ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРИНЯТИЕ РЕШЕНИЙ
ARTIFICIAL INTELLIGENCE AND DECISION MAKING

УДК 004.056 **DOI: 10.18413/2518-1092-2022-7-4-0-7**

Надейкина В.С.
Лагуткина Т.В.

АНАЛИЗ СПОСОБОВ РЕАЛИЗАЦИИ СИСТЕМЫ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ

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

e-mail: nice.nadeykina@mail.ru, lagutkina.tatiana@mail.ru

Аннотация
Роль уязвимостей в защите информации занимает большую нишу, для традиционной однофакторной аутентификации является серьезной проблемой как для специалистов по безопасности и исследователей данной проблемы. Решений безопасности должны быть своевременными и продуктивными. В данном направлении были разработаны новые технологически продвинутые инструменты многофакторной аутентификации. Multi-factor Authentication (MFA). Данная технология сочетает в себе два или более типов аутентификации для обеспечения и улучшения дополнительных способов безопасности аутентификации пользователей. Рассмотрим и проанализируем некоторые способы реализации многофакторной аутентификации.
Ключевые слова: аутентификация; многофакторная аутентификация; принципы аутентификации; способы реализации многофакторной аутентификации; MFA
Для цитирования: Надейкина В.С., Лагуткина Т.В. Анализ способов реализации системы многофакторной аутентификации // Научный результат. Информационные технологии. – Т.7, №4, 2022. – С. 59-66. DOI: 10.18413/2518-1092-2022-7-4-0-7

Nadeikina V.S.
Lagutkina T.V.

ANALYSIS OF WAYS TO IMPLEMENT A MULTI-FACTOR AUTHENTICATION SYSTEM

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

e-mail: nice.nadeykina@mail.ru, lagutkina.tatiana@mail.ru

Abstract
The role of vulnerabilities in information security occupies a large niche, for traditional one-factor authentication is a serious problem for both security specialists and researchers of this problem. Security solutions must be timely and productive. In this direction, new technologically advanced multi-factor authentication tools have been developed. Multi-factor Authentication (MFA). This technology combines two or more types of authentication to provide and enhance additional security methods for user authentication. Consider and analyze some ways to implement multi-factor authentication.
Keywords: authentication; multi-factor authentication; authentication principles; ways to implement multi-factor authentication; MFA
For citation: Nadeikina V.S., Lagutkina T.V. Analysis of ways to implement a multi-factor authentication system // Research result. Information technologies. – T.7, №4, 2022. – P. 59-66. DOI: 10.18413/2518-1092-2022-7-4-0-7

ВВЕДЕНИЕ

С развитием Интернета стали доступны различные виды онлайн-сервисов. Однако Интернет не обеспечивает прямого взаимодействия между пользователями. Невозможно физически аутентифицировать пользователей для доступа к важным ресурсам. Поэтому аутентификация законных пользователей интернет-услуг имеет первостепенное значение.

Для аутентификации пользователей изначально использовали однофакторную аутентификацию, но с ростом уязвимостей и рисков стала острая необходимость в ее более тщательной защите [1].

Несмотря на свою распространенность, системы защиты паролей достаточно слабы с точки зрения безопасности. Если обозначить строгие требования к паролю (пароли должны состоять из 8-16 символов, представлять собой псевдослучайную последовательность и содержать буквы разных регистров, цифры и специальные символы, при этом пароли необходимо менять каждые 3 месяца и использовать разные пароли для разных ресурсов), то это усложнит их запоминание. Предоставление общего доступа к паролю может быстро поставить вашу учетную запись под угрозу. Кроме того, неавторизованные пользователи могут попытаться получить доступ с помощью «атак методом перебора», «радужных таблиц», или методов социальной инженерии.

Компания, ведущая свою деятельность в сфере информационной безопасности, «Лаборатория Касперского» собрала анонимизированную статистику: 150 тысяч россиян за период с января по сентябрь 2022 года подверглись кибератакам, нацеленным на кражи паролей и логинов от учётных записей в мессенджерах, соцсетях, игровых сервисах, онлайн-банках.

Злоумышленники используют вирусы-стилеры (трояны) для кражи паролей и учетных данных из браузеров и мессенджеров для компьютеров. Эти вирусы находят информацию в системных файлах Windows или в реестре, затем отправляют данные мошенникам. [1]

С диверсификацией и изощренностью хакерских методов безопасность и аутентификация больше не зависят исключительно от ее идентификатора и аутентификации по паролю. Таким образом возникает потребность использования дополнительных факторов аутентификации.

ОСНОВНАЯ ЧАСТЬ

Процесс однофакторной аутентификации имеет стандартное описание. Пользователь для своей идентификации оправляет идентификатор – x в систему, которая проверяет его, вычисляя функцию $F(x)$ на получение верного сохраненного значения y. Многофакторная аутентификация (MFA) — это метод идентификации пользователя, который сочетает в себе ряд аутентификаций разных типов.

О силе механизма аутентификации можно судить по тому, от скольких факторов он зависит, чем больше дополнительных уровней безопасности будет применено, тем эффективнее будет защита учетной записи от несанкционированного доступа к аккаунтам пользователей.

Фактор аутентификации – это категория учетных данных, используемых для проверки личности. Для MFA каждый дополнительный элемент предназначен для повышения уверенности в том, является ли подлинным идентификатор объекта, запрашивающего доступ к системе. Использование нескольких форм аутентификации может затруднить работу хакеров. Выделяют три основных фактора для многофакторной аутентификации (рис. 1) [2].

Первый фактор – фактор знания – информация, известная только пользователю. Это, например, пароли, секретные вопросы и ответы на них, кодовые слова, идентификационные номера (PIN-коды) и другое. Чтобы использовать фактор знаний для MFA, пользователь должен ввести информацию, которая соответствует сведениям, ранее сохраненным в базе данных.

Второй фактор – фактор владения – любые предметы, принадлежащие объекту аутентификации. К таким предметам относятся токены безопасности, смарт-карты для генерации одноразовых кодов, сим-карта мобильного телефона и другое.

Третий фактор – фактор свойства – к этому фактору относятся какие-либо биометрические данные (отпечатки пальцев, рисунок радужной оболочки глаза и сетчатки, геометрия кисти руки, очертания и размеры лица, тембры голоса, рисунок вен) или модель поведения [3, 4].

Помимо основных факторов MFA, используются также дополнительные (рис. 1). [5]

Фактор основанные на местоположении и времени – использование метаданных и параметров сети, координат GPS, а также распознавание аппаратных средств, с помощью которых совершается аутентификация.

Фактор на основе использования социальных сетей – использование данных веб-сайта, которому пользователь предоставил разрешение. Среди используемых данных – пароль и имя пользователя для совершения входа на онлайн-ресурс.

Фактор на основе рисков (адаптивная MFA) – сочетание адаптивной аутентификации и алгоритмов вычисления рисков. Эта аутентификация предназначена для уменьшения количества избыточных входов в систему [6].

Многофакторной аутентификация сочетает в себе два или более типов аутентификации, чтобы обеспечить лучший и безопасный способ аутентификации пользователей. Целью MFA является создание многоуровневой защиты, которая затрудняет несанкционированный доступ к цели – вычислительное устройство, сеть, база данных, физическое местоположение и даже компрометация одного фактора или его нарушение не даст ему доступа, а придется еще потратить время для преодоления еще нескольких барьеров для окончательного проникновения или взлома.

Рис. 1. Факторы аутентификации
Fig. 1. Authentication factors

Рассмотрим некоторые из способов реализации MFA.

Биометрическая аутентификация. При таком типе аутентификации используется совокупность нескольких биометрических технологий. В современном подходе, биометрические характеристики можно разделить на два основных класса:

– физиологический класс представляет собой: отпечатки пальцев, распознавание лиц и радужной оболочки, геометрия рук, голос (поскольку у разных людей разные свойства голоса);

– поведенческий класс связан с моделью поведения человека - подпись, динамика нажатия клавиш и манера речи. Голос можно отнести и к физиологическому фактору [6 -8, 15].

Недавно была разработана новая тенденция, которая объединяет человеческое восприятие с компьютером – база данных в интерфейсе мозг-машина. Этот подход называют когнитивной биометрикой – основана на данных о специфической реакции мозга на раздражители, которые могут быть использованы для запуска поиска в компьютерной базе данных.

Биометрические системы могут выполнять две функции: верификацию и аутентификацию. Следовательно, используемые методы, должны быть достаточно надежными, чтобы можно было использовать обе эти возможности одновременно. В настоящее время разрабатываются когнитивные биометрические системы, которые используют реакцию мозга на обонятельные стимулы, распознавание лиц и умственные способности для поиска в портах и зонах повышенной безопасности.

Существуют другие стратегии разработки – ДНК, геометрия рук по отпечаткам ладоней, ходьбе, сетчатки, рисунке вен на руках, запахов, термограмме лица и ушном канале, которые внедряются все больше для решений различных угроз в информационной безопасности. Так как данные неповторимы использование биометрии помогает достигать высокой степени безопасности, которую еще нужно очень серьезно дорабатывать и развивать.

Риски компрометации распределенной базы данных биометрических данных, которые применяют в приложениях безопасности, имеют высокий уровень при определении конфиденциальности отдельных лиц и, следовательно, о неразглашении. Развития и пути решения в необходимости таких баз данных можно достичь путем грамотного применения биометрии без ущерба для безопасности

Биометрическая криптография. При таком способе данные защищены с использованием системы симметричного шифрования, в то время как системы с открытым ключом используются для цифровых подписей и для безопасного обмена ключами между пользователями. От пользователя требуется выбрать легко запоминающийся код доступа, который используется для шифрования криптографического ключа. Затем этот зашифрованный ключ может быть сохранен на жестком диске компьютера. Чтобы получить криптографический ключ, пользователю нужно ввести пароль, который затем будет использован для расшифровки ключа. [9, 10]

Есть разные применяемые методы для защиты ключа с помощью биометрии, например – удаленное сопоставление шаблонов и хранение ключей. Его проверяют путем захвата биометрического изображения и сравнивают с шаблоном, проверяется верификация пользователя – следовательно ключ высвобождается из безопасного хранилища. Данный метод удобен, так как не нужно запоминать свой пароль, и он отлично подходит для приложений физического доступа, в котором ключи, шаблоны хранятся в безопасном месте, т.к. отделены от устройства захвата изображения. При данном методе необходимо обеспечить защиту линий связи от подслушивающих устройств. Минусом является то, что при использовании данного метода на персональном компьютере, ключи чаще всего хранятся в открытом виде на жестком диске и это составляет опасность.

Следующий метод состоит в сокрытии криптографического ключа в самом шаблоне регистрации с помощью доверенного (секретного) алгоритма замены битов. Работа состоит в том, что после прохождения аутентификации данный алгоритм будет извлекать биты ключа из определенных мест и вставлять данный ключ в систему. Так как данный криптографический ключ всегда будет извлекаться из одного и того же местоположения при каждой аутентификации другого пользователя, следовательно, атакуемый сможет легко определить биты и их расположение, которые и определяют данный ключ, что даст возможность восстановить встроенный ключ из любого шаблона других пользователей системы.

Третий же метод использует данные, которые были получены из биометрического изображения, т.е. это биометрический шаблон, который используется в качестве криптографического ключа. Работа заключается в следующем, после регистрации процесс биометрического шифрования объединяет биометрическое изображение с цифровым ключом для создания защищенного блока данных (Bioscrypt), где цифровой ключ используется как криптографический ключ. Т.е. идет проверка биометрического шифрования, где извлекается криптографический ключ, объединяющий биоскрипт и биометрическое изображение. Т.е. процесс дает некраткие ответы при биометическом шифровании – да или нет, а помогает легко получить выпуск ключа, путем извлечения его и воссоздания путем объединения Bioscrypt и биометрического изображения.

Аппаратные токены. Аппаратный аутентификатор – устройство, которое владелец носит с собой для получения разрешения на доступ к каким-либо сетевым ресурсам. Физические токены обеспечивают фактор владения для многофакторной аутентификации, улучшенной для банков и поставщиков приложений, которым необходимо защитить несколько приложений на одном устройстве, путем аутентификации с помощью одноразовых кодов [2]. Каждый токен имеет уникальный секретный криптографический ключ, хранящийся внутри него, используемый для

установления личности токена посредством «рукопожатия» (запрос-ответ). Сторона, устанавливающая аутентификацию, отправляет запрос, ответ на который вычисляется с использованием секретного ключа. Иногда вызов неявно принимается за текущее время. Секретный ключ никогда не должен покидать токен. Попытки взломать токен, чтобы восстановить ключ, должны привести к уничтожению ключа. Аутентификация пользователя по токену может быть основана на паролях в виде PIN-кода (личного идентификационного номера). С технической позиции лучшей комбинацией есть биометрическая аутентификация пользователей по токену с дальнейшей взаимной криптографической аутентификацией между системными службами и токеном.

Аутентификация на основе токенов сегодня является технической реальностью, но ей все еще не хватает значительного проникновения на рынок. Многие существующие системы используют настольную рабочую станцию в качестве «токена» для аутентификации с остальной частью сети. Криптографический ключ вычисляется рабочей станцией на основе пароля пользователя, на основе которой рабочая станция аутентифицирует в сети.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ И ИХ ОБСУЖДЕНИЕ

На сегодняшний день роль цифровизации очень значительна и она большими темпами проникает во все направления современного общества. С постепенным исчезновением традиционного способа ведения бизнеса в реальном пространстве и соответствующим увеличением числа предприятий в киберпространстве наблюдается увеличение частоты, с которой пользователи должны идентифицировать себя онлайн. К сожалению, это также привело к соответствующему увеличению случаев киберпреступности, что создает проблему для уровней безопасности систем управления идентификацией.

По данным Positive Technologies в первом квартале 2022 года атаки направленные на частных лиц учетные данные достигли 46% случаев относящихся к общему объему похищенной информации; во втором с помощью постоянных атак на различные веб-ресурсы данные возросли до 22%, что в предыдущем квартале составляло 13%. За счет проведенных атак с помощью компроментации и подбоа учетных данных на веб-ресурсах, соц.сетях и аккаунтах копаний [14].

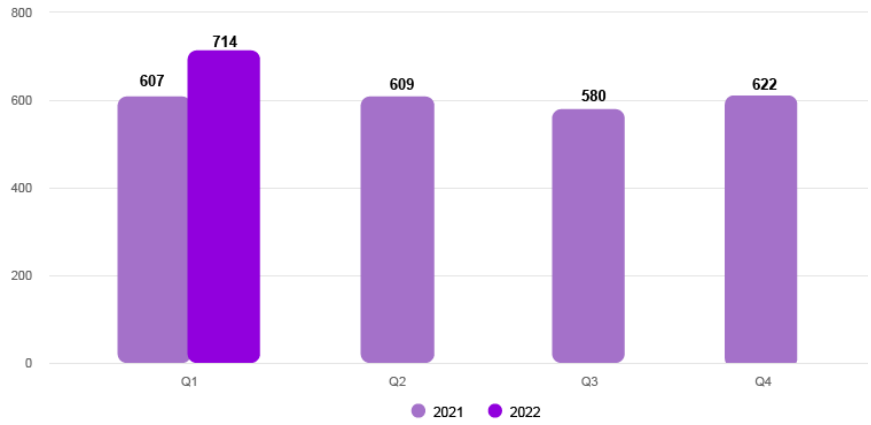

Рис. 2. Количество атак в 2021 и 2022 годах (по кварталам)
Fig. 2. Number of attacks in 2021 and 2022 (quarterly)

Следовательно необходимы надежные и безопасные системы управления идентификацией, которые контролируют все механизмы аутентификации, авторизации и аудита идентификационных данных пользователя – аутентификация является одним из таких ключевых средств обеспечения безопасности и применяется все чаще, наприме пи управлении правами доступа, коммуникациями, онлайн-платежами.

Был проведен опрос среди студентов и преподавателей нашего университета, и приведена статистика - из 200 опрошенных студентов и преподавателей, 70% пользуются многофакторной аутентификации для получения доступа к интернет-ресурсам (рис. 3). Опрос также показал, что только 5% опрошенных, использующих MFA, подвергались краже учетных данных (рис. 4), в то же время среди опрошенных, не использующих MFA карже данных подвергались 20% (рис. 5).

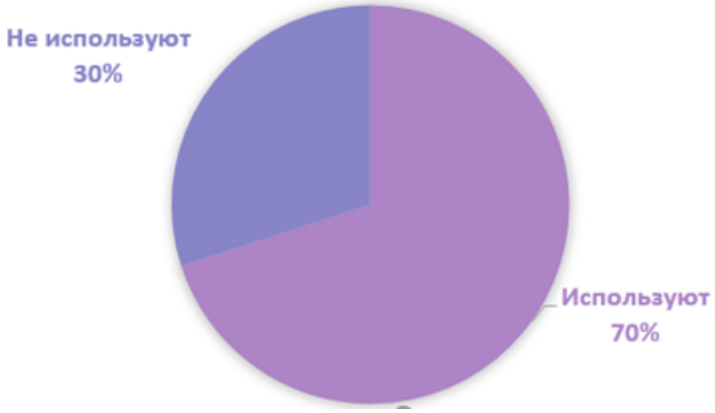

Рис. 3. Использование MFA
Fig. 3. Using MFA

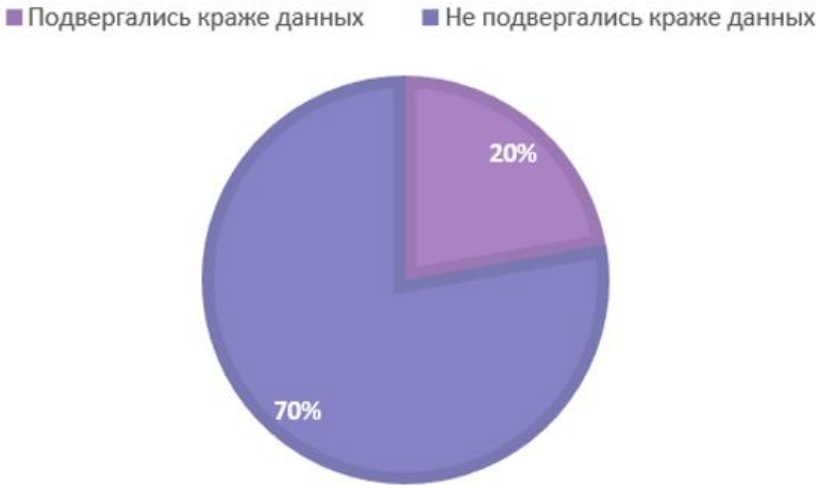

Рис. 4. Подвержение учетных данных при использовании MFA
Fig. 4. Credential verification when using MFA

Рис. 5. Подвержение учетных данных не изспользующих MFA
Fig. 5. Credential verification for non-MFA users

Таким образом, использование многофакторной аутентификации уложняет злоумышленникам реализацию атаки, тем самым снижается риск потери данных.

ЗАКЛЮЧЕНИЕ

Применение и значение аутентификации с каждым днем ростем, так как в мире цифровых технологий пользователи все больше начинают отдавать приоритеты своим биометрическим данным относящимся к авторизации как дополнительный метод защиты при использовании парольной защиты от различных атак и несанкционированных действий. MFA дает пользователям простоту, защиту и большую безопасность при доступе к своим аккаунтам, своим конфиденциальным данным, исключая риски утечки и кражи информации. Многофакторная аутертификация является не стандатизиованной и ее реализация может иметь различные формы, проблема лишь состоит в способности взаимодействия. При выборе, разработке, тестировании, внидрении, обслуживании системы управления полной идентификацией безопасности необходимо обращать тщательное внимание на различные аспекты, процессы и механизмы аутентификации непоседственно связанными с этим технологиями. В данной статье были рассмотрены и проанализированы различные способы возможно реализации многофакторной аутентификации и ее помощь в защите информации пользователей, которая уже есть неотъемлимой частью жизни любого человека. Данная технология имеет большое количество плюсов и конечно тебует еще большего внимания и развития для еще большего увеличения безопасности пользователя в информационной пространстве.

Список литературы

1. Kaspersky Lab has calculated how many times hackers have tried to steal passwords from Russians. URL: https://clck.ru/32kJ6s.
2. What is Multi-factor Authentication (MFA)? URL: https://clck.ru/32kJ8w.
3. Кузьминых Е.С., Маслова М.А. Анализ и сравнение биометрических способов идентификации личности человека // Научный результат. Информационные технологии. – 2021. – Т. 6. – № 4. – С. 13-19.
4. Девицына С.Н., Елецкая Т.А., Балабанова Т.Н., Гахова Н.Н. Разработка интеллектуальной системы биометрической идентификации пользователя // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2019. Т. 46. № 1. С. 148-160.
5. Fedotov A.S. Basic principles of implementing multi-factor authentication // 67th Scientific and Technical Conference of students, undergraduates and undergraduates, April 18-23, Minsk: collection of scientific papers: at 4 h. h. 4.
6. Маслова М.А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. – 2019. – Т. 4. – № 1. – С. 31-37.
7. Troshkov A.M., Kondrashov A.V., Kondrashov Yu. V., Khlobystin N. S., Krylova L. A. Biometric characteristics of identity authentication and their protection system // Questions of defense technology. Series 16: Technical means of countering terrorism. Founders: Scientific and Production Association of Special Materials, FSUE "Scientific and Technical Center "Informtechnika" ISSN: 2306-1456.
8. 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.
9. Bardaev S.E. Multifactorial biometric threshold cryptosystem // Izvestiya SFU. Technical sciences. Founders: Southern Federal University ISSN: 1999-9429eISSN: 2311-3103
10. Devitsyna S., Eletskaya T., Meshkov A.V. Developing facial recognition software to control access to campus facilities sbornike: CEUR Workshop Proceedings. 2. Ser. "InnoCSE 2019 – Proceedings of the 2nd Workshop on Innovative Approaches in Computer Science within Higher Education" 2019. P. 68-76.
11. Krotov A.V., Kutuzov A.V. Application of multi-factor authentication in order to protect EUT funds from unauthorized access // Modern scientific research and innovation. 2021. № 3.
12. Bogdanov D.S., Klyuev S.G. Classification and comparative analysis of multifactor authentication technologies in web applications // Modeling, optimization and information technology. Founders: Voronezh Institute of High Technologies eISSN: 2310-6018
13. Types Of Biometrics: A Complete Guide. URL: https://clck.ru/32knZ3.
14. Current cyber threats: The first quarter of 2022. URL: https://clck.ru/32BQoD

15. Маслова М.А. , Костиков В.А. Использование системы голосовой идентификации в качестве дополнительной защиты пользователя // Современные проблемы радиоэлектроники и телекоммуникаций. – 2021. – № 4. – С. 223.

References

1. Kaspersky Lab has calculated how many times hackers have tried to steal passwords from Russians. URL: https://clck.ru/32kJ6s.
2. What is Multi-factor Authentication (MFA)? URL: https://clck.ru/32kJ8w.
3. Kuzminykh E.S., Maslova M.A. Analysis and comparison of biometric methods for identifying a person // Research result. Information technology. – 2021. – T. 6. – № 4. – P. 13-19.
4. Devitsyna S.N., Eletskaya T.A., Balabanova T.N., Gakhova N.N The development of intelligent biometric identification system user // Belgorod State University Scientific Bulletin. Economics. Information technologies. 2019. T. 46. № 1. P. 148-160.
5. Fedotov A.S. Basic principles of implementing multi-factor authentication // 67th Scientific and Technical Conference of students, undergraduates and undergraduates, April 18-23, Minsk: collection of scientific papers: at 4 h. h. 4.
6. Maslova M.A. Analysis and determination of information security risks // Research result. Information technology. – 2019. – T. 4. – № 1. – P. 31-37.
7. Troshkov A.M., Kondrashov A.V., Kondrashov Yu.V., Khlobystin N.S., Krylova L.A. Biometric characteristics of identity authentication and their protection system // Questions of defense technology. Series 16: Technical means of countering terrorism. Founders: Scientific and Production Association of Special Materials, FSUE "Scientific and Technical Center "Informtechnika" ISSN: 2306-1456.
8. Gerasimov V.M., Maslova M.A. Possible threats and attacks on the user voice identification system // Research result. Information technology. – 2022. – T. 7. – № 1. – P. 32-37.
9. Bardaev S.E. Multifactorial biometric threshold cryptosystem // Izvestiya SFU. Technical sciences. Founders: Southern Federal University ISSN: 1999-9429eISSN: 2311-3103.
10. Devitsyna S., Eletskaya T., Meshkov A.V. Developing facial recognition software to control access to campus facilities sbornike: CEUR Workshop Proceedings. 2. Ser. "InnoCSE 2019 – Proceedings of the 2nd Workshop on Innovative Approaches in Computer Science within Higher Education" 2019. P. 68-76.
11. Krotov A.V., Kutuzov A.V. Application of multi-factor authentication in order to protect EUT funds from unauthorized access // Modern scientific research and innovation. 2021. № 3.
12. Bogdanov D.S., Klyuev S.G. Classification and comparative analysis of multifactor authentication technologies in web applications // Modeling, optimization and information technology. Founders: Voronezh Institute of High Technologies eISSN: 2310-6018
13. Types Of Biometrics: A Complete Guide. URL: https://clck.ru/32knZ3.
14. Current cyber threats: The first quarter of 2022. URL: https://clck.ru/32BQoD
15. Maslova M.A., Kostikov V.A. Using the voice identification system as an additional user protection // Modern problems of radio electronics and telecommunications. – 2021. – № 4. – P. 223.

Надейкина Виктория Сергеевна, студент третьего курса кафедры Информационная безопасность Института информационных технологий
Лагуткина Татьяна Владимировна, ассистент кафедры Информационная безопасность Института информационных технологий

Nadeikina Victoria Sergeevna, third-year student of the Department of Information Security of the Institute of Information Technologies
Lagutkina Tatyana Vladimirovna, Assistant of the Department of Information Security of the Institute of Information Technologies