ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СОВРЕМЕННЫХ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ В КОНТЕКСТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Калининский Даниил Сергеевич
Студент магистратуры
2 курс, факультет «Информационные технологии»
Кафедра «Сетевые информационные технологии и сервисы»
Московский технический университет связи и информатики
e-mail: daniilblag28@gmail.com

Аннотация

В рамках данного исследования представлен сравнительный анализ разнообразных методов аутентификации, широко применяемых в области кибербезопасности. В работе проводится детальное изучение преимуществ и недостатков основных подходов к аутентификации: электронной подписи, парольной аутентификации, аутентификации с использованием SMS, биометрической аутентификации, аутентификации на основе географического местоположения, многофакторной и адаптивной аутентификации. Анализ позволяет понять степень эффективности каждого из методов, основываясь на критериях безопасности, удобства использования и стоимости реализации. Исследование способствует пониманию сложностей и вызовов, связанных с процессом аутентификации, и может быть полезным для специалистов в области информационной безопасности при выборе подходящего метода аутентификации для конкретной системы или приложения.

Ключевые слова: аутентификация, кибербезопасность, электронная подпись, аутентификация по паролям, SMS аутентификация, биометрическая аутентификация, аутентификация через географическое местоположение, многофакторная аутентификация, адаптивная аутентификация.

COMPARATIVE ANALYSIS OF MODERN AUTHENTICATION MECHANISMS IN THE CONTEXT OF INFORMATION SECURITY

Daniil S. Kalininskiy
Master's degree student
2nd year, Faculty of Information Technology
Department of "Network Information Technologies and Services"
Moscow Technical University of Communications and Informatics

ABSTRACT

Within the framework of this study, a comparative analysis of various authentication methods widely used in the field of cybersecurity is presented. The paper provides a detailed study of the advantages and disadvantages of the main approaches to authentication: electronic signature, password authentication, SMS authentication, biometric authentication, location-based authentication, multi-factor and adaptive authentication. The analysis allows you to understand the degree of effectiveness of each of the methods, based on the criteria of security, ease of use and cost of implementation. The study contributes to the understanding of the complexities and challenges associated with the authentication process and may be useful for information security professionals in choosing the appropriate authentication method for a particular system or application.

Keywords: authentication, cybersecurity, electronic signature, password authentication, SMS authentication, biometric authentication, geographic location authentication, multi-factor authentication, adaptive authentication.

Введение

В свете постоянно растущих киберугроз, необходимость в надежной аутентификации пользователя становится все более важной. Методы аутентификации привлекают все больше внимания, поскольку они являются первым линией обороны в защите информационных систем. Данная статья рассматривает различные методы аутентификации, их преимущества и недостатки, с целью помочь специалистам в области кибербезопасности выбрать наиболее подходящие методы для их систем.

Подтверждение подлинности, или аутентификация, обозначает процедуру верификации идентификационных данных пользователя. Этот шаг критичен для обеспечения безопасности в различных системах, включая компьютерные, финансовые и другие. Существует множество методов аутентификации, которые могут быть классифицированы по разным признакам и основаны на различных факторах [1, 2].

Подтверждение подлинности с использованием электронной подписи

Один из методов подтверждения подлинности – использование электронной подписи (ЭП). Этот метод применяется для проверки идентичности документов, сообщений или электронных транзакций. Электронная подпись является цифровым эквивалентом ручной подписи, служащей для подтверждения авторства и сохранности документа [3].

При использовании ЭП применяется специальный ключ, который выдаётся после проверки пользователя сертифицирующим центром (СЦ). Данный ключ может быть представлен в виде смарт-карты, USB-устройства или храниться на сервере СЦ. В процессе создания ЭП, этот ключ применяется для создания уникального отпечатка, включающего информацию о документе и ключе. Данная подпись затем может быть подтверждена с помощью публичного ключа, который также предоставляется СЦ (рис. 1).

Рисунок 1. Аутентификация при помощи ЭП

Электронная подпись предоставляет высокий уровень безопасности и точности в процессе аутентификации, поскольку она служит цифровым эквивалентом ручной подписи пользователя. Этот подход активно применяется в различных сферах, включая электронную почту, онлайн-банкинг, электронные документы и транзакции в области электронной коммерции.

Тем не менее, использование электронной подписи в качестве метода аутентификации имеет свои недостатки. Это может быть сложнее и менее удобно для пользователей по сравнению с другими методами, такими как пароли. Для активации электронной подписи требуется доступ к устройству, на котором хранится соответствующий ключ. Это может быть неудобно при удаленной работе или использовании общедоступного компьютера. Кроме того, возможно, потребуются дополнительные затраты на получение и обновление электронной подписи [4].

Парольная аутентификация

Парольная аутентификация основана на использовании пользователем уникального секретного кода или фразы для подтверждения своей личности. Этот метод является наиболее общим и находит широкое применение во многих системах и приложениях (рис. 2) [5].

Для прохождения процедуры аутентификации пользователь вводит предварительно установленный или выданный системой пароль. Введенный пароль затем сравнивается с хранящимся в системе, и если они совпадают, пользователь считается аутентифицированным и получает доступ к защищенной информации или функционалу системы.

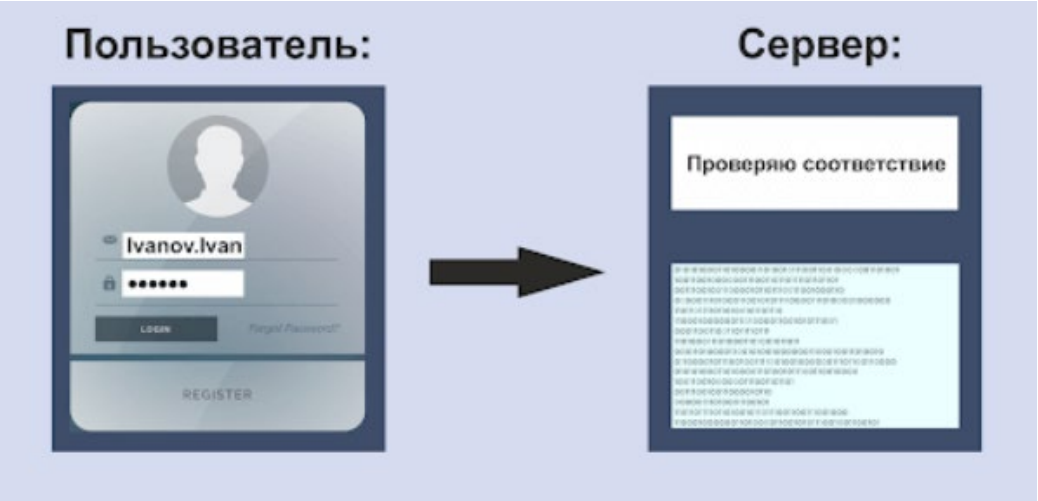

Рисунок 2. Парольная аутентификация

Преимуществами использования паролей в качестве средства аутентификации являются и их простота в использовании и удобство для конечного пользователя. В дополнение к этому, пользователь имеет возможность периодически менять пароль, что помогает обеспечить его надежность, если существует подозрение на компрометацию.

Тем не менее, аутентификация на основе паролей также имеет свои ограничения. Сложные для взлома пароли зачастую являются сложными для запоминания, что может влечь за собой необходимость их записи или использования одного пароля для нескольких систем, что, в свою очередь, увеличивает риск их утечки. К тому же, пароли могут стать добычей хакеров или быть взломаны при помощи подбора, что может привести к несанкционированному доступу к конфиденциальной информации [6].

Аутентификация посредством СМС

Аутентификация с применением СМС (Службы коротких сообщений) представляет собой процедуру подтверждения личности пользователя, основанную на использовании мобильного устройства и коротких текстовых сообщений [7]. При таком подходе пользователь предоставляет номер своего мобильного телефона и получает уникальный одноразовый код, который затем необходимо ввести на сайте или в приложении для завершения процедуры аутентификации (рис. 3).

Рисунок 3. Аутентификация с помощью СМС

Основным достоинством этой модели является ее простота и удобство для широкого круга пользователей, поскольку большинство людей обладают мобильными устройствами. Дополнительно, этот подход предоставляет высокий уровень безопасности, так как он требует физического доступа к мобильному устройству для получения кода подтверждения.

Вместе с тем, этот метод не лишен недостатков, поскольку он может быть подвержен атакам вроде кражи телефона или перехвата текстовых сообщений. Помимо этого, применение данного метода может сопровождаться рядом неудобств, таких как задержки при получении сообщения или проблемы с мобильной связью [8].

Биометрическая идентификация

Биометрическая аутентификация представляет собой процесс подтверждения идентичности пользователя путем анализа его биологических характеристик, таких как отпечатки пальцев, голос, лицо или сетчатку глаза [9]. В ходе этого процесса, пользователь представляет свои биометрические данные, которые затем сопоставляются с данными, предварительно сохраненными в базе. Если данные совпадают, пользователь получает доступ к системе. В противном случае, доступ отклоняется (рис. 4).

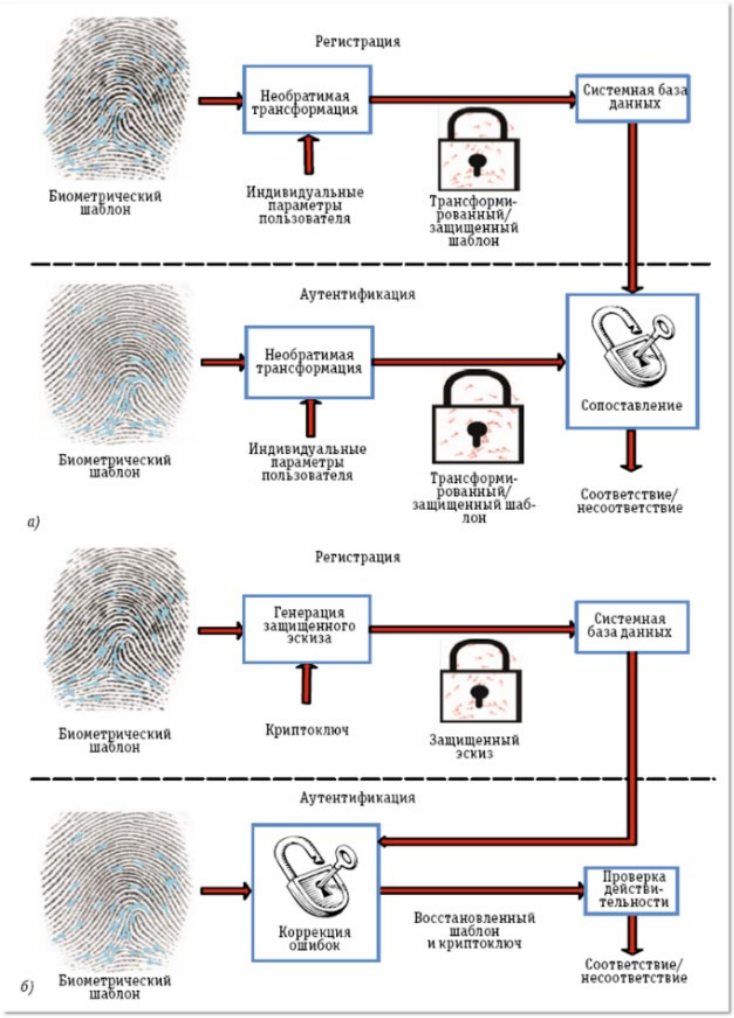

Рисунок 4. Биометрическая аутентификация

Аутентификация по биометрическим данным представляет собой более надежную и удобную альтернативу классическим методам аутентификации, таким как пароли или PIN-коды. Пользователи не в состоянии забыть свои биометрические данные, а их подделка или угадывание являются весьма затруднительными. Однако, как любая другая технология, биометрическая аутентификация имеет свои слабые стороны, включая высокую стоимость установки и настройки системы, возможность ошибок при распознавании биометрических данных и риск компрометации пользовательских данных при утечке информации из базы данных [10].

Геолокационная аутентификация

Геолокационная аутентификация основывается на определении местоположения устройства пользователя. Этот подход может применяться для подтверждения законности доступа пользователя к системе, исходя из его текущего местоположения [11].

При использовании этого метода применяется информация о местоположении, полученная через GPS, Wi-Fi или мобильные сети. При попытке входа в систему пользователь дает согласие на обработку своих геолокационных данных, которые затем сопоставляются с заранее установленными параметрами. Если местоположение пользователя соответствует установленным критериям, то он получает доступ к системе (рис. 5).

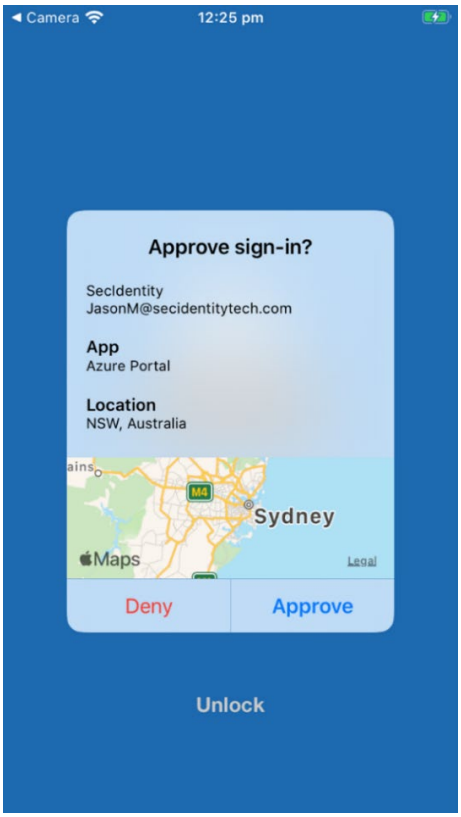

Рисунок 5. Аутентификация через географическое местоположение

Преимуществом этого метода является его простота и удобство, так как для аутентификации не требуется дополнительных устройств или специальных приложений [12]. Однако, этот метод не гарантирует высокого уровня безопасности, так как данные о геопозиции могут быть подделаны или изменены с помощью специальных инструментов. Кроме того, использование этого метода может быть ограничено в зависимости от настроек устройства и доступности геолокационных служб.

Многофакторная аутентификация

Многофакторная аутентификация – это метод аутентификации, который использует несколько различных типов проверки подлинности для повышения безопасности доступа к системам и данным. Он сочетает в себе два или более фактора аутентификации, такие как пароль, биометрические данные, смарт-карта, устройство для генерации одноразовых паролей и другие [13]. Каждый фактор проверяет подлинность пользователя на основе различных данных и поведенческих характеристик, что увеличивает уровень безопасности (рис. 6).

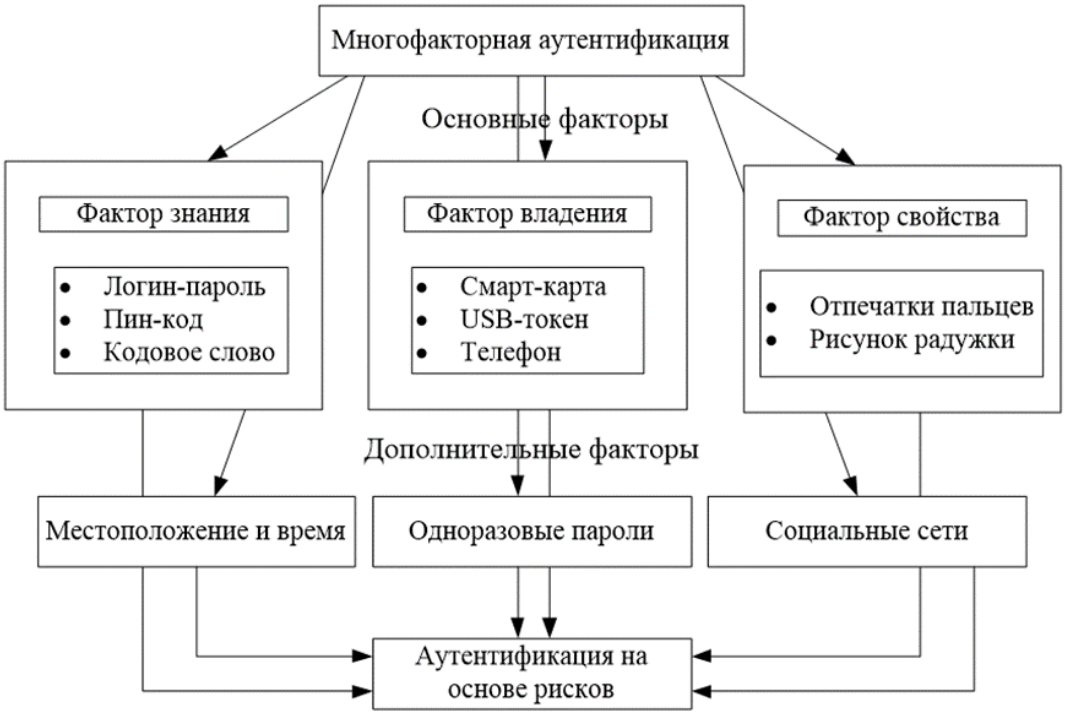

Рисунок 6. Многофакторная аутентификация

Многофакторная аутентификация предоставляет более надежную защиту, чем использование только одного фактора, такого как пароль. Если злоумышленник получит доступ к паролю, он все еще должен пройти через дополнительные факторы проверки подлинности, такие как ввод кода, использование биометрических данных или физическое присутствие пользователя. Это делает доступ к системе или данным намного сложнее для злоумышленников [14].

Однако многофакторная аутентификация может быть менее удобной для пользователей, так как она требует дополнительных шагов для входа в систему или получения доступа к данным. Кроме того, некоторые факторы аутентификации могут быть дорогими в реализации и управлении, такие как использование биометрических данных или смарт-карт.

Заключение

Аутентификация играет важную роль в кибербезопасности, предоставляя первую линию обороны против несанкционированного доступа. Как показано в этом обзоре, каждый метод аутентификации имеет свои сильные и слабые стороны, и выбор подхода зависит от конкретного контекста и требований безопасности. В то время как некоторые методы могут быть более подходящими для сценариев, требующих высокого уровня безопасности, другие могут быть более подходящими для ситуаций, когда удобство использования является приоритетом. В любом случае, важно поддерживать баланс между безопасностью и удобством, чтобы обеспечить защиту информационных систем, не нарушая при этом удобство пользователей.

Список литературы:

1. Калининский Д.С., Асначев И.А., Анисимов А.Р. Реализация защищенной офисной системы на основе криптографии. МЕЖДУНАРОДНЫЙ ЖУРНАЛ гуманитарных и естественных наук № 6-1 (69), июнь 2022 г. с. 141-146.

2. Калининский Д.С., Сурков В.Н., Горнаева Н.В. Разработка алгоритма защищенной офисной системы на основе криптографии. МЕЖДУНАРОДНЫЙ ЖУРНАЛ гуманитарных и естественных наук № 6-1 (69), июнь 2022 г. с. 147-149.
3. Иванов, А. Б., Смирнов, А. В. Организация безопасного офиса: проблемы и решения. Журнал "Информационная безопасность", № 3(25), 2019, с. 20-28.
4. Петров, И. Н., Сидорова, О. А. Анализ угроз информационной безопасности в офисных средах. Сборник трудов конференции "Информационная безопасность и защита информации", 2017, с. 123-135.
5. Петрова, Н. С. (2020). Анализ угроз информационной безопасности офисных сетей. Информационные технологии и безопасность, 8(2), 45-52.
6. Иванов, А. В., Смирнова, Е. П. (2018). Методы обнаружения и предотвращения утечки данных в офисных сетях. Информационная безопасность, 6(4), 17-24.
7. Кузнецов, В. А., Сидорова, М. И. (2019). Развитие систем контроля доступа в офисных помещениях. Научно-технический вестник информационных технологий, механики и оптики, 19(6), 78-84.
8. Смирнов, П. Н., Ковалева, О. А. (2017). Применение методов машинного обучения для обнаружения вторжений в офисные сети. Информационная безопасность и защита информации, 5(2), 33-40.
9. Антонов, А. В., Григорьев, В. П. (2018). Анализ уязвимостей офисных приложений и методы их защиты. Научно-технический вестник информационных технологий, механики и оптики, 18(4), 56-63.
10. Белов, В. С., Соловьева, Е. Г. (2019). Методы и средства обеспечения безопасности электронной почты в офисных сетях. Информационная безопасность и защита информации, 7(1), 21-28.
11. Гусев, А. В., Лебедева, Н. В. (2020). Проблемы и методы защиты информации в офисных мобильных приложениях. Информационные технологии и безопасность, 8(4), 60-68.
12. Соколов, В. М., Чернов, Д. А. (2018). Анализ методов шифрования данных в офисных сетях. Информационная безопасность, 6(2), 9-16.
13. Макарова, О. Н., Никитина, Е. А. (2019). Защита периметра офисных сетей: проблемы и решения. Информационная безопасность и защита информации, 7(3), 45-52.
14. Попов, А. С., Морозов, В. В. (2017). Применение технологии виртуализации для обеспечения безопасности офисных сетей. Научно-технический вестник информационных технологий, механики и оптики, 17(2), 30-37.

References:

1. Kalininsky D.S., Asnachev I.A., Anisimov A.R. Implementation of a secure office system based on cryptography. INTERNATIONAL JOURNAL OF THE HUMANITIES AND SCIENCES No. 6-1 (69), June 2022 p. 141-146.
2. Kalininsky D.S., Surkov V.N., Gornaeva N.V. Development of an algorithm for a secure office system based on cryptography. INTERNATIONAL JOURNAL OF THE HUMANITIES AND SCIENCES No. 6-1 (69), June 2022 p. 147-149.

3. Ivanov, A. B., Smirnov, A. V. Organization of a safe office: problems and solutions. Journal "Information Security", No. 3(25), 2019, p. 20-28.
4. Petrov, I. N., Sidorova, O. A. Analysis of threats to information security in office environments. Collection of proceedings of the conference "Information security and information protection", 2017, p. 123-135.
5. Petrova, N. S. (2020). Analysis of threats to information security of office networks. Information Technology and Security, 8(2), 45-52.
6. Ivanov, A. V., Smirnova, E. P. (2018). Methods for detecting and preventing data leakage in office networks. Information Security, 6(4), 17-24.
7. Kuznetsov, V. A., Sidorova, M. I. (2019). Development of access control systems in office premises. Scientific and technical bulletin of information technologies, mechanics and optics, 19(6), 78-84.
8. Smirnov, P. N., Kovaleva, O. A. (2017). Application of machine learning methods for intrusion detection in office networks. Information Security and Information Protection, 5(2), 33-40.
9. Antonov, A. V., Grigoriev, V. P. (2018). Vulnerability analysis of office applications and methods of their protection. Scientific and technical bulletin of information technologies, mechanics and optics, 18(4), 56-63.
10. Belov, V. S., Solovieva, E. G. (2019). Methods and means of ensuring the security of e-mail in office networks. Information Security and Information Protection, 7(1), 21-28.
11. Gusev, A. V., Lebedeva, N. V. (2020). Problems and methods of information protection in office mobile applications. Information Technology and Security, 8(4), 60-68.
12. Sokolov, V. M., Chernov, D. A. (2018). Analysis of data encryption methods in office networks. Information Security, 6(2), 9-16.
13. Makarova, O. N., Nikitina, E. A. (2019). Protecting the perimeter of office networks: problems and solutions. Information Security and Information Protection, 7(3), 45-52.
14. Popov, A. S., Morozov, V. V. (2017). Application of virtualization technology to ensure the security of office networks. Scientific and technical bulletin of information technologies, mechanics and optics, 17(2), 30-37.