Инженерный вестник Дона, №10 (2025)
ivdon.ru/ru/magazine/archive/n10y2025/10454

Проблемы парольной аутентификации: обзор потенциальных вариантов замены, их анализ и сравнение

А. Р. Панченко

Южный федеральный университет, Таганрог

Аннотация: В работе представлен обзор актуального состояния парольной аутентификации, отражены основные проблемы. В качестве замены парольной аутентификации рассматриваются разные варианты беспарольной аутентификации. Каждый из вариантов рассматривается с точки зрения недостатков и возможности замены паролей. В результате анализа явными фаворитами намечены два направления беспарольной аутентификации: биометрическая и ключи доступа (passkey). В рамках сравнения между двумя финалистами выбор пал на passkey, так как в нем отсутствует основной и критический недостаток биометрической аутентификации – зависимость от сокрытия оригиналов биометрии, в случае компрометации которой человек получает огромные проблемы, так как свою биометрию без хирургического вмешательства он не в силах изменить. Ключи доступа, напротив, показывают высокий уровень защиты, сравнимый с биометрией, но такого недостатка лишены. При этом passkey, а точнее текущий стандарт FIDO2 имеет ряд недостатков, которые мешают распространению. В рамках решения данной задачи необходимо разработать безопасный протокол беспарольной аутентификации с использованием технологии passkey.
Ключевые слова: парольная аутентификация, беспарольная аутентификация, push-уведомление, QR-код, биометрическая аутентификация, passkey, FIDO2, WebAuthn, CTAP2.1.

Введение

На данный момент сложно найти человека, который бы не пользовался паролями. Данный механизм защиты проник в нашу жизнь повсеместно, начиная от работы и заканчивая личной жизнью. Но на данный момент можно с уверенностью сказать, что пароли окончательно устарели. ««В июне 2024 года «Лаборатория Касперского» проанализировала 193 млн паролей, обнаруженных в публичном доступе на даркнет-ресурсах. Результаты исследования показали, что: почти половину из них (45%, или 87 млн.) мошенники смогут подобрать менее чем за минуту; большинство проанализированных паролей могут быть легко скомпрометированы с помощью умных алгоритмов; только 23% (44 млн.) комбинаций оказались достаточно стойкими: на их взлом ушло бы больше года» [1, с. 3]. Данная ситуация возникла из-за человеческого фактора. Люди в основной своей

массе не стремятся сделать сложный пароль или, если его им сделала организация, просто записывают его на клочке бумаги. Подтверждение данной точки зрения можно найти в статье [2, с. 79]: «Пароли, самостоятельно устанавливаемые пользователями, бывают качественными крайне редко. Сложность паролей, генерируемых различными информационными системами, на практике часто оказывается обесцененной самими работниками предприятия, записывающими и сохраняющими выданные им пароли». Так же данный тезис подтверждает и securitylab. «Так, по информации securitylab в 2008 году 84% случаев взломов систем безопасности компаний и персональных страниц причиной была именно слабая парольная защита» [3]. Отдельно стоит указать проблему, связанную с тем, что люди используют не набор символов в качестве пароля, а «информативные последовательности символов» [4], что тоже не является хорошим вариантом для пароля. Однако нужно заметить, что небольшая модификация такой последовательности символов может превратить её в крайне стойкий и надежный пароль. Способ такой модификации показан в статье [5, с. 159].

Другой важной и острой проблемой для парольной аутентификации является повтор одинаковых или минимально изменённых паролей. « We find that password reuse and modification is very common (observed on 52% of the users) » [6]. В данной ситуации проблема обостряется тем фактом, что число сервисов и учетных записей только растет, а в каждой из них нужно использовать уникальный пароль, иначе, в случае компрометации одного из ресурсов, под угрозу попадут и другие. «Также очень важно не использовать одинаковые пароли для разных учётных записей, ведь если один пароль будет скомпрометирован, это может повлечь за собой взлом и других учётных записей, где соответствующий пароль используется» [7].

В рамках способа улучшения парольной аутентификации можно использовать метод «комплексирования символов пароля и временных интервалов между ними». Данный метод показан и оценен в статье [8]. Он повышает сложность подбора пароля, но требует от пользователя последовательного выдерживания интервала между вводом очередного символа. В реальности люди вводят пароли или определенные символы из него с огромной скоростью. С учетом этого факта данный способ станет скорее проблемой для пользователя.

Если рассмотреть статистику используемых паролей, представленную в статье [9], то можно увидеть достаточно удручающую картину: более половины от всех паролей составляют цифирные пароли, в которых нет ни одной буквы. Такие пароли легко взламываются атакой по словарю или методом грубой силы за крайне малое время, а если учитывать наличие облачных вычислений, то время может быть вообще ничтожным.

Фишинг так же является одной из основных проблем парольной аутентификации. Фишинг — это вид интернет-мошенничества, при котором злоумышленник пытается получить доступ к конфиденциальным данным пользователей, в большинстве случаев логину и паролю. Статистика успешных фишинговых атак говорит о серьезных проблемах паролей. «Что касается глобальных тенденций, то в 2022 году APWG зафиксировала около 4,7 миллиона фишинговых атак. С 2019 года наблюдается ежегодное увеличение числа атак более чем на 150» [10]. Все перечисленные моменты говорят и подтверждают проблематику использования парольной аутентификации и необходимость использования альтернативных способов аутентификации.

В рамках данной статьи рассматривается беспарольная аутентификация как потенциальный способ замены устаревшей парольной. В беспарольной аутентификации используется смена парадигмы: переход от фактора знания –

пароля – к фактору владения чем-либо, например, аутентификатором или токеном, или какой-либо отличительной чертой, если речь идет о биометрической аутентификации индивида. Данное направление является крайне перспективным [11, 12, с. 144].

Беспарольная аутентификация содержит в себе несколько видов и подходов к аутентификации: одноразовые пароли или OTP, QR-код, Push-уведомления, биометрия, passkey. В данной статье все эти способы рассматриваются с точки зрения недостатков, которые могут помешать их потенциальной замене пароля.

OTP

OTP, или One-Time Password, или Одноразовый пароль – это уникальный пароль, действительный только для одного сеанса входа или транзакции в информационной системе или приложении. Данные пароли в отличие от постоянных (статических) паролей создаются динамически. Их необходимо использовать в течение определённого промежутка времени иначе пароль перестанет быть действующим и станет лишь бесполезным набором символов. Так же данные коды часто используются в системах многофакторной аутентификации в качестве дополнительного фактора.

Так как данный пароль создается динамически, то фактором надёжности становится механизм генерации данной псевдослучайной последовательности символов. В статье [13] рассматриваются разные варианты создания таких кодов. Выводы, сделанные авторами, говорят о том, что текущие алгоритмы достаточны, но стоит задуматься о модификации.

Другим не менее важным моментом является тот факт, что код необходимо передать пользователю, которой проходит процедуру аутентификации. Необходимо, чтобы код не был перехвачен во время передачи. В статьях [14,15] авторами рассматривается данная проблема и

предложен алгоритм, позволяющий обеспечить конфиденциальность одноразового кода во время передачи по каналам связи.

Одним из наиболее известных и распространенных решений для двухфакторной аутентификации на основе OTP можно считать GoogleAuthenticator. Анализ и сравнение данного продукта с другими представителями рынка показан в статье [16].

Подведем итог. Данный способ аутентификации может быть использован в качестве добавочного фактора в многофакторной аутентификации (MFA), но использовать его в качестве основного слишком опрометчиво.

QR-код

Quick Response Code или QR-код – это двумерный код, способный хранить информацию разного рода. Например текст, ссылки, контакты, платёжные данные. Внешний вид QR кода состоит из чёрно-белых модулей, расположенных в квадратном поле.

Можно провести параллель с традиционным штрих-кодом, но последний может хранить информацию только в одном измерении (горизонтально); QR-код, напротив, способен хранить данные в двух измерениях (горизонтально и вертикально). Данная особенность позволяет QR-кодам нести в себе значительно больше информации на единицу пространства.

Для взаимодействия с QR-кодами можно использовать камеру смартфона, данная возможность сильно повышает удобство использования, а соответственно помогает широкому распространению.

Удобство является одним из основных факторов распространения какой-либо технологии, но нужно не забывать про безопасность. В случае с QR-кодами стоит обратить внимание на тот факт, что человеку крайне сложно заметить мелкие модификации самого кода, что дает огромную

возможность злоумышленникам для всякого рода атак, например фишинга. В статье [17] показаны примеры таких модификаций, а также даны советы по защите себя от таких атак. Метод, который позволяет превратить текст в QR-код представлен в работе [18].

Стоит упомянуть, что считывание кода происходит по-разному для профессионального считывателя и телефона рядового пользователя. «Таким образом, можно сделать вывод, что профессиональные сканеры направлены на восстановление потерянной информации штрихового кода, а приложения мобильных телефонов предполагают считывание более нестандартных вариантов их оформления» [19].

Отдельно можно рассмотреть работы, посвященные защищенности QR-кодов. В своей работе Кизеберг и др. исследовали QR-код, с целью объяснения того, как его можно использовать для атаки на автоматизированную систему и взаимодействия с человеком [20]. В работе [21] авторы анализировали две программы считывания QR-кодов и попытались создать сканер для QR-кода. Они пришли к выводу что в текущем виде QR-коды ни в коем случае не безопасный формат. Дабровски и др. проанализировали состояние, названное "Атака штрих-кодом" [22]. Атака штрих-кодом – это использование вредоносных штрих-кодов для запуска нежелательных сценариев на компьютерах и загрузки вредоносного ПО. Один из примеров такой атаки – BadBarcode. Её обнаружили специалисты китайской компании Tencent's Xuanwu Lab в 2015 году. Основной принцип — внедрение специальных управляющих символов в штрих-код, чтобы считывающее устройство выполнило внутрисистемные «нажатия горячих клавиш» в хост-системе и вызывало конкретные функции. В работе [23] автор также рассматривал модификацию QR-кодов и обсуждал их безопасность.

Стоит так же упомянуть атаку «штрихкод в штрихкоде». В рамках данной атаки два разных штрихкода кодируются в одной и той же прямоугольной области, которая визуально воспринимается как один штрихкод. Однако эта атака основана не столько на вероятностных ошибках, сколько на различиях в реализации декодеров. Она похожа на декодирование протокола, при котором, например, брандмауэр или антивирусный сканер декодируют и интерпретируют данные иначе, чем сервер, на котором они находятся, что позволяет использовать уязвимость. Таким образом, любая двусмысленность представляет собой потенциальную угрозу безопасности [24-26].

Если сложить все написанное вместе, то становится ясно, что QR-коды не могут заменить пароли, так как человек не способен заметить тонкую модификацию кода. Присутствуют ошибки, связанные с разными считывателями, что тоже не прибавляет безопасности данному варианту беспарольной аутентификации.

Push-уведомления

Данный метод не является полноценной беспарольной аутентификаций и используется только в рамках MFA. Аутентификация через push-уведомления – это метод двухфакторной аутентификации, который отправляет уведомление на устройство пользователя через специальное приложение. Работает это следующим образом: пользователь вводит логин и пароль после чего получает мгновенное уведомление на смартфон или планшет с просьбой подтвердить или отклонить попытку входа одним касанием. Такой подход не требует вручную вводить коды и значительно ускоряет процесс авторизации. Немного о плюсах и минусах push-уведомлений.

Плюсы использования следующие:

Простота использования. Нужно только нажать «Подтвердить» в полученном уведомлении без необходимости копировать или вводить коды;

Повышенная безопасность. Push-уведомления сложнее перехватить по сравнению с СМС, они приходят по зашифрованным каналам;

Информативность. Уведомления могут содержать детали о попытке входа (локация, устройство), помогая выявить несанкционированный доступ.

Недостатки push-уведомлений:

Требуется интернет. Без доступа к интернету push-уведомления не будут доставлены;

Ограниченное распространение. Не все сервисы поддерживают аутентификацию через push-уведомления;

Зависимость от устройства. Как и с другими мобильными методами, потеря телефона может привести к проблемам с доступом;

Уязвимость для потенциального мошенничества. Пользователи могут машинально подтверждать уведомления, не вчитываясь в их содержание.

Биометрическая аутентификация

Аутентификация на основе биометрических черт или характеристик – это методы идентификации и аутентификации, основанные на уникальных биологических характеристиках человека. В данном методе вместо традиционных паролей или PIN-кодов система использует сканирование отпечатков пальцев, распознавание лица, сканирование радужной оболочки глаза или анализ голоса для подтверждения личности. Данный метод аутентификации можно назвать наиболее удобным методом аутентификации [27,28]. Все из-за того, что фактор аутентификации всегда находится с человеком и не может быть утрачен. Несмотря на все достоинства данного вида аутентификации, злоумышленники нашли способ обходить защиту [29], реализуемую некоторыми из таких систем [30]. Известны случаи, когда злоумышленник получил доступ при помощи изготовления муляжа

отпечатков пальцев или разблокирования телефона по лицу похожего человека. Потенциальный способ повысить безопасность биометрической аутентификации представлен в статье [31], он основан на «тепловой карте ладоней пользователя», что потенциально повышает защиту конкретного пользователя и предотвращает возможность фальсификации с помощью муляжей.

Другим направлением биометрической аутентификации может стать речь. Голосовая аутентификация – динамический метод биометрической аутентификации, использующий уникальные характеристики человеческого голоса в качестве признака, позволяющего распознать субъекта и подтвердить его личность [32]. Речь каждого человека уникальна. На основании такого фактора уже достаточно долго разрабатываются системы аутентификации. Пример такой системы показан в работе [33]. У данного метода аутентификации есть ряд потенциальных проблем, которые показаны в работе [34, с. 34, 35]. Важно заметить, что даже при наличии проблем данный способ аутентификации повышает защищенность пользователя в 1,5 раза [34, с. 36]. Потенциальные способы защиты от спуфинга, а именно так называются действия злоумышленника, направленные на успешную аутентификацию в системе под видом другого лица показаны в работе [36]. Все ранее описанные проблемы голосовой аутентификации, говорят, что данный способ не идеален, но он достаточно хорошо себя показывает, как и другие биометрические способы аутентификации.

Другим потенциальным способом аутентификации может стать рукописный ввод. Данный способ рассматривается в работе Баянова [37]. В ней автор рассматривает методы предварительной обработки данных, оценку качества биометрических признаков, а также метод передискретизации биометрических данных. Данный способ аутентификации тоже, как и все биометрические, дает высокую надежность.

Если собрать воедино все, что было ранее сказано про биометрическую аутентификацию, то можно сказать следующее: все они надежно защищены, их надёжность выше, чем у пароля, но есть один недостаток, который вытекает из их же плюсов. Так как фактор аутентификации не может быть утрачен (за исключением критических ситуаций с травмами), то при компрометации серверов или баз данных, где хранятся биометрические данные аутентификации, человек будет находиться в критической опасности, так как он не сможет, как в случае с паролем, просто взять и заменить свой голос или почерк.

Passkey

Passkey [38, с. 203] или ключи доступа – это беспарольная технология аутентификации пользователей, которая позволяет заменить пароли на внешний аутентификатор или токен. Вместо запоминания сложных комбинаций символов в качестве пароля для входа в учётные записи используются токены. Во время процедуры регистрации или аутентификации пользователь взаимодействует с аутентификатором посредством PIN-кода или биометрических данных (отпечаток пальца, скан лица). Важным отличием от других методов беспарольной аутентификации является тот факт, что с токена на сервер ресурса никогда не попадает ничего кроме логина, а все PIN-коды или биометрические данные остаются только на устройстве владельца, тем самым убирая проблемы пароля в виде фишинга и проблемы биометрии, связанные с компрометацией сервера.

На текущий момент действует стандарт FIDO2, который реализует данную технологию на практике. В данном стандарте участвуют два протокола: WebAuthn, CTAP2.1. Данные о текущей версии стандарта FIDO2 были получены из документации стандарта с официального сайта FIDO, а также из статьи [39]. Информация о протоколе WebAuthn была получена из официального сайта консорциума W3C, а также из статей [40-42]. Важно

заметить, что предыдущие анализы безопасности WebAuthn показывали его достаточно высокую криптостойкость в рамках стандарта FIDO2 [43, 44, с. 453]. Принцип работы протокола CTAP2.1 был получен из официальной документации FIDO, а также из статей [45,46]. На данный момент исследования говорят о высокой стойкости данного стандарта беспарольной аутентификации.

Если говорить о недостатках, то к ним можно отнести проблему, связанную с отвязкой старого и привязкой нового аутентификатора в случае потери первого. Так же стоит заметить проблему, связанную с архитектурой стандарта FIDO2, которая базируется на WebAuthn, в котором присутствует потенциальная уязвимость, связанная с использованием вредоносного ПО в качестве клиента. Так же стоит заметить тот факт, что далеко не все ресурсы вводят у себя возможность использования ключей доступа в качестве метода аутентификации. Все эти проблемы приводят к той мысли, что текущий стандарт является вполне защищенным, но не лишенным недостатков. Эти недостатки отталкивают людей переходить на данный вариант аутентификации. Для решения данной проблемы стоит заняться разработкой безопасного протокола беспарольной аутентификации с использованием технологии passkey, который будет доказательно устойчив.

Заключение

В рамках данной статьи были рассмотрены основные замечания и нарекания, относящиеся к парольной аутентификации. Исходя из всего описанного ранее можно смело утверждать, что пароли устарели и требуют замены. Промедление будет с каждым годом обходиться все дороже как для компаний, так и для конечных пользователей. Так же в рамках данной статьи были рассмотрены основные аналоги для замены парольной аутентификации. Из них некоторые могут быть лишь вторым фактором аутентификации, как, например, OTP-коды и Push-уведомления; какие-то вообще не стоит

использовать для замены пароля, как, например, QR-коды. Основными фаворитами на замену паролей выступают биометрическая аутентификация и passkey. Если рассматривать только эту пару, то предпочтение стоит отдать ключам доступа (passkey), так как они показывают высокий уровень надежности и, в отличие от биометрии, их можно заменить в случае чрезвычайных ситуаций, компрометации или кражи. Биометрия крайне чувствительна к сокрытию оригиналов, и любая компрометация сервера подставит под удар людей на годы вперед, так как свою биометрию они изменить не в силах.

Литература

1. Тенячкина М. О., Богданова М. В., Быкова К. И., Сакалова К. А. Современные направления применения комбинаторики в области защиты персональных данных // Международный научно-исследовательский журнал. 2024. № 9(147). URL: research-journal.org/media/articles/8886.pdf.

2. Рябов И.А., Койцан М.Г., Кузнецов А.А., Ермолаева В.В. Информационная безопасность: парольная защита // Тенденции развития науки и образования. 2023. № 93-8. С. 76-79. URL: doicode.ru/doifile/lj/93/trnio-01-2023-401.pdf.

3. Снегуров А.В., Чакрян В.Х. Анализ устойчивости ко взлому современных механизмов парольной защиты операционных систем // Восточно-Европейский журнал передовых технологий. 2011. № 10. С. 27–29.

4. Тюрин К.А., Сёмин Р.В. Анализ стойкости парольных фраз на основе информационной энтропии // Известия ЮФУ. Технические науки. 2015 № 5. С. 18–27.

5. Назаров, Д. М. Методика создания надежного пароля для обеспечения экономической безопасности в условиях цифровизации // Известия Санкт-Петербургского государственного экономического университета. 2022. № 1(133). С. 155-160.

6. Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang. The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services // CODASPY '18: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018. pp. 196-203. URL: dl.acm.org/doi/pdf/10.1145/3176258.3176332.

7. Кочанова А. Г. Надёжные пароли: как их создать и чем они полезны // Вестник науки. 2023. № 6 (63). С. 902-908.

8. Фатхи Д.В., Галушка В.В. Повышение сложности пароля пользователя на основе комплексирования символов пароля и временных интервалов между ними // Инженерный вестник Дона, 2019, № 1. URL: ivdon.ru/ru/magazine/archive/n1y2019/5594.

9. Абидарова А.А. Анализ надежности паролей для обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки. 2021. № 8. С. 66–68.

10. Селиверстов В.В., Корчагин С.А. Анализ актуальности и состояния современных фишинг-атак на объекты критической информационной инфраструктуры // Инженерный вестник Дона. 2024. № 6. С. URL: ivdon.ru/ru/magazine/archive/n6y2024/9277.

11. S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes and S. Bugiel, "Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication" // 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 268-285. URL: ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152694

12. Докучаев В.А., Мытенков С.С., Рахмани Д.Д., Сафонов И.А. Анализ уязвимостей и рисков традиционных парольных систем в контексте корпоративных распределенных систем и критически важных инфраструктур // Экономика и качество систем связи. 2025. №36. С. 135-148.

13. Арзиева, Ж. Т., Арзиев А. Т. Анализ методов генерации одноразовых паролей и высокая степень случайности генерируемых паролей // Бюллетень науки и практики. 2022. Т. 8, № 7. С. 382-388. URL: bulletennauki.ru/gallery/Арзиева%20Ж.%20Т.,%20Арзиев%20А.%20Т.%20.pdf.

14. Yevseiev S., Kots H., Minukhin S. [et al.]The development of the method of multifactor authentication based on hybrid cryptocode constructions on defective codes // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 5, № 9(89). pp. 19-35.

15. Yevseiev S., Kots H., Liekariev Ye. Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system // Eastern-European Journal of Enterprise Technologies. 2016. – Vol. 6, № 4(84). pp. 11-23.

16. Мукымов Б., Бадырова Д., Гызылов Ч., Бекмаммедов С. Двухфакторная аутентификация и их использование при защите персональных данных // Символ науки: международный научный журнал. 2024. Т. 1, № 5-2. С. 48-49.

17. Godwin Awuah Amoah, Hayfron-Acquah J.B. QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing) // International Journal of Computer Applications. 2022. Vol. 184, № 33. pp. 34-39. URL: ijcaonline.org/archives/volume184/number33/amoah-2022-ijca-922425.pdf.

18. Riansah, W. Aplikasi QR Code Generator Dan QR Code Reader Menggunakan Metode Stroke Histogram // Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD. 2021. Vol. 4, № 1. pp. 38.

19. Ткачева, М. В. Оценка допустимых преобразований Qr Code // Известия Тульского государственного университета. Технические науки. 2013. № 3. С. 151-156.

20. Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. // QR code security. In

Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia (MoMM '10). Association for Computing Machinery, New York, NY, USA. 2010. pp. 430–435.

21. Peng, K., Sanabria, H., Wu, D., Zhu, C. Security Overview of QR Codes. // Student project in the MIT course 6.857,'14. 2014. URL: courses.csail.mit.edu/6.857/2014/files/12-peng-sanabria-wu-zhu-qr-codes.pdf

22. Dabrowski, Adrian, Katharina Krombholz, Johanna Ullrich and Edgar R. Weippl. "QR Inception: Barcode-in-Barcode Attacks." // Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices. 2014. URL: ics.uci.edu/~dabrowsa/dabrowski-ccsspsm2014-qrinception.pdf.

23. Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Weippl, E. QR Code Security: A Survey of Attacks and Challenges for Usable Security. In: Tryfonas, T., Askoxylakis, I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533. Springer, Cham. pp 79-90.

24. Alvarez S, Zoller T. The Death of AV Defense in Depth? -revisiting anti-virus software. // CanSecWest, Vancouver, B.C., Canada. 2008.

25. Jana S., Shmatikov V. Abusing File Processing in Malware Detectors for Fun and Profit. In Proceedings of the 33rd IEEE Symposium on Security & Privacy, San Francisco, CA, May 2012. pp. 80-94.

26. Sassaman L., Patterson M. L., Bratus S., Locasto M. E. "Security Applications of Formal Language Theory," // IEEE Systems Journal. Sept 2013. vol. 7, № 3. pp. 489-500.

27. Nadort A. The Hand Vein Pattern Used as a Biometric Feature: Literature thesis for Master of Science programmed Physics of Life. — Amsterdam: Medical Natural Sciences at the Free University, 2007. – 179 p.

28. Fuksis R., Pudzs M., Greitans M. Palm Vein Biometrics Based on Palm Infrared Imaging and Complex Matched Filtering: The 12th ACM Workshop on Multimedia and Security, Rome, 2009. – 27 p

29. Копиев Г. Восковая модель ладони обманула систему аутентификации по рисунку вен. URL: nplus1.ru/news/2018/12/28/vein (дата обращения: 05.08.2025).

30. Баранов С.О., Абрамов Д.Б. Технология биометрической аутентификации пользователя по венозному рисунку кистей рук // Научный рецензируемый журнал "Вестник СибАДИ". 2017; (2(54)):134-139.

31. Петров, Д. А. Исследование системы контроля управления доступом на основе тепловой карты ладоней пользователя // Инженерный вестник Дона. 2021. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6795.

32. Ravika, N. An Overview of Automatic Speaker Verification System // Intelligent Computing and Information and Communication: Proceedings of 2nd International Conference, ICICC 2017, 2–4 August 2017. Pune, India, 2017. pp. 603–610.

33. Лушников, Н. Д. Система распознавания пользователей по извлекаемым признакам голоса с применением фильтра Калмана // Инженерный вестник Дона. 2024. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9016.

34. Герасимов В. М., Маслова М. А. Возможные угрозы и атаки на систему голосовой идентификации пользователя // Научный результат. Информационные технологии. 2022. №1. URL: dspace.bsuedu.ru/bitstream/123456789/46222/1/Gerasimov_Vozmozhnye_22.pdf

35. Hao B., Hei Xiali. Voice Liveness Detection for Medical Devices // Design and Implementation of Healthcare Biometric Systems. 2019. pp. 109–136.

36. Евсюков М. В., Путято М. М., Макарян А. С., Немчинова В. О. Методы защиты в современных системах голосовой аутентификации //

Прикаспийский журнал: управление и высокие технологии. 2022. № 3(59). С. 84-92.

37. Баянов, Б. И. Методы обработки биометрических данных рукописного почерка // Инженерный вестник Дона. 2022. № 12. URL: ivdon.ru/ru/magazine/archive/n12y2022/8100.

38. Dr.A.Shaji George. The Dawn of Passkeys: Evaluating a Passwordless Future. Partners Universal Innovative Research Publication (PUIRP). 2024. № 02(01). pp. 202–220. URL: zenodo.org/records/10697886.

39. Mitra, A., Ghosh, A. FIDO2: A comprehensive study on passwordless authentication. // International Journal of Engineering Research and Applications. 2024. № 14(7). pp. 58–63. URL: ijera.com/papers/vol14no7/14075863.pdf.

40. Dourado, M. R., Gestal, M., Vázquez-Naya, J. M. (2020). Implementing a web application for W3C WebAuthn protocol testing. MDPI, 5. pp. 12-14.

41. Bindel, N., Gama, N., Guasch, S., Ronen, E. To Attest or Not to Attest, This is the Question – Provable Attestation in FIDO2. In: Guo, J., Steinfeld, R. (eds) Advances in Cryptology – ASIACRYPT 2023. ASIACRYPT 2023. Lecture Notes in Computer Science. 2023. Vol 14443. Springer, Singapore. pp. 297-328.

42. Hanzlik L., Loss J., Wagner B. Token meets Wallet: Formalizing Privacy and Revocation for FIDO2. // 2022 IEEE Symposium on Security and Privacy (SP), pp. 1491–1508. URL: eprint.iacr.org/2022/084.pdf.

43. Barbosa M., Boldyreva A., Chen S., Warinschi B. Provable Security Analysis of FIDO2. In: Malkin, T., Peikert, C. (eds) Advances in Cryptology – CRYPTO 2021. CRYPTO 2021. Lecture Notes in Computer Science, vol 12827. Springer, Cham. URL: iacr.org/archive/crypto2021/12826142/12826142.pdf.

44. Gudipati, R. R. (2025). Demystifying FIDO: A Technical Deep Dive into Modern Authentication. International journal of information technology and management information systems. 2025. № 16(2). pp. 452–466.

45. Bindel N., Cremers C., Zhao M. FIDO2, CTAP 2.1, and WebAuthN 2: Provable Security and Post-Quantum Instantiation. // 2022 IEEE Symposium on Security and Privacy (SP). URL: eprint.iacr.org/2022/1029.

46. Guan, J., Li, H., Ye, H., Zhao, Z. A Formal Analysis of the FIDO2 Protocols. In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds) Computer Security – ESORICS 2022. ESORICS 2022. Lecture Notes in Computer Science, vol 13556. Springer, Cham. URL: cactilab.github.io/assets/pdf/jingjing2022fido2.pdf.

References

1. Tenyachkina M. O., Bogdanova M. V., Bykova K. I., Sakalova K. A. Meždunarodnyj naučno-issledovatel'skij žurnal (International Research Journal). 2024. № 9(147). URL: research-journal.org/media/articles/8886.pdf.

2. Ryabov I.A., Koytsan M.G., Kuznetsov A.A., Ermolaeva V.V. Tendentsii razvitiya nauki i obrazovaniya. 2023. № 93-8. pp. 76-79. URL: doicode.ru/doifile/lj/93/trnio-01-2023-401.pdf.

3. Snegurov A.V., Chakryan V.Kh. Vostochno-Evropeyskiy zhurnal peredovykh tekhnologiy. 2011. № 10. pp. 27–29.

4. Tyurin K.A., Semin R.V. Izvestiya YuFU. Tekhnicheskie nauki. 2015 № 5. pp. 18–27.

5. Nazarov, D. M. Izvestiya Sankt-Peterburgskogo gosudarstvennogo ekonomicheskogo universiteta. 2022. № 1(133). pp. 155-160.

6. Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, Gang Wang. CODASPY '18: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018. pp. 196-203. URL: dl.acm.org/doi/pdf/10.1145/3176258.3176332.

7. Kochanova A. G. Vestnik nauki. 2023. № 6 (63). p. 902-908.

8. Fatkhi D.V., Galushka V.V. Inzhenernyj vestnik Dona, 2019, № 1. URL: ivdon.ru/ magazine/archive/n1y2019/5594.

9. Abidarova A.A. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2021. № 8. pp. 66–68.

10. Seliverstov V.V., Korchagin S.A. Inzhenernyj vestnik Dona. 2024. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9277.

11. S. Ghorbani Lyastani, M. Schilling, M. Neumayr, M. Backes and S. Bugiel, IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2020, pp. 268-285. URL: ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152694

12. Dokuchaev V.A., Mytenkov S.S., Rakhmani D.D., Safonov I.A. Ekonomika i kachestvo sistem svyazi. 2025. №36. pp. 135-148.

13. Arzieva, Zh. T., Arziev A. T. Byulleten' nauki i praktiki. 2022. T. 8, № 7. p. 382-388. URL: bulletennauki.ru/gallery/Arzieva%20Zh.%20T.,%20Arziev%20A.%20T.%20.pdf.

14. Yevseiev S., Kots H., Minukhin S. [et al.] Eastern-European Journal of Enterprise Technologies. 2017. Vol. 5, № 9(89). pp. 19-35.

15. Yevseiev S., Kots H., Liekariev Ye. Eastern-European Journal of Enterprise Technologies. 2016. Vol. 6, № 4(84). pp. 11-23.

16. Mukymov B., Badyrova D., Gyzylov Ch., Bekmammedov S. Simvol nauki: mezhdunarodnyy nauchnyy zhurnal. 2024. T. 1, № 5-2. pp. 48-49.

17. Godwin Awuah Amoah, Hayfron-Acquah J.B. International Journal of Computer Applications. 2022. Vol. 184, № 33. pp. 34-39. URL: ijcaonline.org/archives/volume184/number33/amoah-2022-ijca-922425.pdf.

18. Riansah, W. Aplikasi Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD. 2021. Vol. 4, № 1. p. 38.

19. Tkacheva, M. V. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2013. № 3. pp. 151-156.

20. Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, and Edgar Weippl. In Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia

(MoMM '10). Association for Computing Machinery, New York, NY, USA. 2010. pp. 430–435.

21. Peng, K., Sanabria, H., Wu, D., Zhu, C. Student project in the MIT course 6.857,'14. 2014. URL: courses.csail.mit.edu/6.857/2014/files/12-peng-sanabria-wu-zhu-qr-codes.pdf

22. Dabrowski, Adrian, Katharina Krombholz, Johanna Ullrich and Edgar R. Weippl. Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices. 2014. URL: ics.uci.edu/~dabrowsa/dabrowski-ccsspsm2014-qrinception.pdf.

23. Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., Weippl, E. In: Tryfonas, T., Askoxylakis, I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2014. Lecture Notes in Computer Science, vol 8533. Springer, Cham. pp. 79-90.

24. Alvarez S, Zoller T. CanSecWest, Vancouver, B.C., Canada. 2008.

25. Jana S., Shmatikov V. In Proceedings of the 33rd IEEE Symposium on Security & Privacy, San Francisco, CA, May 2012. pp. 80-94.

26. Sassaman L., Patterson M. L., Bratus S., Locasto M. E. IEEE Systems Journal. Sept 2013. vol. 7, № 3. pp. 489-500.

27. Nadort A. Literature thesis for Master of Science programmed Physics of Life. Amsterdam: Medical Natural Sciences at the Free University, 2007. 179 p.

28. Fuksis R., Pudzs M., Greitans M. The 12th ACM Workshop on Multimedia and Security, Rome, 2009. 27 p.

29. Kopiev G. Voskovaya model' ladoni obmanula sistemu autentifikatsii po risunku ven [A wax model of a palm fooled the authentication system based on the pattern of the veins]. URL: nplus1.ru/news/2018/12/28/vein (accessed: 05.08.2025).

30. Baranov S.O., Abramov D.B. Nauchnyy retsenziruemyy zhurnal "Vestnik SibADI". 2017; (2(54)). pp. 134-139.

31. Petrov, D. A. Inzhenernyj vestnik Dona. 2021. № 1. URL: ivdon.ru/ru/magazine/archive/n1y2021/6795.

32. Ravika, N. Intelligent Computing and Information and Communication: Proceedings of 2nd International Conference, ICICC 2017, 2–4 August 2017. Pune, India, 2017. p. 603–610.

33. Lushnikov, N. D. Inzhenernyj vestnik Dona. 2024. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2024/9016.

34. Gerasimov V. M., Maslova M. A. Nauchnyy rezul'tat. Informatsionnye tekhnologii. 2022. №1. URL: dspace.bsuedu.ru/bitstream/123456789/46222/1/Gerasimov_Vozmozhnye_22.pdf

35. Hao B., Hei Xiali. Design and Implementation of Healthcare Biometric Systems. 2019. p. 109–136.

36. Evsyukov M. V., Putyato M. M., Makaryan A. S., Nemchinova V. O. Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii. 2022. № 3(59). pp. 84-92.

37. Bayanov, B. I. Inzhenernyj vestnik Dona. 2022. № 12. URL: ivdon.ru/ru/magazine/archive/n12y2022/8100.

38. Dr.A.Shaji George. Partners Universal Innovative Research Publication (PUIRP). 2024. № 02(01). pp. 202–220. URL: zenodo.org/records/10697886.

39. Mitra, A., Ghosh, A. International Journal of Engineering Research and Applications. 2024. № 14(7). pp. 58–63. URL: ijera.com/papers/vol14no7/14075863.pdf.

40. Dourado, M. R., Gestal, M., Vázquez-Naya, J. M. (2020). MDPI, 5. pp. 12-14.

41. Bindel, N., Gama, N., Guasch, S., Ronen, E. In: Guo, J., Steinfeld, R. (eds) Advances in Cryptology – ASIACRYPT 2023. ASIACRYPT 2023. Lecture Notes in Computer Science. 2023. vol 14443. Springer, Singapore. pp. 297-328.

42. Hanzlik L., Loss J., Wagner B. 2022 IEEE Symposium on Security and Privacy (SP), pp. 1491–1508. URL: eprint.iacr.org/2022/084.pdf.

43. Barbosa M., Boldyreva A., Chen S., Warinschi B. In: Malkin, T., Peikert, C. (eds) Advances in Cryptology – CRYPTO 2021. CRYPTO 2021. Lecture Notes in Computer Science, vol 12827. Springer, Cham. URL: iacr.org/archive/crypto2021/12826142/12826142.pdf.

44. Gudipati, R. R. (2025). International journal of information technology and management information systems. 2025. № 16(2). pp. 452–466.

45. Bindel N., Cremers C., Zhao M. 2022 IEEE Symposium on Security and Privacy (SP). URL: eprint.iacr.org/2022/1029.

46. Guan, J., Li, H., Ye, H., Zhao, Z. In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds) Computer Security – ESORICS 2022. ESORICS 2022. Lecture Notes in Computer Science, vol 13556. Springer, Cham. URL: cactilab.github.io/assets/pdf/jingjing2022fido2.pdf.

Дата поступления: 5.08.2025

Дата публикации: 25.09.2025