УДК 004.05 **DOI: 10.18413/2518-1092-2024-9-2-0-2**

Абселямов А.-Х.А.
Лагуткина Т.В.

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ НА ВЕБ-СЕРВИСАХ. ТЕКУЩИЕ ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

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

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

Аннотация
При развитии информационных технологий, обеспечение и защита данных на веб-сервисах имеет важное значений. Для обеспечения безопасности применяют различные методы и одним из главных есть процесс аутентификации пользователей. Применяют разные методы аутентификации: парольную, двухфакторную аутентификацию, биометрическую, многофакторную, на основе искусственного интеллекта и блокчейн технологий. Несмотря на их многообразие, каждый метод имеет свои преимущества и недостатки. Текущие тенденции в области аутентификации включают комбинирование различных методов для повышения надежности и улучшение пользовательского опыта. Перспективы развития данной технологии связаны с поиском новых способов балансировки между безопасностью и удобством использования, а также постоянным обновлениям и адаптацией методов к изменяющимся угрозам безопасности. В данной статье проводится исследование различных методов аутентификации на веб-сервисах с целью выявления их эффективности, преимуществ и недостатков.

Ключевые слова: аутентификация; веб-сервисы; безопасность данных; угрозы; защита; многофакторная аутентификация; биометрическая идентификация; пароль; двухфакторная аутентификация; технологии

Для цитирования: Абселямов А.-Х.А., Лагуткина Т.В. Исследование методов аутентификации на веб-сервисах. Текущие тенденции и перспективы развития // Научный результат. Информационные технологии. – Т.9, №2, 2024. – С. 12-20. DOI: 10.18413/2518-1092-2024-9-2-0-2

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

INVESTIGATION OF AUTHENTICATION METHODS ON WEB SERVICES. CURRENT TRENDS AND DEVELOPMENT PROSPECTS

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

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

Abstract
In the development of information technology, software and data protection on web services are of great importance. To ensure security, various methods are used, and one of the main ones is the user authentication process. They use different authentication methods: password, two-factor authentication, biometric, multi-factor, based on artificial intelligence and blockchain technologies. Despite their diversity, each method has its own advantages and disadvantages. Current trends in authentication include combining different methods to increase reliability and improve the user experience. The future of this technology involves finding new ways to balance security and usability, as well as continually updating and adapting methods to changing security threats. This article conducts a study of various authentication methods for web services in order to identify their effectiveness, advantages and disadvantages.

Keywords: authentication; web services; data security; threats; protection; multi-factor authentication; biometric identification; password; two-factor authentication; technology
For citation: Abselyamov A.-H.A., Lagutkina T.V. Investigation of authentication methods on web services. Current trends and development prospects // Research result. Information technologies. – T. 9, №2, 2024. – P. 12-20. DOI: 10.18413/2518-1092-2024-9-2-0-2

ВВЕДЕНИЕ

Исследование методов аутентификации на веб-сервисах становится все более актуальной темой в современном цифровом мире. С ростом числа онлайн-платформ и сервисов усиливается и потребность в эффективных методах обеспечения безопасности данных и контроля доступа.

Аутентификация пользователей на веб-сервисах является первым шагом в обеспечении безопасности информации. Существует множество методов аутентификации, от классической парольной защиты до более современных биометрических технологий.

В статье будет проведен анализ эффективности, положительные и отрицательные стороны различных методов аутентификации на веб-сервисах с выявлением нынешних тенденции в области аутентификации, а также их перспективы развития. Необходимо так же обратить внимание на критически важные аспекты безопасности в контексте веб-сервисов, таких как угрозы безопасности, методы защиты от них и перспективы развития технологий аутентификации. Проанализируем и выявим, какие методы аутентификации являются наиболее эффективными и как можно улучшить безопасность веб-сервисов в целом [1, 2].

ОСНОВНАЯ ЧАСТЬ

Рассмотрим и проанализируем существующие методы аутентификации.

1) Парольная аутентификация – один из самых распространенных методов проверки подлинности пользователя в сети. Она основывается на знании уникального комбинированного пароля, который вводит пользователь для доступа к своему аккаунту. Однако, несмотря на свою популярность, парольная аутентификация имеет недостатки, такие как:

– недостаточная безопасность. Пароли могут быть подвержены атакам перебора, особенно если они короткие или слабые; многие пользователи используют один и тот же пароль для разных сервисов, что увеличивает риск компрометации;

– фишинг. Злоумышленники могут пытаться выманить пароли у пользователей, под видом официальных запросов, что делает парольную аутентификацию уязвимой к атакам фишинга;

– забывчивость. Пользователи часто забывают свои пароли или используют сложные комбинации, которые трудно запомнить, что может вызвать неудобство в работе и снизить возможное использование сервиса.

Отрицательные стороны всегда присутствуют, необходимо стремиться к их уменьшению. Парольная аутентификация применяется везде и является самой часто используемой, так как проста и затраты на ее внедрение минимальные. Для того, чтобы избавиться от отрицательных сторон метода, подстроиться под изменения, своевременно реагировать на различные виды мошенничества – необходимо внедрять в работу дополнительные виды аутентификации [3].

2) Двухфакторная аутентификация. Данный метод выполняет проверку подлинности паролем и применением дополнительного метода. Для этого применяют физические устройства, биометрические данные или одноразовый поступающий код, что дает возможность увеличить уровень безопасности в несколько раз.

Что собой представляют данные методы:

– физические устройства, в данном методе пользователь применяет дополнительное устройство в виде смарт – карты или USB-ключа для того, чтобы подтвердить свою личность. Для этого устройства защищают дополнительными мерами для большей безопасности, а именно PIN- кодами или биометрическими данными:

– биометрическая аутентификация – это дополнительное подтверждение при входе пользователя в систему. Для этого используют отпечаток пальца, или распознавание по лицу, которые устанавливается заранее, когда пользователь регистрируется.

– одноразовые коды, представляют собой дополнительный метод аутентификации, который помогает хорошо обезопасить несанкционированный вход другого пользователя. Так как пользователя приходит уникальный код, который генерируется автоматически после запроса пользователя и вводится в необходимое окно после ввода пароля. Обязательным условием кода есть ограниченное время его действия, что тоже добавляет большей защищенности. Воспользоваться можно лишь завладев телефоном пользователя и зная его входы в систему. Для этого желательно не ставить автоматическое сохранение паролей, чтобы обезопасить себя от неправомерного входа в ваш аккаунт.

Двухфакторная аутентификация набирает популярность все в больших сферах жизнедеятельности человека, таких как банковские операции, вход на госуслуги, налоговый аккаунт и другие важные для человека ресурсы. Она помогает уменьшить возможные риски и компрометацию аккаунтов пользователей [4].

3) Биометрическая аутентификация. Данный вид дает возможность человеку подтвердить вход с помощью уникальных биологических характеристик: лица, сетчатки глаза, отпечатка пальца, голоса, походки и других неповторяющиеся данные пользователя. Данный вид постоянно увеличивает свое поле деятельности, так как является серьезной защитой. В таблице 1 приведены основные методы и их характеристики.

Таблица 1

Основные биометрические методы и их характеристики

Table 1

Basic biometric methods and their characteristics

№	Название	Точность	Стоимость	Характеристика
1.	Отпечаток пальца	Высокая	Низкая	Самый распространенный на данный момент метод. Используется множеством пользователей для блокировки и разблокировки смартфонов, банковских приложений и других видов программ. В организациях используется для прохождения на секретные объекты.
2.	Лицо	Средняя	Высокая	Распознавание проводится на основе уникальных черт лица пользователя: форма, расстояние между глазами, особенности носа и основываться метод так же может на основе фотографии или видеоизображении лица
3.	Голос	Низкая	Средняя	Голос также является уникальным у каждого человека: тональность, быстрота речи, интонация и т.д. очень важный метод, так как существуют системы, которые работают только на основе голосовой идентификации
4.	Сетчатка глаза	Высокая	Высокая	Не очень распространена, но уже некоторые системы используют данный вид биометрической аутентификации за счет уникальности каждого глаза человека. Метод основывается на формировании до 266 уникальных точек идентификации на изображении роговицы. Проверка по данному типу происходит не более чем за 1 м и идет формирование действий таких как: выделение зрачка, определение количества точек радужной оболочки и уже принятие решений и сравнение в имеющейся базе данных. Даже при неполном скане зрачка, хватает 1/3 радужки, чтобы

				проверить его на точность, и ошибка всего может иметь вероятность 1 к 100 тыс. [5].
5.	Походка	Высокая	Средняя	Ходьба человека является также индивидуальной и не повторимой, различается ее стиль хождения, длина и ширина шага, скорость ходьбы. По-разному происходит движение суставов и угол их поворота. Эффективность распознавания походки зависит от различных методов компьютерного зрения который проводят слежку, обнаружение и анализируют походку при ходьбе. Данный вид мало применим в нынешнее время, но является одним из эффективных методов.
6.	Вены	Высокая	Средняя	Структура вен человека неповторима и это один из методов будущей биометрии, который хотят внедрить для технологий создания биометрических паспортов людей. Пока данный вид биометрии слабо развит и применяется всего лишь около 3%. В данном виде биометрии применяют сканер с инфракрасным светом, считывающий изображение вен ладони человека. Далее с помощью математических преобразований происходит построение узора и преобразование его в цифровой код. Постепенно формируется база, по которой после и проходит идентификация.
7.	Поведение	Средняя	Средняя	Данный вид аутентификации не такой распространённый, но действенный. Он устанавливается на основе действий пользователей, а именно по его действиям с ПК: набор текста, движение мыши и т.д. [10].

Благодаря уникальным характеристикам человека данный вид биометрии является одним из самых точных. Минусами данного метода является то, что люди имеют свойство меняться, а именно: косметические средства, травмы и раны человека, операции по изменению и корректировки тела человека, а также старение человека.

Но применение данных методов в мошенничестве так же продолжает развиваться и дает возможность использование и применение биометрии в коррупционных и обманных схемах [6, 7].

1) Токены. Данный вид мошенничества аутентификации через социальные сети владельцев. Мошенники используют чужие социальные сети, аккаунты. Одним из частых видов аутентификации является подтверждение через социальные сети своей личности [8]. Что дает возможность мошенникам заходить и выполнять действия за пользователя «взорвав» их аккаунт. Токены дают возможность пользователю входов в приложения и системы. Они могут быть как временные, так и постоянные с предоставлением доступа к определенным функциям и ресурсам [8].

2) SMS. Очень удобный способ, так как телефон всегда с человеком и мало кто в него может войти, если, конечно, его не украдут, и пользователь не оставляет его без присмотра. Пользователю может установить дополнительное подтверждение своей личности через SMS. При входе ему будет приходить проверочный код, который необходимо ввести для подтверждения своей личности. Если же он неверный, то зайти в свой аккаунт не будет возможности. Минус данного метода в том, что, если покрытие сети будет плохое или там, где ее нет – пользователь не сможет выполнить вход. А в нынешнем ритме жизни не всегда это удобно.

3) Электронная почта является также дополнительным методом аутентификации. При регистрации на каком-либо ресурсе или входе в какой-либо аккаунт устанавливается дополнительная аутентификация с помощью электронной почты. Пользователю приходит письмо с подтверждением с ссылкой, по которой необходимо перейти и подтвердить свою личность. Угрозой

так же является возможное несанкционированное завладение электронной почтой пользователя и является одним из часто используемых для краж и компрометации владельцев.

4) Характеристики устройства. Аутентификация в данном виде проходит с помощью идентификаторов устройства, IP-адресов. Очень часто так вычисляют мошенников и хакеров с помощью спец. служб.

5) Многофакторная аутентификация. Данный вид представляет собой использования различных видов входа пользователя в систему или к ресурсам, а также в значительной мере повышает уровень безопасности и предотвращает несанкционированный доступ к данным и аккаунтам пользователя. Все чаще используется многофакторная аутентификация, особенно в специализированных и государственных учреждениях. Так как злоумышленники находят все более новые способы для взлома и несанкционированного входа в базы данных организаций и личные данные, и аккаунты пользователей. При многофакторной аутентификации повышается уровень безопасности и даже если злоумышленникам удалось взломать, например пароль, то следующий уровень уже даст препятствие и невозможность взлома, и завладение информацией пользователей.

Какими же методами пользуются злоумышленники для перехватов и фишинга, чтобы обойти уровни аутентификации, см. таблицу 2.

Таблица 2

Уязвимости и угрозы

Table 2

Vulnerabilities and threats

№	Вид	Характеристика
1.	Социальная инженерия	Один из самых распространенных методов на сегодняшний день. Не смотря на угрозы, люди продолжают доверять друг другу и самое главное то, что в данном методе мошенники «играют» на чувствах людей и на методе «неожиданности». Они втираются в доверие, предоставляются жертвами или родственниками жертвы, сотрудниками банков и других государственных служб и выманивают необходимые им данные. Просят сообщить SMS код с телефона, предоставить пароль или проверочное слово для банковской карты, перевести деньги на номер, как будто случилось что с родственником и это единственный выход и т.д., все то, что может быстро повлиять на человека и в растерянности он может сделать.
2.	Технические уязвимости	Это технические проблемы, недостатки или «дыры» в программном обеспечении, устаревшие или слабые алгоритмы шифрования. Необходимым методом является наличие грамотного сотрудника, постоянный мониторинг рисков, новых уязвимостей и наличие постоянно дополняющихся рекомендаций к действиям при сложившейся ситуации и методам их устранения.
3.	Компрометация устройств	Кража, компрометация или потеря устройства, с помощью которого можно выполнить вход в аккаунты пользователя, которое предназначено для дополнительного фактора аутентификации. Например – мобильный телефон, на который приходят SMS, имеется беспарольная почта и др. виды подтверждения аутентификации.
4.	Обход многофакторной аутентификации	Методы, с помощью которых злоумышленники могут обойти многофакторную аутентификация: выманивание у жертвы данных, SMS-сообщений, использование биометрических данных жертвы и т.д.

Из приведенных данных видно, что многофакторная аутентификация является хорошей защитой данных пользователей и их аккаунтов. Но для этого необходимо быть внимательным, соблюдать меры безопасности, не отвечать на подозрительные звонки, не переходить по

подозрительным и неизвестным ссылкам и тогда данные будут хорошо защищены на сервисах и платформах. Но многие пользователи не приемлет данный вид аутентификации, так как это доставляет им неудобства в долгом входе, дополнительных действиях, которые им кажутся сложными и утомительными. Поэтому разработчикам стоить обратить внимание на более удобные, быстрые и понятные самым обычным и малограмотным пользователям методам для защиты их аккаунтов [12].

В цифровом мире даже для обычных пользователей начали развиваться такие методы, например:

– биометрические технологии или как их еще называют мультимодальная биометрия, о которой говорилось выше – распознавание лица, использование отпечатков пальцев, голосовая аутентификация которые применяют одновременно, тем самым увеличивая безопасность и уменьшая вероятность ошибок;

– блокчейн технологии. Данная технология обладает большей сложностью к мошенничеству, дает новые подходы к аутентификации. Блокчейн основана на распределенном реестре данных и дает высокие уровень безопасности, который используется в различных сферах жизнедеятельности: финансовых, государственных, электронной коммерции и т.д.;

– искусственный интеллект и машинное обучение. За этими методами аутентификации – будущее. Уже применение их очень велико, растет с каждый годом. Предприятия, организации и фирмы все больше внедряют данный вид аутентификации. Данные технологии используют для анализа биометрических данных, поведения пользователей, поиска аномалий, улучшения аутентификации в реальном времени. Благодаря искусственному интеллекту (ИИ), применяемому в биометрии, появилась возможность обучать ИИ и создавать более точные, надежные и автоматизированные системы идентификации с высокой точностью. С помощью искусственного интеллекта появилась возможность для высокой защиты личных данных пользователей и аккаунтов от взломов и киберугроз[13].

На данный момент нет действующего четкого законодательства в данной сфере, то в марте 2023 г. этот вопрос был поднят главой SpaceX, Tesla, X Илоном Маском и другими экспертами и руководителями отрасли по внедрению и развитию ИИ. Они обратились с открытым письмом о том, чтобы приостановили различные разработки ИИ пока не будут приняты, внедрены меры, законы и наказания в данной сфере, а также пока не будут проверены общие протоколы безопасности специально назначенными независимыми экспертами, для того, чтобы все могли понимать то, что данные ИИ будут идти на благо людям и обществу, и будут управляемыми с возможностью приостановки или изменения [14].

По статистике динамика сумм инвестиций в компании по кибербезопасности, которые занимаются продуктами с применением технологий ИИ с каждым годом растет в 3–5 раз, а оценка использования технологий ИИ в кибербезопасности по функциональным направлениям также возрастает (рис.).

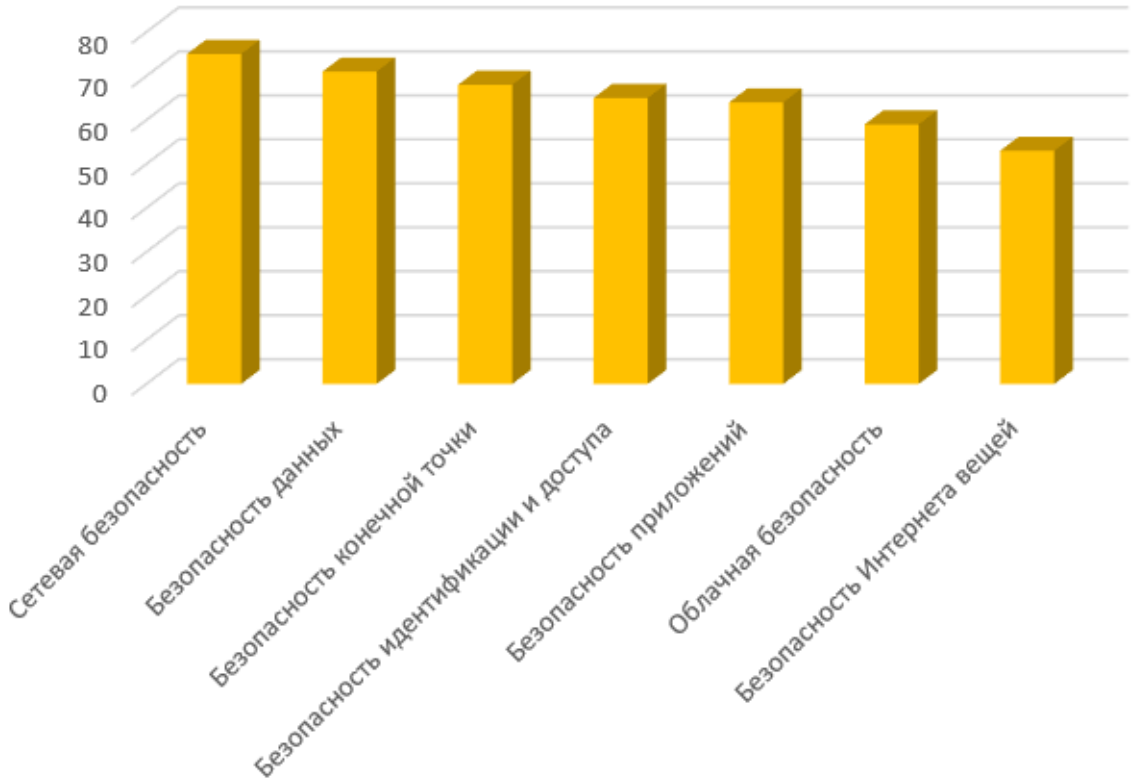

Рис. Использование кибербезопасности в различных областях, %
Fig. Use of cybersecurity in various areas, %

Как говорят эксперты, что использование, усовершенствование технологий и разработка ИИ особенно в сфере биометрии распознавания по лицам может привести к самым неожиданным, негативным и катастрофическим последствия, если данная технология будет использоваться без определенного понимания, как же может влиять они на права человека. Поэтому во всем должен быть порядок, определены правила, законы и наказания по применению и использованию данных технологий.

ЗАКЛЮЧЕНИЕ

Из представленного анализа и описания можно сделать вывод, что рассмотренные методы аутентификации имеют свои достоинства и недостатки, эффективность, методы применения, но при выборе защиты данных необходимо исходить из удобства, необходимости в определенном уровне защиты, эффективности методов, требований пользователя к защите данных. Все приведенные методы должны быть как удобны, так и безопасны в использовании. Поэтому очень важно постоянно следить не только за новыми появляющимися методами, но и за появляющимися новыми уязвимостями и рисками, которые придумывают мошенники. В целом, биометрическая идентификация играет важную роль в современном мире, и ее безопасность является приоритетной задачей для разработчиков и исследователей.

Список литературы

1. Феоктистов И.В. Сравнительное исследование методов аутентификации в информационных системах // Инновации и инвестиции. – 2023. – №. 7. – С. 193-198.
2. Хрунов С.Н. Разработка и исследование методов аутентификации // Аспирант. – 2016. – №. 3. – С. 189-191.
3. Байдицкая В.К., Лиманова Н.И. Исследование методов аутентификации на основе генерации одноразовых паролей // Прикладная математика и информатика: современные исследования в области естественных и технических наук. – 2017. – С. 57-60.

4. Маслова М.А., Аветисян В.А. Риски информационной безопасности в условиях удаленного подключения и облачного присутствия // Вестник УрФО. Безопасность в информационной сфере. – 2023. – № 3(49). – С. 54-60.

5. Сканер вен как будущее биометрии (bio-smart.ru) [Электронный ресурс]. URL: https://bio-smart.ru/tpost/pjx36nnktb-skaner-ven-kak-buduschee-biometrii

6. Герасимов В.М., Маслова М.А. Возможные угрозы и атаки на систему голосовой идентификации пользователя // Научный результат. Информационные технологии. – 2022. – Т. 7, № 1. – С. 32-37.

7. Герасимов В.М., Маслова М.А. Необходимость комплексной системы защиты биометрического голосового отпечатка от воздействия кибермошенников в сети интернет // Вестник Луганского государственного университета имени Владимира Даля. – 2022. – № 5(59). – С. 95-102.

8. Обзор способов и протоколов аутентификации в веб-приложениях [Электронный ресурс]. URL: https://habr.com/ru/companies/dataart/articles/262817/.

9. Мартынова Л.Е., Умницын М.Ю., Назарова К.Е., Пересыпкин И.П. Исследование и сравнительный анализ методов аутентификации // Молодой ученый. – 2016. – № 19 (123). – С. 90-93. – URL: https://moluch.ru/archive/123/34077/.

10. Анализ уязвимостей процесса аутентификации [Электронный ресурс]. URL: https://bmsdave.github.io/blog/auth-vulnerabilities/.

11. Халилаева Э.И., Маслова М.А., Герасимов В.М. Система противодействия методам социальной инженерии в области информационной безопасности // Вестник УрФО. Безопасность в информационной сфере. – 2023. – № 2(48). – С. 54-61.

12. Палютина Г. Н. Применение технологии вероятностных экспертных систем для оценки заключений системы многофакторной аутентификации // Актуальные вопросы информационной безопасности регионов в условиях перехода России к цифровой экономике : материалы VII Всероссийской научно-практической конференции, Волгоград, 26–27 апреля 2018 года / Волгоградский государственный университет. – Волгоград: Волгоградский государственный университет, 2018. – С. 51-55.

13. Коровянский И.А., Пильгаева В.В., Палютина Г.Н. Методы защиты и атаки с помощью искусственного интеллекта // Информационные системы, экономика и управление: Ученые записки. Выпуск 24. – Ростов-на-Дону: Ростовский государственный экономический университет "РИНХ", 2022. – С. 38-40.

14. Регулирование ИИ (AI) / Хабр (habr.com) [Электронный ресурс]. URL: https://habr.com/ru/articles/789544/.

References

1. Feoktistov I.V. Comparative study of authentication methods in information systems // Innovations and investments. – 2023. – No. 7. – pp. 193-198.

2. Khrunov S.N. Development and research of authentication methods // Postgraduate student. – 2016. – No 3. – pp. 189-191.

3. Baiditskaya V.K., Limanova N.I. Research of authentication methods based on generation of one-time passwords //Applied mathematics and computer science: modern research in the field of natural and technical sciences. – 2017. – P. 57-60.

4. Maslova M.A., Avetisyan V.A. Risks of information security in conditions of remote connection and cloud presence // Bulletin of the Urals Federal District. Security in the information sphere. – 2023. – No. 3(49). – P. 54-60.

5. Vein scanner as the future of biometrics (bio-smart.ru) [Electronic resource]. URL: https://bio-smart.ru/tpost/pjx36nnktb-skaner-ven-kak-buduschee-biometrii

6. Gerasimov V.M., Maslova M.A. Possible threats and attacks on the user voice identification system // Research result. Information technologies. – T.7, №1, 2022. – P. 32-37. DOI: 10.18413/2518-1092-2022-7-1-0-4

7. Gerasimov V.M., Maslova M.A. The need for a comprehensive system for protecting a biometric voice print from the influence of cyber fraudsters on the Internet // Bulletin of Lugansk State University named after Vladimir Dahl. – 2022. – No. 5(59). – P. 95-102.

8. Review of authentication methods and protocols in web applications [Electronic resource]. URL: https://habr.com/ru/companies/dataart/articles/262817/.

9. Martynova L.E., Umnitsyn M.Yu., Nazarova K.E., Peresypkin I.P. Research and comparative analysis of authentication methods // Young scientist. – 2016. – No. 19 (123). – P. 90-93. – URL: https://moluch.ru/archive/123/34077/.

10. Analysis of vulnerabilities of the authentication process [Electronic resource]. URL: https://bmsdave.github.io/blog/auth-vulnerabilities/.

11.Khalilaeva E.I., Maslova M.A., Gerasimov V.M. System of counteraction to social engineering methods in the field of information security // Bulletin of the Urals Federal District. Security in the information sphere. – 2023. – No. 2(48). – P. 54-61.

12.Palutina G.N. Application of the technology of probabilistic expert systems to evaluate the conclusions of a multi-factor authentication system // Current issues of regional information security in the context of Russia's transition to a digital economy: materials of the VII All-Russian Scientific and Practical Conference, Volgograd, April 26–27, 2018 / Volgograd State University. – Volgograd: Volgograd State University, 2018. – pp. 51-55.

13.Korovyansky I.A., Pilgaeva V.V., Palutina G.N. Methods of defense and attack using artificial intelligence // Information systems, economics and management: Scientific notes. Volume Issue 24. – Rostov-on-Don: Rostov State Economic University "RINH", 2022. – P. 38-40.

14.Regulation of AI (AI) / Habr (habr.com) [Electronic resource]. URL: https://habr.com/ru/articles/789544/.

Абселямов Амет-Хан Алим-оглы, студент четвертого курса кафедры «Информационная безопасность»
Лагуткина Татьяна Владимировна, ассистент кафедры «Информационная безопасность»

Abselyamov Amet-Han Alim-ogly, 4th year student of the Department of Information Security
Lagutkina Tatyana Vladimirovna, Assistant of the Department of Information Security