БЕЗОПАСНАЯ АУТЕНТИФИКАЦИЯ — ФУНДАМЕНТ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Леонид ШАПИРО
руководитель Центра Компетенций Аладдин

1. КРАТКОЕ РЕЗЮМЕ

Четыре крупнейших отчёта о киберугрозах 2024–2025 годов — Verizon DBIR2025, Microsoft Digital Defense Report 2025, CrowdStrike Global Threat Report 2025 и отчёт российской компании Positive Technologies, специализирующейся на киберзащите, — независимо друг от друга приходят к одному выводу: подавляющее большинство успешных взломов начинается с компрометации учётных данных, а не с технической эксплуатации уязвимостей.

Очевидно, что необходимо кардинальное изменение модели аутентификации — переход от паролей, то есть однофакторной аутентификации на основе запоминаемых данных, к двухфакторной аутентификации на основе технологий асимметричной криптографии и аппаратных устройств (смарт-карты, USB-токены).

Это является не просто техническим улучшением, а стратегическим решением, непосредственно устраняющим доминирующий вектор атак. Этот вывод дополнительно подтверждается результатами внедрения этих технологий безопасной аутентификации крупнейшими мировыми корпорациями, такими как Microsoft и Google.

Стоит также учитывать тот факт, что использование строгой аутентификации является базовым требованием российских регуляторов для широкого спектра компаний как государственных, так и коммерческих.

Эта статья является продолжением материалов компании «Аладдин» об аутентификации, опубликованных в BIS Journal № 1 (60) за 2026 год [23] и в BIS Journal № 3 (58) за 2025 год [24].

2. ОСНОВНЫЕ УГРОЗЫ ИЛИ ЧТО ГОВОРЯТ АНАЛИТИЧЕСКИЕ ОТЧЁТЫ...

2.1. Кража учётных данных — доминирующий вектор атак. Отчёт Verizon DBIR2025, основанный на анализе 22 052 инцидентов и 12 195 подтверждённых утечек данных в 139 странах, говорит, что кража учётных данных остаётся важнейшим вектором первоначального доступа, присутствуя в 22% всех утечек [1]. Похожую статистику в этой категории инцидентов предоставляет отчёт центра противодействия кибератакам ГК «Солар» Solar JSOC. По его данным, несанкционированный доступ составляет 23% от общего количества атак [22].

При этом в атаках на базовые веб-приложения этот показатель достигает 88%. Другими словами, почти в 9 из 10 случаев атаки на веб-сервисы атакующий не взламывает систему, а просто использует чужие учётные данные [1].

Ситуацию усугубляет катастрофическое качество паролей: лишь 3% скомпрометированных паролей удовлетворяли базовым требованиям сложности [1]. «Лаборатория Касперского» установила, что 54% паролей, утёкших в 2025 году, уже были замечены в более ранних утечках. Средний срок жизни пароля составляет 3,5–4 года [15].

Атаки методом перебора (brute-force) на веб-приложения утроились за год — с примерно 20% до 60%. При этом credential stuffing (вброс скомпрометированных пар логин-пароль) составляет в медиане 19% всех попыток аутентификации в корпоративных системах, а в крупных enterprise-организациях достигает 25% [1],[2]. Microsoft Digital Defense Report 2025 подтверждает эту картину данными принципиально иного масштаба: компания фиксирует более 600 миллионов атак на учётные данные в сутки, из которых 97% — это попытки массового перебора паролей. Microsoft блокирует свыше 7000 парольных атак в секунду. Несмотря на это, лишь 41% корпоративных пользователей в мире защищены какой-либо формой многофакторной аутентификации [3].

2.2. Рост атак с помощью инфостилеров[1]. Отдельный вектор угрозы — инфостилеры, которые не взламывают аутентификацию, а похищают готовые учётные данные из хранилищ браузеров, менеджеров паролей и операционной системы.

По данным DBIR2025, 30% корпоративных устройств были обнаружены в логах инфостилеров. Что особенно тревожно, 46% устройств с корпоративными логинами в этих логах являются неуправляемыми устрой-

[1] Инфостилер (англ. infostealer, information stealer) — это класс вредоносного ПО, обеспечивающего сбор конфиденциальных данных с заражённого устройства и их передачу злоумышленникам.

ствами (BYOD, личные компьютеры сотрудников), то есть высока вероятность, что никакие корпоративные средства защиты на них не применялись [1],[3].

Проводя анализ жертв, имена которых были опубликованы на сайтах утечек ransomware-групп, исследователи Verizon обнаружили: 54% этих жертв имели свои домены в дампах с украденными учётными данными, а 40% — корпоративные email-адреса. Это прямое доказательство взаимосвязи и совместной работы: инфостилер собирает учётные данные, брокер первоначального доступа передаёт доступ, а ransomware-группа применяет его для атаки [1].

Positive Technologies фиксирует аналогичный тренд для России и СНГ. За Q4 2024 — Q1 2025 учётные записи стали целью кражи в 24% успешных атак на организации. При этом по данным расследований PT Expert Security Center, ключевой причиной успешности кибератак названо отсутствие двухфакторной аутентификации наряду с устаревшим ПО и недостаточной сегментацией сети [5], [6].

Метрика	Значение	Источник
Доля утечек, начавшихся с украденных учётных данных	22%	Verizon DBIR2025
Категории подтверждённых инцидентов в 2025 (НСД)	23%	ГК «Солар» Solar JSOC
Доля атак на веб-приложения через украденные учётные данные	88%	Verizon DBIR2025
Средняя стоимость утечки через скомпрометированные учётные данные	$4,81M	IBM Cost of Data Breach 2025
Среднее время обнаружения утечки через учётные данные	292 дня	IBM Cost of Data Breach 2025
Средняя глобальная стоимость утечки данных	$4,44M	IBM Cost of Data Breach 2025
Рост числа голосового фишинга (vishing)	+442%	CrowdStrike CTR2025
Рост активности брокеров первоначального доступа	+50%	CrowdStrike CTR2025
Доля облачных инцидентов через легитимные учётные записи	35%	CrowdStrike CTR2025
Пароли, выставленные на продажу в 2024 г.	2,8 млрд	Verizon DBIR2025

Таблица 1. Сводные данные

3. СВОДНЫЕ ДАННЫЕ (КЛЮЧЕВЫЕ ЦИФРЫ ГЛОБАЛЬНЫХ ОТЧЁТОВ)

Если свести в одну таблицу метрики из нескольких глобальных отчётов, то нетрудно заметить удручающую картину с безопасностью учётных данных, сроками обнаружения утечек и их стоимостью (таблица 1).

4. ПОЧЕМУ АУТЕНТИФИКАЦИЯ — ОСНОВА БЕЗОПАСНЫХ СИСТЕМ

Аутентификация определяет границу между «своим» и «чужим» субъектом для любой информационной системы. Если этот барьер преодолён, то все последующие меры защиты теряют значительную часть своей эффективности или полностью становятся бесполезными. Злоумышленник, вошедший от имени легитимного пользователя, будет действовать со всеми его полномочиями. В ряде случаев можно говорить о полной компрометации всей информационной системы.

Таким образом, можно считать безопасную аутентификацию основой построения безопасных систем. Ещё три аргумента дополнительно подтверждают этот вывод.

1. Статистическое доминирование. Компрометация учётных данных устойчиво лидирует среди всех векторов первоначального проникновения на протяжении более чем десятилетия, по данным как Verizon DBIR, так и CrowdStrike Global Threat Report 2025 [1], [7].

2. Экономический ущерб. Утечки через украденные учётные данные обходятся в среднем в $4,81 млн за инцидент. Среднее время обнаружения такого события составляет 292 дня (IBM Cost of Data Breach Report 2025) [8].

3. Эффект домино. Получив легитимный доступ, атакующий компрометирует контроллеры домена (21% инцидентов), внутренние информационные системы (19%), серверы средств защиты информации (11%) — создавая каскадный эффект разрушения, что видно из исследования Positive Technologies [9].

5. ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ КАК СИСТЕМНЫЙ ОТВЕТ НА УГРОЗЫ ПОХИЩЕНИЯ УЧЁТНЫХ ДАННЫХ

5.1. Технологии асимметричной криптографии — ответ на кражу учётных данных. Прежде чем рассматривать конкретные сценарии защиты посредством технологий открытых ключей, необходимо понять, почему именно предлагаемый подход принципиально отличается от доступа по запоминаемому паролю и как именно будет организовано противодействие известным атакам. Пароль — это запоминаемая секрет-

ная информация, существующая в памяти пользователя, в базе данных сервиса аутентификации и в канале передачи данных. Уязвимости могут существовать во всех областях, следовательно, и атаки могут осуществляться на клиента, сервер и среду передачи.

Технологии инфраструктуры открытых ключей (PKI) предусматривают, что пользователю принадлежит ключевая пара, состоящая из закрытого и открытого ключей, где закрытый ключ должен храниться в защищённом аппаратном устройстве (смарт-карта, USB-токен) и никогда не покидать это устройство (принцип неизвлекаемости).

В процессе аутентификации используется закрытый ключ для подписи криптографического запроса (challenge), который проверяется сервером с помощью открытого ключа, хранящегося в сертификате, который распространяется свободно, и его перехват не несёт угрозы безопасности.

CISA (Агентство США по кибербезопасности и защите инфраструктуры) признаёт лишь два метода аутентификации «золотым стандартом» в категории phishing-resistant MFA: FIDO/WebAuthn и PKI-based Certificate Authentication. Все иные методы (SMS, OTP, push-уведомления) не входят в этот список, поскольку уязвимы к AiTM[2] и социальной инженерии [11].

6. АНАЛИЗ СЦЕНАРИЕВ ТИПОВЫХ АТАК НА УЧЁТНЫЕ ДАННЫЕ

Рассмотрим, каким образом PKI обеспечивает противодействие основным сценариям кражи учётных данных, описанных в аналитических отчётах.

6.1. Фишинг с поддельной страницей входа. При аутентификации с помощью технологий асимметричной криптографии и использовании смарт-карт и USB-токенов аутентификационный ответ привязан к домену запрашивающей стороны. Если злоумышленник создаёт поддельный домен corp-nwtraders.com вместо nwtraders.msft, токен просто не сформирует ответ, поскольку система автоматически обнаружит несовпадение домена без какого-либо участия пользователя. Это даёт возможность противостоять фишингу техническими методами, а не ориентироваться на осведомлённость и бдительность пользователя.

6.2. Инфостилер на персональном устройстве. Инфостилеры охотятся за паролями в браузерах, Windows Credential Manager и других менеджерах паролей. При PKI-аутентификации паролей как объекта для кражи просто не существует.

6.3. Повторное использование паролей (Credential Stuffing[3]). Если пользователь переходит на двухфакторную аутентификацию на основе асимметричной криптографии и перестаёт использовать пароли, то атаки на повторное использование паролей теряют всякий смысл, поскольку система не будет принимать ничего, кроме подписанного challenge от зарегистрированного пользователя с сертификатом.

6.4. Prompt Bombing и MFA Fatigue[4]. Push-уведомления с кнопкой «Подтвердить» уязвимы к систематической бомбардировке запросами на подтверждение, пока уставший от шквала запросов пользователь не нажмёт «ОК» или «Подтвердить».

Аутентификация на основе асимметричной криптографии не предусматривает никаких push-запросов и подтверждений для пользователя. При аутентификации устройство генерирует криптографический запрос и подписывает его закрытым ключом, который никогда не покидает защищённую область PKI-токена, поэтому злоумышленники не могут его перехватить или скопировать [12], [13].

7. ПОДТВЕРЖДЕНИЯ СО СТОРОНЫ MICROSOFT И GOOGLE

Microsoft Digital Defense Report 2025 делает вывод, основанный на данных о 600 миллионах ежедневных атак, о том, что «внедрение phishing-resistant MFA доказало свою способность предотвращать более 99% атак на идентификационные данные». При этом отчёт 2025 года подчёркивает, что традиционные методы MFA «больше недостаточны», и рекомендует переход на phishing-resistant методы – FIDO2 и certificate-based authentication (CBA) в качестве базового способа аутентификации [10],[4]. Важно понимать, что это не просто теоретическая рекомендация, а реальное уменьшение ландшафта атаки на учётные данные [4].

Google, после развёртывания FIDO2/PKI-ключей для 85 000+ сотрудников, зафиксировал нулевое количество успешных фишинговых атак против этих пользователей [14].

8. ВОПРОСЫ ВЫБОРА АППАРАТНЫХ УСТРОЙСТВ ДЛЯ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ В КОРПОРАТИВНОЙ СРЕДЕ

Исходя из проведённого анализа, мы видим, что использование технологий двухфакторной аутентификации на FIDO/PKI-ключах предоставляет очевидное преимущество для корпоративного потребителя. По сути, это единственный эффективный вариант с точки зрения информационной безопасности. Вместе с тем необходимо учесть особенности российского рынка, а они в нынешних условиях, очевидно, существуют.

8.1. Ключи FIDO2. Механизмы FIDO2 предполагают самостоятельную регистрацию токена на каждом информационном ресурсе, то есть от-

[2] AiTM (Adversary-in-the-Middle) – это современный вариант атаки «человек посередине» (MitM), при котором злоумышленник встраивается между пользователем и сервисом, например, веб-порталом, и участвует в аутентификации, включая MFA

[3] Credential stuffing (подстановка учётных данных) – это атака, при которой злоумышленник берёт уже украденные пары логин/пароль из утечек и массово автоматизированно пробует их на других сайтах и сервисах, рассчитывая на повторное использование паролей пользователями.

[4] Prompt bombing (MFA prompt bombing, push bombing, MFA fatigue attack) – это атака на многофакторную аутентификацию, при которой злоумышленник засыпает пользователя множеством push-запросов/уведомлений MFA, чтобы тот по ошибке или от усталости нажал «Разрешить» и дал злоумышленнику доступ к учётной записи.

сутствует возможность контролировать, к чему пользователь получает доступ. Также нет возможности централизованной блокировки доступа ко всем ресурсам, например при увольнении сотрудника или иных обстоятельствах, требующих прекращения доступа.

Этой проблемы нет при использовании PKI-токенов – достаточно просто отозвать сертификат, и пользователь потеряет доступ ко всем ресурсам, где этот сертификат использовался.

В результате применение FIDO2-ключей имеет ограниченные возможности для корпоративного сектора. Ключи FIDO2 могут использоваться для доступа к корпоративным веб-сервисам в организациях, не являющихся субъектами критической информационной инфраструктуры (КИИ) и не обрабатывающих сведений, требующих применения сертифицированных средств криптографической защиты информации (СКЗИ). Также они могут применяться для доступа ко внешним облачным SaaS-сервисам, например Google Workspace, Microsoft 365 и им подобным, а также ко внешним веб-порталам [16], [17].

8.2. PKI-токены. Для российского государственного и корпоративного сектора остаётся единственная возможность существенно повысить уровень безопасности аутентификации – применять USB-токены и смарт-карты, использующие PKI-технологии, что в ряде случаев напрямую предписывается регуляторами.

Обычные коммерческие организации, не являющиеся субъектами КИИ и не попадающие под приказ ФСТЭК № 117, не имеют прямого законодательного обязательства применять аппаратные PKI-ключи для аутентификации рядовых пользователей в службе каталога. Тем не менее это настоятельно рекомендуется, поскольку иные методы аутентификации не только приводят к операционным рискам, но и повышают вероятность претензий со стороны регуляторов при киберинцидентах [9].

Если говорить о выборе аппаратного решения, то по сложившейся практике для задач аутентификации в информационных системах достаточно наличия сертификата соответствия, выданного ФСТЭК.

9. ТРЕБОВАНИЯ ПРИКАЗА ФСТЭК №117 ОТ 11.04.2025

Стоит обратить внимание на то, что одним из важнейших нововведений приказа ФСТЭК № 117 является появление понятия «строгой аутентификации» [18]. Это многофакторная взаимная аутентификация с использованием криптографических протоколов [19]. Очевидно, что речь идёт о PKI-токене.

Важно понимать, на какие организации распространяется этот приказ, когда и в каких случаях внедрение строгой аутентификации обязательно.

9.1. Какие организации должны использовать PKI-ключи. Приказ распространяется на государственные органы – федеральные и региональные органы исполнительной власти (министерства, ведомства, службы, агентства), государственные учреждения – федеральные и региональные (казённые, бюджетные, автономные): вузы, больницы, научные организации, музеи и т.д., государственные унитарные предприятия (ГУП и ФГУП), муниципальные органы и учреждения – если иное не установлено законодательством (см. Общие Положения п. 1 [18]).

Кроме того, под действие приказа попадают не только государственные информационные системы (ГИС), но и любые информационные системы организаций, обрабатывающие информацию ограниченного доступа: системы электронного документооборота (ЭДО), кадровые, бухгалтерские, учётные и т.п. (См. Общие Положения п. 2 [18]).

Получается, что любая организация, получающая информацию ограниченного доступа из ГИС, также должна соответствовать требованиям приказа ФСТЭК № 117.

Требования использования строгой аутентификации также распространяются на объекты КИИ [20], [21].

Итоговая сводка о необходимости использования PKI-ключей приведена в таблице 2.

Тип организации	Нормативная база	Требование использования PKI-ключей
Федеральные и региональные органы исполнительной власти	Приказ ФСТЭК №117	Обязательно для всех
ГУП, ФГУП	Приказ ФСТЭК №117	Обязательно для всех
Муниципальные органы и учреждения	Приказ ФСТЭК №117	Обязательно для всех
КИИ 1 категории	Приказ ФСТЭК №117 и ФЗ-187	Обязательно для привилегированных пользователей
КИИ 2 категории	Приказ ФСТЭК №117 и ФЗ-187	Обязательно для привилегированных пользователей
Прочие коммерческие организации	Не регулируется	Рекомендовано (Best Practice) [9]

Таблица 2. Итоговая сводка о необходимости использования PKI-ключей

10. ВЫВОДЫ

В результате анализа опубликованной в доверенных открытых источниках информации о кибератаках и их последствиях становится вполне очевидным, что использование традиционных методов аутентификации с помощью запоминаемого пароля неэффективно для любой организации и несёт понятные угрозы безопасности.

Следует рассмотреть кардинальное изменение модели аутентификации, перейдя к строгой аутентификации, которая предусматривает наличие у пользователя уникального неклонируемого (защищённого) устройства с поддержкой криптографии, неизвлекаемым закрытым ключом и защитой от несанкционированного использования.

В организации должна быть развёрнута корпоративная инфраструктура открытых ключей (PKI).

Строгая аутентификация обеспечивает высокий уровень доверия к информационной системе и является самым надёжным и удобным для пользователя способом. Такой способ аутентификации не просто представляет собой техническое улучшение, а является стратегическим решением, устраняющим доминирующий вектор атак, и, кроме того, обязательным методом для пользователей большинства организаций в соответствии с требованиями ФСТЭК.

ИСТОЧНИКИ

1. Verizon. *2025 Data Breach Investigations Report*. 2025 (https://www.verizon.com/business/resources/T3ed/reports/2025-dbir-data-breach-investigations-report.pdf).
2. Verizon. *Additional 2025 DBIR Research on Credential Stuffing*. 2025 (https://www.verizon.com/business/resources/articles/credential-stuffing-attacks-2025-dbir-research/).
3. Microsoft. *Microsoft Digital Defense Report 2024*. 2024 (https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024).
4. Microsoft. *Microsoft Releases 2025 Digital Defense Report: Highlighting the Changing Cyber Threat Landscape and the Importance of Security in the AI Era*. 7 января 2026 г. (https://news.microsoft.com/source/asia/2026/01/07/microsoft-releases-2025-digital-defense-report-highlighting-the-changing-cyber-threat-landscape-and-the-importance-of-security-in-the-ai-era/).
5. Positive Technologies. *Актуальные киберугрозы для организаций в СНГ: второе полугодие 2024 года — третий квартал 2025 года* (https://ptsecurity.com/research/analytics/cis-cyberthreat-landscape-h2-2024-q3-2025/).
6. Positive Technologies. *Результаты расследований Positive Technologies: каждая вторая атака привела к нарушению бизнес-процессов*. 6 ноября 2024 г. (https://ptsecurity.com/ru-ru/about/news/rezultaty-rassledovanij-positive-technologies-kazhdaya-vtoraya-ataka-privela-k-narusheniyu-biznes-proczessov/).
7. CrowdStrike. *CrowdStrike 2025 Global Threat Report: Executive Summary*. 2025 (https://www.crowdstrike.com/en-us/resources/reports/global-threat-report-executive-summary-2025/).
8. IBM. *Cost of a Data Breach Report 2025*. 2025 (https://www.ibm.com/reports/data-breach).
9. Positive Technologies. *Итоги проектов по расследованию инцидентов и ретроспективному анализу — 2024–2025* (https://ptsecurity.com/research/analytics/results-of-incident-investigation-and-retrospective-analysis-projects-2024-2025/).
10. Microsoft. *Microsoft Digital Defense Report 2025*. 2025 (https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/reports/microsoft-digital-defense-report-2025/).
11. Cybersecurity and Infrastructure Security Agency. *Implementing Phishing-Resistant MFA* (https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf).
12. CrucialLogics. *Phishing-Resistant MFA: Methods, Risks and Rollout*. 30 сентября 2025 г. (https://cruciallogics.com/blog/phishing-resistant-mfa/).
13. SentinelOne. *What Is Phishing-Resistant MFA? Modern Security* (https://www.sentinelone.com/cybersecurity-101/identity-security/phishing-resistant-mfa/).
14. Krebs B. *Google: Security Keys Neutralized Employee Phishing*. 23 июля 2018 г. (https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/).
15. «Лаборатория Касперского». *Половина скомпрометированных в 2025 году паролей утекли не впервые*. 8 декабря 2025 г. (https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-polovina-skomprometirovannyh-v-2025-godu-parolej-utekli-ne-vpervye).
16. Microsoft. *What Is FIDO2?* (https://www.microsoft.com/en-us/security/business/security-101/what-is-fido2).
17. FIDO Alliance. *Why FIDO?* (https://fidoalliance.org/).
18. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений: приказ ФСТЭК России от 11 апреля 2025 г. № 117 (https://publication.pravo.gov.ru/document/0001202506170011).
19. ГОСТ Р 58833–2020. *Защита информации. Идентификация и аутентификация. Общие положения* (https://protect.gost.ru/gost/details/554a46bc-50ea-4232-ad71-e5bbe251c0f2).
20. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России от 25 декабря 2017 г. № 239, в ред. приказа ФСТЭК России от 28 августа 2024 г. № 159 (https://publication.pravo.gov.ru/Document/View/0001201803270041; https://publication.pravo.gov.ru/document/0001202410250022).
21. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ (https://publication.pravo.gov.ru/document/0001201707260023).
22. ГК «Солар». *Кого и как атаковали в 2025 году* // BIS Journal. 2026. № 2 (61). 7 апреля (https://ib-bank.ru/bisjournal/post/2673).
23. Груздев С. *Аутентификация и ЭП с использованием биометрии* // BIS Journal. 2026. № 1 (60). 10 февраля (https://ib-bank.ru/bisjournal/post/2623).
24. Груздев С. *Аутентификация. От паролей к адаптивной МФА* // BIS Journal. 2025. № 3 (58). 18 сентября (https://ib-bank.ru/bisjournal/post/2523).