 6. С. 39–42.
16. *Paul A.* Grassi, James L. Fenton, Elaine M. Newton and others. NIST Special Publication 800–63 — B. Authentication and Lifecycle Management. June 2017. https://pages.nist.gov/800–63–3/sp800–63b.html, https://doi.org/10.6028/NIST.SP.800–63b
17. Canada User Authentication Guidance for Information Technology Systems https://www.csecst.gc.ca/en/system/files/pdf_documents/itsp.30.031v3-eng_0.pdf
18. *Сабанов А. Г.* Уровни доверия к аутентификаторам // Вопросы защиты информации. 2019. № 2. С. 10–17.
19. *Сабанов А. Г.* Аутентификация и системы разграничения доступа: концепция оценки доверия к результатам // Инсайд. Защита информации. 2021. № 2. С. 10–17.
20. *Жиляев А. Е.*, *Сабанов А. Г.*, *Брагин Д. С.*, *Шелупанова П. А.*, *Мицель А. А.*, *Катаев М. Ю.* Подход к формированию уровней доверия для оценки рисков ошибок аутентификации // Вопросы защиты информации. 2022. № 1. С. 17–22.