УДК 004 **Информационные технологии**

Юрченко Кирилл Иванович, *студент,*
ФГБОУ ВО Донской государственный технический университет

УСИЛЕНИЕ КОНТРОЛЯ ДОСТУПА В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Аннотация: В мире, который становится все более цифровым, где информация является ценным активом, защита доступа к конфиденциальным данным и системам имеет первостепенное значение. Традиционные методы однофакторной аутентификации, такие как пароли, оказались уязвимыми для кибератак, таких как фишинг, атаки методом перебора и подбор пароля. Многофакторная аутентификация (MFA) стала мощным решением для улучшения контроля доступа и защиты информационных систем от несанкционированного доступа. В статье рассматривается значение многофакторной аутентификации, ее принципы, преимущества и ее роль в усилении контроля доступа в информационных системах.

Ключевые слова: аутентификация, двухфакторная аутентификация, многофакторная аутентификация, информационная безопасность.

Annotation: In an increasingly digital world where information is a valuable asset, protecting access to sensitive data and systems is paramount. Traditional single-factor authentication methods such as passwords have proven vulnerable to cyberattacks such as phishing, brute-force attacks, and password guessing. Multi-factor authentication (MFA) has become a powerful solution for improving access control and protecting information systems from unauthorized access. The article discusses the importance of multi-factor authentication, its principles, advantages and its role in strengthening access control in information systems.

Keywords: authentication, two-factor authentication, multi-factor

authentication, information security.

Понимание многофакторной аутентификации

Многофакторная аутентификация, также известная как двухфакторная аутентификация (2FA) или многоступенчатая верификация, представляет собой механизм безопасности, который требует от пользователей предоставления двух или более форм идентификации перед получением доступа к системе, приложению или данным. Эти факторы обычно делятся на три категории [1]:

1. Фактор знаний: что-то, что известно пользователю, например пароль, PIN-код или ответ на секретный вопрос.

2. Фактор владения: что-то, чем владеет пользователь, например смартфон, токен безопасности или смарт-карта.

3. Фактор принадлежности: что-то присущее пользователю, например отпечатки пальцев, распознавание голоса или черты лица.

Фундаментальный принцип, лежащий в основе MFA, заключается в создании уровней безопасности, значительно затрудняющих взлом системы неавторизованными лицами, даже если им удастся скомпрометировать один фактор [2].

Преимущества многофакторной аутентификации

1. Повышенная безопасность: Сочетая множество факторов, MFA значительно усиливает контроль доступа. Даже если один фактор будет скомпрометирован, злоумышленнику все равно потребуется обойти дополнительные уровни аутентификации, что сделает несанкционированный доступ чрезвычайно сложным.

2. Снижение рисков, связанных с паролями: Слабые или повторно используемые пароли являются распространенной уязвимостью, используемой злоумышленниками. MFA снижает эти риски, добавляя дополнительный уровень безопасности помимо паролей, снижая шансы на успешные кибератаки.

3. Защита от фишинга: Фишинговые атаки часто заставляют пользователей обманом раскрывать свои пароли. MFA добавляет дополнительный уровень

защиты, затрудняя злоумышленникам получение доступа, даже если они получат пароль пользователя.

4. Соответствие нормативным требованиям: Во многих отраслях промышленности действуют строгие правила защиты данных. Внедрение MFA помогает организациям соответствовать требованиям соответствия и обеспечивает конфиденциальность и целостность конфиденциальной информации.

5. Удобство в использовании: Современные решения MFA предлагают удобный интерфейс, часто легко интегрируясь со смартфонами и другими персональными устройствами. Это удобство поощряет пользователей к принятию мер безопасности и сотрудничеству с ними [3].

Роль многофакторной аутентификации в усилении контроля доступа

1. Аутентификация пользователя: MFA обеспечивает надежную аутентификацию пользователя, гарантируя, что только авторизованные лица могут получить доступ к конфиденциальным системам и данным. Это снижает риск несанкционированного доступа из-за украденных, слабых или просочившихся паролей.

2. Удаленный доступ: С ростом популярности удаленной работы и облачных сервисов потребность в безопасном удаленном доступе становится первостепенной. MFA обеспечивает надлежащую защиту удаленных подключений, снижая риск несанкционированного доступа из внешних источников.

3. Привилегированные учетные записи: Во многих организациях привилегированные учетные записи имеют доступ к критически важным системам и данным. Внедрение MFA для привилегированных учетных записей добавляет дополнительный уровень защиты, снижая риск несанкционированного доступа и потенциальной утечки данных.

4. Двусторонняя проверка: MFA не только улучшает контроль доступа для пользователей, пытающихся получить доступ к системе, но и защищает систему от потенциальных атак злоумышленников, пытающихся получить

несанкционированный доступ.

5. Непрерывный мониторинг: Некоторые передовые решения MFA включают поведенческий анализ и мониторинг в режиме реального времени, которые могут обнаруживать аномалии и потенциальные нарушения безопасности. Это позволяет упреждающе реагировать на инциденты безопасности [4, 5].

Вывод

В заключение следует отметить, что многофакторная аутентификация является жизненно важным инструментом усиления контроля доступа в информационных системах. Комбинируя несколько факторов аутентификации, MFA повышает безопасность, снижает риски, связанные с использованием паролей, и защищает от фишинговых атак. Его внедрение не только обеспечивает соблюдение правил защиты данных, но и обеспечивает удобство работы с пользователями. Поскольку киберугрозы продолжают развиваться, MFA остается важным компонентом комплексной стратегии безопасности, защищая конфиденциальные данные, системы и ресурсы от несанкционированного доступа и потенциальных кибератак. Внедрение многофакторной аутентификации — это упреждающий шаг на пути к созданию устойчивой и безопасной цифровой среды как для организаций, так и для частных лиц.

Библиографический список:

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.