ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ
INFORMATION SYSTEM AND TECHNOLOGIES

УДК 004.056.5 **DOI: 10.18413/2518-1092-2026-11-1-0-1**

Абселямов А.-Х.А.
Маслова М.А.
Лагуткина Т.В.

ВЛИЯНИЕ ПОЛЬЗОВАТЕЛЬСКОГО ОПЫТА НА ВЫБОР МЕТОДОВ АУТЕНТИФИКАЦИИ

Севастопольский государственный университет,
ул. Университетская, 33, г. Севастополь, 299053, Россия

e-mail: batrebless@gmail.com, mashechka-81@mail.ru, t.v.lagutkina@mail.sevsu.ru

Аннотация
В статье рассматривается значение пользовательского опыта (UX) в процессах аутентификации, подчеркивая его влияние на эффективность и комфорт взаимодействия с системами. Обзор современных методов аутентификации демонстрирует, что, несмотря на популярность паролей, существующие альтернативы способны предложить более высокий уровень безопасности. Важными критериями выбора методов аутентификации выделены безопасность, удобство использования и доступность. В информационной среде кибератаки наносят серьезный вред, ставя под угрозу сохранность важных данных, а иной и полную работу организации. Злоумышленники используют различные методы для взлома систем, кражи личной и финансовой информации, что приводит к значительным финансовым потерям и нарушению доверия клиентов. Аналитика в данной области является важным элементом работы компаний. В статье проводится анализ по распространенным ошибкам организаций при выборе методов аутентификации и влияния кибератак на эти решения. Так как многофакторная аутентификация дает контроль над доступом к важным системам компаний и дает возможность снизить риски утечек. Кроме того, ее внедрение и использование экономит время сотрудников, что является эффективным инструментом для защиты бизнеса в современном цифровом мире.

Ключевые слова: пользовательский опыт, аутентификация, безопасность, многофакторная аутентификация, биометрическая аутентификация, информационная безопасность
Для цитирования: Абселямов А.-Х.А., Маслова М.А., Лагуткина Т.В. Влияние пользовательского опыта на выбор методов аутентификации // Научный результат. Информационные технологии. – Т.11, №1, 2026. – С. 3-11. DOI: 10.18413/2518-1092-2026-11-1-0-1

Abselyamov A.-H.A.
Maslova M.A.
Lagutkina T.V.

THE USER EXPERIENCE INFLUENCE ON THE AUTHENTICATION METHODS CHOICE

Sevastopol State University,
33 Universitetskaya St., Sevastopol, 299053, Russia

e-mail: batrebless@gmail.com, mashechka-81@mail.ru, t.v.lagutkina@mail.sevsu.ru

Abstract
The article examines the importance of user experience (UX) in authentication processes, highlighting its impact on the efficiency and comfort of interacting with systems. A review of modern authentication methods shows that, despite the popularity of passwords, existing alternatives can offer a higher level of security. Key criteria for choosing authentication methods are identified as security, ease of use, and accessibility. In the information environment, cyberattacks cause serious harm, threatening the safety of important data and even the full operation

of an organization. Malicious actors use various methods to hack systems and steal personal and financial information, leading to significant financial losses and erosion of customer trust. Analytics in this area is an important aspect of company operations. The article analyzes common mistakes organizations make when choosing authentication methods and the impact of cyberattacks on these decisions. Since multi-factor authentication provides control over access to important company systems and allows reducing the risk of data leaks. In addition, its implementation and use save employees' time, making it an effective tool for business protection in the modern digital world.
Keywords: user experience; authentication; security; multi-factor authentication; biometric authentication; information security
For citation: Abselyamov A.-H.A., Maslova M.A., Lagutkina T.V. The User Experience Influence on the Authentication Methods Choice // Research result. Information technologies. – T.11, № 1, 2026. – P. 3-11. DOI: 10.18413/2518-1092-2026-11-1-0-1

ВВЕДЕНИЕ

User Experience (далее UX) или пользовательский опыт – показатель общего удобства и эффективности взаимодействий между пользователем и системой или программой. В случае процесса аутентификации, пользовательский опыт напрямую влияет на эффективность взаимодействия системы с пользователем, а также на общий комфорт пользователя при работе.

Основным фактором, влияющим на показатель пользовательского опыта в контексте аутентификации, является оценка уровня усилий и затраченного времени для совершений действий в системе. Также на общий показатель пользовательского опыта влияет соотношение усилий и безопасности – как пользователь воспринимает безопасность, предоставляемую процессом аутентификации.

Одним из критических факторов в этом контексте становится возможность комбинирования простых методов аутентификации с многофакторной аутентификацией (MFA) и интеграции продвинутых технологий, таких как применение биометрии в процессе аутентификации. Интеграция различных техник и методик позволяет не только повысить безопасность, но и улучшить пользовательский опыт за счет уменьшения усилий, прилагаемых пользователем для проверки. Множество пользователей предпочитают менее трудоемкие методы, которые в то же время обеспечивают необходимую защиту [1, 2].

ОСНОВНАЯ ЧАСТЬ

Наиболее распространенный метод аутентификации – применение паролей. Преимуществом использования паролей является их простота и повсеместность. Большинство пользователей уже давно знакомы с тем, как работают пароли. Однако распространенность этого метода не делает его идеальным выбором в проектировке будущих систем и технологий аутентификации. Существует множество причин, почему пароли вызывают негативный опыт среди пользователей. Исследования показывают, что одна из причин привязана к распространенности сервисов, использующих пароли. Большинство пользователей используют не более трех разных паролей в различных сервисах, что делает их подверженными риску, если один из аккаунтов будет скомпрометирован [3].

Среди альтернатив, распространенных среди технологий аутентификации одной из самых популярных, стала биометрическая аутентификация. Достоинством систем, использующих биометрию, становится высокий уровень предоставляемой безопасности, однако главным недостатком является высокий уровень внедрения систем, а также возможность недоверия со стороны пользователей. Некоторые потенциальные клиенты могут не чувствовать себя комфортно, предоставляя свои биометрические данные [4]. Помехой для внедрения также может быть неполная точность таких систем, что может вести к сбоям в аутентификации [5].

Двухфакторная аутентификация (2FA) является распространенной практикой, которая набирает популярность из-за повышения уровня безопасности. В любой из её форм, будь то SMS-коды или генерируемые приложения, она требует от пользователя дополнительных шагов для подтверждения личности. Это может быть как плюсом, так и минусом. С одной стороны, уметь

подтвердить вход одноразовым кодом является надежным способом преодоления угроз. С другой стороны, осталось много критичных замечаний о фальсификации SMS и ненадежности кодов в некоторых случаях, что может вызывать разочарование у пользователей. Но также ее могут обойти злоумышленники, если они заполучили логин и пароль, им необходимо только выманивать у пользователя одноразовый код.

Этот способ является одним из частых обманов пользователей. Злоумышленники звонят под видом МВД, служб банка, государственных служащих, пользуются неожиданностью звонка, придумывая разные виды приемов просят пользователя сообщить им пароль. При получении пароля они получают полный доступ к аккаунту пользователя и дальше выполняют различные махинации, связанные с финансовыми сервисами, банковскими приложениями, платежными системами и т.д. Через определенные сервисы они могут оформит кредит на владельца, завладеть его личными данными для дальнейшего мошенничества, регистрироваться на каких-либо сервисах, менять пароль от аккаунта, изменить настойки безопасности, привязать дугой телефон, подавать заявления, распоряжаться недвижимостью, выполнять другие незаконные действия. Такой взлом приравнивают к фактической краже цифровой идентичности. По фактам пресс-центра МВД РФ за 2024 год Россияне потеряли более 168 миллиардов рублей, что на 14,3 % больше предыдущего года. Чаще всего это женщины – 52,6 %, чем мужчины – 47,4 %, возраст пострадавших более попадает на людей, более часто пользующихся финансовыми операциями – это возраст от 25 до 64 лет и растет рост обманутых свыше 65 лет (рис.1) [6].

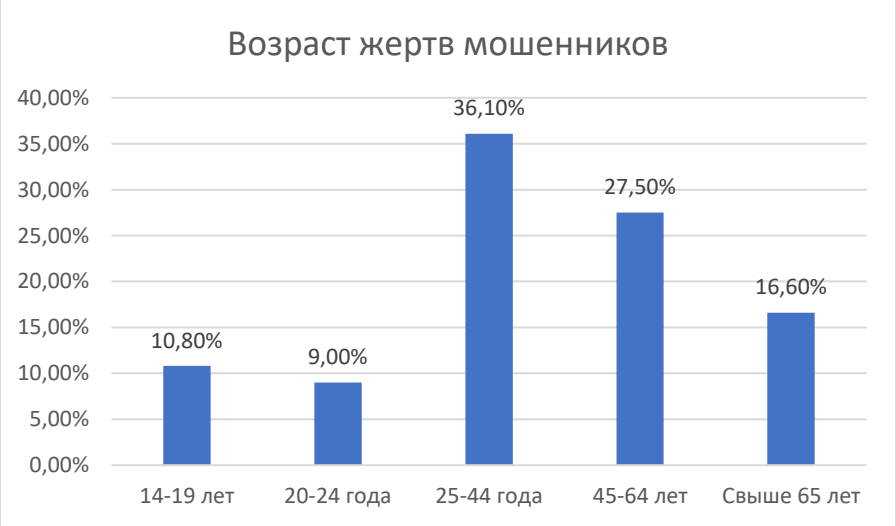

Рис. 1. Количество жертв (%) пострадавших от звонков мошенников в России
Fig. 1. Number of victims (%) affected by scam calls in Russia

Технология TOTP (временные одноразовые пароли) также используется для аутентификации с высоким уровнем безопасности. Главное её преимущество – это то, что пароли генерируются на стороне клиента и действуют только в течение короткого времени, что значительно усложняет взлом. Но для их применения необходимости постоянного доступа к Интернету может снизить комфорт пользователей [7]. На сегодняшний день очень часто «глушат» интернет, сотовую связь и из-за этого возникает такое неудобство и недовольство пользователей. Так как пароль приходит в течении минуты, а из-за плохой связи он не успевает прийти, и пользователь не может зайти на свой аккаунт так быстро, как ему бы хотелось.

При выборе методов аутентификации важными критериями считаются безопасность, удобство использования и доступность. Эти принципы играют решающую роль в формировании положительного пользовательского опыта, что в свою очередь определяет, насколько успешно и безопасно функционирует система.

Безопасность – это первостепенный критерий, требующий тщательной оценки. Уровень защиты данных зависит от использованных методов аутентификации и их уязвимостей.

Кроме того, удобство использования является ключевым аспектом. Метод аутентификации должен соответствовать потребностям пользователей. Если система окажется слишком сложной, это может вызвать негативные последствия, включая низкий уровень принятия и частые ошибки при вводе данных. Использование биометрической проверки способно повысить удовлетворенность пользователей и сократить количество ошибок [8].

Доступность включает в себя не только финансовые затраты на реализацию и поддержку конкретного метода, но и его применимость в различных условиях. Разные организации могут иметь определённые ресурсы, стандарты и требования, которые необходимо учитывать при выборе метода аутентификации. Например, решения с более высокой степенью безопасности могут быть более дорогостоящими, но их использование является обоснованным в контексте высокой ценности защищаемой информации [1].

Таблица 1

Классификация методов аутентификации

Table 1

Classification of authentication methods

Метод аутентификации	Типичные атаки на метод	Уровень стойкости метода	Уровень безопасности	Удобство использования	Затраты на обслуживание
Парольная аутентификация	Подбор пароля	Средний	Низкий	Высокое	Низкие
Двухфакторная аутентификация	Фишинг, перехват	Высокий	Высокий	Среднее	Средние
Биометрическая аутентификация	Моделирование отпечатков	Высокий	Высокий	Высокое	Высокие
Аутентификация посредством SMS	Замена-SIM, перехват	Средний	Средний	Среднее	Средние
Аутентификация посредством e-mail	Подбор пароля, перехват	Средний	Средний	Среднее	Средние
Аутентификация посредством социальных сетей	Фишинг, взлом аккаунта	Низкий	Низкий	Высокое	Низкие
Ключи безопасности	Перехват, утеря	Высокий	Высокий	Среднее	Средние
Одномоментная аутентификация	Подбор ключа	Высокий	Высокий	Высокое	Низкие
Токенная аутентификация	Подделка токена	Высокий	Высокий	Среднее	Средние
OAuth аутентификация	Подделка токена	Высокий	Высокий	Среднее	Средние
OpenID Connect	Подделка токена	Высокий	Высокий	Среднее	Средние
Карта доступа (Access Token)	Подделка токена	Высокий	Высокий	Среднее	Средние
Kerberos	Атаки MITM, перехват	Высокий	Высокий	Среднее	Высокие

На основе этих критериев организации должны проводить полноценный анализ перед выбором методов аутентификации. Рекомендуется рассматривать потенциальные риски и последствия, которые могут возникнуть при недостаточном внимании к указанным аспектам. При этом необходимо учитывать различия в отраслях, требования регуляторов и специфические особенности целевой аудитории [9].

Таблица 2

Использование методов аутентификации физическими лицами и организациями

Table 2

Use of authentication methods by individuals and organizations

Физ. лицо		**Организация**	
Логин и пароль (пользователь)	Пользователь передаёт логин и пароль. Сервер хранит только хэш. При совпадении хэшей выдаётся сессионный токен. Корпоративный вариант – Kerberos через Active Directory.	Корпоративный сценарий (сотрудник)	Active Directory
Двухфакторная аутентификация – TOTP (RFC 6238)	Одноразовый пароль на основе времени. Обе стороны независимо вычисляют: TOTP = Truncate (HMAC-SHA1 (secret, floor (unixTime/30))). Шаг времени - 30 секунд. Допускается отклонение ±1 окно на случай рассинхрона часов: 1) Первоначальная настройка (Provisioning), 2) Вход с TOTP по алгоритму RFC 6238	SSO - SAML 2.0 (SP-initiated Web SSO)	Сотрудник открывает приложение (SP). SP перенаправляет браузер к IdP с AuthnRequest. IdP аутентифицирует и POST'ит подписанный SAMLAssertion обратно в SP. IdP и SP не общаются напрямую - только через браузер
OAuth 2.0 Authorization Code Flow + PKCE	Физ. лицо входит через стороннего провайдера. Приложение никогда не видит пароль пользователя. PKCE защищает от перехвата кода. ID Token из OIDC несёт данные профиля пользователя	PKI - Сертификаты X.509 и Mutual TLS (mTLS)	Организации используют взаимную TLS-аутентификацию для B2B интеграций и госсистем. Каждая сторона предъявляет сертификат, подписанный Удостоверяющим Центром (CA). Приватный ключ никогда не передаётся. Получение сертификата X.509 через CSR mTLS Handshake – взаимная аутентификация организаций по RFC 8446

Частые ошибки при выборе метода аутентификации связаны с недостаточным анализом, недооценкой многофакторной аутентификации и игнорированием требований регуляторов. Это может привести к неэффективному управлению рисками и несанкционированному доступу к данным.

По данным специалистов, игнорирование многофакторной аутентификации является распространенной ошибкой среди организаций, полагающихся на аутентификацию. В частности, многие организации продолжают применять парольную аутентификацию, не осознавая, что такая стратегия оставляет значительные уязвимости, ведь 80% успешных атак можно предотвратить при наличии MFA [10].

Помимо этого, неправильный выбор технологий аутентификации также приводит к проблемам. Использование сложных систем, таких как биометрические или применение жетонов аутентификации, не всегда оправдано для сервисов с низким уровнем риска. Применение решений такого типа увеличивает затраты на внедрение, что ведёт к снижению качества предоставления услуг. Плохо спроектированные системы способны вызывать у пользователей раздражение, что в итоге негативно сказывается на их лояльности. Даже самые безопасные методы аутентификации теряют свою эффективность, если пользователи не могут или не хотят ими пользоваться [11, 12].

Важно учитывать фактор игнорирования нормативных требований в области аутентификации. В условиях растущих киберугроз соблюдение этих норм становится критически важным. Регулярные аудиты систем безопасности и адаптация методов аутентификации к актуальным стандартам требуют более пристального внимания. В противном случае организации рискуют столкнуться с серьезными юридическими последствиями [13].

Даже такие, казалось бы, надежные методы, как двухфакторная аутентификация (2FA), не защищают в полной мере, если атакующий знает пароль. Современные исследовательские работы подчеркивают, что не все способы многофакторной аутентификации равны. Некоторые из них могут быть легче обойдены, чем другие [14]. В случае, если два способа аутентификации зависят от одного и того же пароля, это, как правило, ставит под угрозу всю защиту системы [15].

Примеры инцидентов безопасности показывают, как кибератака может кардинально изменить предпочтения организаций. Например, в ряде случаев злоумышленники использовали виртуальные вирусы для перехвата временных кодов аутентификации из SMS-сообщений, что вынудило компании пересмотреть свою стратегию по использованию таких методов [16]. Это подчеркивает необходимость выбирать более надежные и безопасные методы аутентификации, которые способны противостоять новым типам угроз. Важным моментом является недостаток осведомленности пользователей о рисках безопасности и их методах защиты. Исследования показывают, что многие пользователи не осознают, какие методы аутентификации наиболее безопасны и какие могут быть обойдены злоумышленниками. Следовательно, организации должны уделять внимание обучению сотрудников, информируя их о рисках и лучших практиках по безопасности, чтобы минимизировать воздействие человеческого фактора на защищенность своих систем [17].

ЗАКЛЮЧЕНИЕ

Рассмотрим практические рекомендации по выбору методов аутентификации.

При выборе методов аутентификации для организаций рекомендуется учитывать специфику их работы и требования пользователей. Каждая категория организаций требует индивидуального подхода к выбору более подходящего метода, опираясь на оценку уровня безопасности и удобства использования.

Для традиционных компаний и малого бизнеса оптимально применять многослойную аутентификацию (MFA), основанную на паролях и одноразовых паролях (OTP). Это балансирует безопасность и простой доступ. Кроме того, внедрение менеджеров паролей и регулярная смена паролей помогут минимизировать риски несанкционированного доступа [1].

Финансовые и медицинские учреждения должны ориентироваться на методы с высокой степенью защиты, такие как аппаратные токены и биометрия, например, отпечатки пальцев. Для

этих организаций защита данных является критически важной задачей, что делает MFA весьма актуальным [10].

Технологические и интернет-компании могут рассмотреть беспарольные методы аутентификации, такие как FIDO2, в сочетании с биометрией. Это решение сочетает высокий уровень безопасности с удобством для пользователей, а также соответствует современным трендам [18].

Государственные и критически важные инфраструктуры требуют наиболее защищенных подходов – комбинации биометрических методов, таких как сканирование радужной оболочки, и сертификатов X.509. Эти требования обусловлены необходимостью защиты от высококвалифицированных атак [19].

Образовательные учреждения должны сосредоточиться на использовании многофакторной аутентификации, при этом акцентируя внимание на удобстве для студентов и преподавателей. Методы, такие как OTP и мобильные приложения, обеспечивают упрощенный доступ, снижая сложности, связанные с традиционными паролями [20].

Организации, работающие с IoT, могут использовать сертификаты X.509 для аутентификации устройств. Это необходимо для надежной идентификации множества устройств в развивающейся экосистеме смарт-технологий. Следует понимать, что растущая сложность такой среды требует проработанных решений [1].

Общие рекомендации для всех типов организаций заключаются в необходимости регулярного обновления политики аутентификации, обучения сотрудников основам кибербезопасности для снижения рисков фишинга и использования нежелательных паролей.

Список литературы

1. Лучшие методы аутентификации пользователей // skyeng.ru – URL: https://skyeng.ru/it-industry/it/luchshiye-metody-autentifikatsii-polzovatelya/

2. Аветисян В.А. Анализ существующих моделей обеспечения информационной безопасности в организациях / В.А. Аветисян, М.А. Маслова, С.П. Белов // Информационная безопасность в контексте развития общества: Материалы III Международной научно-практической и научно-методической конференции, Белгород, 28 марта 2023 года. – Белгород: Автономная некоммерческая организация высшего образования «Белгородский университет кооперации, экономики и права», 2023. – С. 67-79.

3. Карцан И.Н. Влияние кибербезопасности на обработку информации в развивающихся новых технологиях / И.Н. Карцан, Ю.Ю. Гончаренко // Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления: материалы VII Всероссийской научно-практической конференции, Москва, 29 декабря 2021 года. – Москва: Федеральное государственное бюджетное научное учреждение "Экспертно-аналитический центр", 2022. – С. 471-479.

4. Двухфакторная аутентификация: плюсы и минусы основных... // kontur.ru – URL: https://kontur.ru/aegis/blog/55728-dvuhfaktornaya_autentifikaciya

5. Кузьминых Е.С. Анализ роста кибератак и рынка информационной безопасности РФ / Е.С. Кузьминых, М.А. Маслова // Научный результат. Информационные технологии. – 2023. – Т. 8, № 2. – С. 11-17.

6. Кибермошенничество: портрет пострадавшего | Банк России… // cbr.ru – URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/

7. The Pros and Cons of Two-Factor Authentication Types and Methods // www.makeuseof.com – URL: https://www.makeuseof.com/tag/pros-cons-2fa-types-methods/

8. Определение критериев оценки для подбора оптимального... // moluch.ru – URL: https://moluch.ru/archive/131/36402

9. Как выбрать вендора для двухфакторной аутентификации: 10... // www.anti-malware.ru – URL: https://www.anti-malware.ru/practice/methods/how-to-choose-2fa-vendor

10. Белов Е.Б. К вопросу о культуре информационной безопасности / Е.Б. Белов, М.И. Ожиганова, А.Д. Костюков // Социотехнические и гуманитарные аспекты информационной безопасности: материалы Всероссийской научно-практической конференции, Пятигорск, 10–13 апреля 2019 года. – Пятигорск: Пятигорский государственный университет, 2019. – С. 43-48.

11. Защита биометрических данных систем искусственного интеллекта от состязательных атак / В.М. Герасимов, М.А. Маслова, Э.И. Халилаева, Н.С. Смирнов // Информация и безопасность. – 2023. – Т. 26, № 1. – С. 133-142.

12. Ошибка аутентификации: что такое, причины и способы решения // skyeng.ru – URL: https://skyeng.ru/magazine/wiki/it-industriya/chto-takoe-oshibka-autentifikatcii/

13. Часто встречающиеся ошибки при использовании 2FA и их... // sky.pro – URL: https://sky.pro/wiki/profession/chasto-vstrechayushiesya-oshibki-pri-ispolzovanii-2fa-i-ih-resheniya/

14. Эксперт предупредил об уязвимости двухфакторной... // 1prime.ru – URL: https://1prime.ru/20251005/ekspert--863169642.html

15. Могут ли злоумышленники обойти многофакторную... // www.keepersecurity.com – URL: https://www.keepersecurity.com/blog/ru/2024/03/14/can-mfa-be-bypassed-by-cybercriminals/

16. Аутентификация: стойкость к кибератакам, перспективы MFA... // cisoclub.ru – URL: https://cisoclub.ru/autentifikacija/

17. Девицына С.Н., Пилькевич П.В. Обеспечение совместимости технических компонентов при создании системы мониторинга инцидентов информационной безопасности. – Вопросы кибербезопасности. 2024. № 4 (62). С. 38-44.

18. Обзор способов и протоколов аутентификации... / Хабр // habr.com – URL: https://habr.com/ru/companies/dataart/articles/262817/

19. Системы и методы аутентификации... – Контур.Эгида // kontur.ru – URL: https://kontur.ru/aegis/blog/54186-sistemy_i_metody_autentifikacii_polzovatelej

20. Кузьминых Е.С. Анализ сетевых атак и защита от них / Е.С. Кузьминых, А.Ю. Мордвинова // Проблемы проектирования, применения и безопасности информационных систем в условиях цифровой экономики: Материалы XXII Международной научно-практической конференции, Ростов-на-Дону, 21–22 ноября 2022 года. – Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2022. – С. 105-109.

References

1. Best Methods of User Authentication // skyeng.ru – URL: https://skyeng.ru/it-industry/it/luchshiye-metody-autentifikatsii-polzovatelya/

2. Avetisyan V.A. Analysis of Existing Models of Information Security in Organizations / V.A. Avetisyan, M.A. Maslova, S.P. Belov // Information Security in the Context of Society Development: Proceedings of the III International Scientific-Practical and Scientific-Methodological Conference, Belgorod, March 28, 2023. – Belgorod: Autonomous Non-Commercial Organization of Higher Education “Belgorod University of Cooperation, Economics and Law”, 2023. – Pp. 67-79.

3. Kartsan I.N. The Impact of Cybersecurity on Information Processing in Developing New Technologies / I.N. Kartsan, Yu.Yu. Goncharenko // Issues of control of economic activity and financial audit, national security, systems analysis and management: Proceedings of the VII All-Russian scientific and practical conference, Moscow, December 29, 2021. – Moscow: Federal State Budgetary Scientific Institution "Expert-Analytical Center", 2022. – Pp. 471-479.

4. Two-factor authentication: pros and cons of the main... // kontur.ru/ – URL: https://kontur.ru/aegis/blog/55728-dvuhfaktornaya_autentifikaciya

5. Kuzminykh E.S. Analysis of the growth of cyberattacks and the information security market of the Russian Federation / E.S. Kuzminykh, M.A. Maslova // Scientific result. Information technologies. – 2023. – Vol. 8, No. 2. – Pp. 11-17.

6. Cyber fraud: portrait of the victim | Bank of Russia... // cbr.ru – URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/

7. The Pros and Cons of Two-Factor Authentication Types and Methods // www.makeuseof.com – URL: https://www.makeuseof.com/tag/pros-cons-2fa-types-methods/

8. Defining Evaluation Criteria for Selecting the Optimal... // moluch.ru – URL: https://moluch.ru/archive/131/36402

9. How to Choose a Vendor for Two-Factor Authentication: 10... // www.anti-malware.ru – URL: https://www.anti-malware.ru/practice/methods/how-to-choose-2fa-vendor

10. Belov E.B. On the Issue of Information Security Culture / E.B. Belov, M.I. Ozhiganova, A.D. Kostyukov // Sociotechnical and Humanitarian Aspects of Information Security: Proceedings of the All-Russian Scientific and Practical Conference, Pyatigorsk, April 10–13, 2019. – Pyatigorsk: Pyatigorsk State University, 2019. – Pp. 43-48.

11. Protecting Biometric Data of Artificial Intelligence Systems from Adversarial Attacks / V.M. Gerasimov, M.A. Maslova, E.I. Khalilaeva, N.S. Smirnov // Information and Security. – 2023. – Vol. 26, No. 1. – Pp. 133–142.

12. Authentication Error: What It Is, Causes, and Solutions // skyeng.ru – URL: https://skyeng.ru/magazine/wiki/it-industriya/chto-takoe-oshibka-autentifikatcii/

13. Frequently Encountered Errors When Using 2FA and Their... // sky.pro – URL: https://sky.pro/wiki/profession/chasto-vstrechayushiesya-oshibki-pri-ispolzovanii-2fa-i-ih-resheniya/

14. An Expert Warned of the Vulnerability of Two-Factor... // 1prime.ru – URL: https://1prime.ru/20251005/ekspert--863169642.html

15. Can Attackers Bypass Multi-Factor... // www.keepersecurity.com – URL: https://www.keepersecurity.com/blog/ru/2024/03/14/can-mfa-be-bypassed-by-cybercriminals/

16. Authentication: Resistance to Cyberattacks, MFA Prospects... // cisoclub.ru – URL: https://cisoclub.ru/autentifikacija/

17. Devitsyna S.N., Pilkevich P.V. Ensuring Compatibility of Technical Components When Creating an Information Security Incident Monitoring System. – Cybersecurity Issues. – 2024. – No. 4 (62). – Pp. 38-44.

18. Review of authentication methods and protocols... / Habr // habr.com – URL: https://habr.com/ru/companies/dataart/articles/262817/

19. Authentication systems and methods... – Kontur.Egida // kontur.ru – URL: https://kontur.ru/aegis/blog/54186-sistemy_i_metody_autentifikacii_polzovatelej

20. Kuzminykh E.S. Analysis of network attacks and protection against them / E.S. Kuzminykh, A.Yu. Mordvinova // Problems of design, application and security of information systems in the digital economy: Proceedings of the XXII International Scientific and Practical Conference, Rostov-on-Don, November 21–22, 2022. – Rostov-on-Don: Rostov State University of Economics "RINH", 2022. – P. 105–109.

Абселямов Амет-Хан Алим-оглы, студент второго курса магистратуры кафедры «Информационная безопасность», ФГАОУ ВО Севастопольский государственный университет, г. Севастополь, Россия
Маслова Мария Александровна, доцент кафедры «Информационная безопасность», ФГАОУ ВО Севастопольский государственный университет, г. Севастополь, Россия
Лагуткина Татьяна Владимировна, старший преподаватель кафедры «Информационная безопасность», ФГАОУ ВО Севастопольский государственный университет, г. Севастополь, Россия

Abseljamov Amet-Khan Alim-ogly, second-year Master's Student of the Department of Information Security, Sevastopol State University, Sevastopol, Russia
Maslova Maria Aleksandrovna, Associate Professor of the Department of Information Security, Sevastopol State University, Sevastopol, Russia
Lagutkina Tatiana Vladimirovna, Senior Lecturer of the Department of Information Security, Sevastopol State University, Sevastopol, Russia