Список использованных источников

1. Иванов, Д. Управление глобальной цепочкой поставок и операциями / Д. Иванов, А. Ципуланидис, Й. Шёпбергер. – М. : Springer, 2019. – 250 с.
2. Tapscott, D. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World / D. Tapscott, A. Tapscott. – Penguin, 2016. – 348 p.
3. Кшетри, Н. Роль блокчейна в достижении ключевых целей управления цепочками поставок / Н. Кшетри // Международный журнал управления информацией. – 2018. – Т. 39. – С. 80–89.
4. Androulaki E. et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains // Proceedings of the Thirteenth EuroSys Conference. – 2018.
5. Чебакова, В.М. Цифровая трансформация логистики как фактор устойчивого экономического развития / В.М. Чебакова // Вестник ОмГТУ. – 2024. – № 3. – С. 45–52.

УДК 004.9

А. Шатеков, Е.А. Спирина
Карагандинский национальный исследовательский университет имени академика Е.А. Букетова
Караганда, Казахстан

ИНТЕГРАЦИЯ ТЕХНОЛОГИЙ АУТЕНТИФИКАЦИИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМАХ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Аннотация. *Современные цифровые технологии являются основой развития электронной коммерции. Безопасность персональных данных становится ключевым фактором доверия пользователей. В статье рассматриваются подходы к реализации многофакторной аутентификации (MFA) как средства защиты данных в e-commerce. Внедрение MFA способствует повышению уровня цифровой безопасности и устойчивости онлайн-бизнеса.*

A. Shatekov, Ye.A. Spirina
Buketov Karaganda National Research University
Karaganda, Kazakhstan

INTEGRATION OF AUTHENTICATION TECHNOLOGIES AND PERSONAL DATA PROTECTION IN E-COMMERCE SYSTEMS

Abstract. *Modern digital technologies are the basis for the development of e-commerce. The security of personal data is becoming a key factor in user trust. The article discusses approaches to implementing multi-factor authentication (MFA) as a means of data protection in e-commerce. The implementation of MFA contributes to increasing the level of digital security and sustainability of online businesses.*

Бурное развитие электронной коммерции в последние годы стало одним из ключевых направлений цифровой трансформации экономики. Рост онлайн-платежей, сервисов и маркетплейсов сопровождается увеличением объёмов персональных данных, что делает сектор e-commerce одной из наиболее уязвимых областей с точки зрения киберугроз. Потери от утечек информации и компрометации аккаунтов наносят не только экономический, но и репутационный ущерб компаниям. В этой связи разработка надёжных систем аутентификации приобретает особую значимость.

Одним из наиболее эффективных направлений в повышении безопасности является многофакторная аутентификация (MFA) — технология, основанная на проверке нескольких независимых факторов: знания (пароль, PIN-код), владения (устройство, токен, мобильное приложение) и присущих характеристик (биометрия). Такой подход существенно снижает вероятность несанкционированного доступа, даже при компрометации одного из факторов.

Как отмечается в исследовании Надейкиной В.С. и Лагуткиной Т.В. [1], многофакторная аутентификация позволяет значительно повысить уровень защиты пользователей и минимизировать риски атак, связанных с кражей учётных данных. Однако при её внедрении важно учитывать удобство использования: чрезмерно сложные схемы могут негативно сказаться на пользовательском опыте, что особенно критично для онлайн-платформ.

В работе [2] подробно проанализированы различные способы реализации MFA, включая методы на основе одноразовых паролей (OTP), push-уведомлений и биометрической идентификации. Подчёркивается, что комбинирование факторов аутентификации должно осуществляться в зависимости от контекста доступа и уровня риска. Подобный адаптивный подход согласуется с современными тенденциями, изложенными в рекомендациях Национального института стандартов и технологий (NIST) [3].

Исследование Henricks, A. и Kettani, H. [4] показало, что применение многофакторных механизмов в архитектуре web-сервисов требует переработки логики взаимодействия между клиентом и сервером, а также внедрения безопасных протоколов обмена данными. В этой связи особое значение приобретает стандартизация механизмов обмена токенами (OAuth 2.0, OpenID Connect) и шифрования (TLS 1.3, AES-256).

На практике архитектура безопасной e-commerce-платформы с MFA строится на трёхуровневом взаимодействии. Клиентская часть обеспечивает удобный интерфейс и сбор факторов аутентификации, серверная часть — верификацию данных и управление сессиями, а модуль безопасности — хранение ключей, токенизацию и мониторинг рисков. Такой подход соответствует рекомендациям проекта NIST NCCoE Multifactor Authentication for E-Commerce [3], где отмечено, что многофакторная аутентификация должна стать обязательным элементом цифровых экосистем, особенно в сферах, связанных с финансовыми операциями.

Особое внимание в современных исследованиях уделяется вопросам защиты персональных данных. В работе Safin, R., Abdiraman, A., Nurusheva, A., и Aldasheva, L. [5] подчёркивается необходимость применения криптографических методов и токенизации при передаче данных, а также принципов «privacy by design» и «security by default». Эти подходы позволяют снизить вероятность утечки информации при обработке пользовательских данных внутри распределённых систем.

Опыт реализации MFA в приложениях электронной коммерции показывает, что внедрение таких систем положительно влияет не только на уровень безопасности, но и на экономические показатели компаний. Согласно исследованию NIST [3], использование MFA сокращает количество мошеннических операций и повышает доверие пользователей, что ведёт к росту объёмов транзакций. Для развивающихся цифровых экономик, включая Казахстан, подобные технологии становятся важным фактором повышения конкурентоспособности предприятий и ускорения цифровой трансформации.

Таким образом, интеграция технологий многофакторной аутентификации в инфраструктуру электронной коммерции обеспечивает комплексную защиту персональных данных и способствует формированию доверенной цифровой среды. MFA выступает не только инструментом информационной безопасности, но и драйвером технологического развития: внедрение подобных решений

стимулирует создание новых сервисов, развитие отечественных ИКТ-платформ и повышение цифровой зрелости бизнеса.

Многофакторная аутентификация является эффективным средством защиты данных и ключевым элементом цифровой экосистемы. Её внедрение в e-commerce-приложениях способствует снижению киберугроз, росту доверия пользователей и повышению устойчивости цифровой экономики. Использование международных стандартов (NIST, ISO), адаптивных моделей и технологий искусственного интеллекта открывает перспективы для дальнейшего развития безопасных и удобных цифровых сервисов.

Список использованных источников

1. Надейкина В.С., Лагуткина Т.В. Анализ способов реализации системы многофакторной аутентификации// Научный результат. Информационные технологии. - 2022. - №4. URL: https://cyberleninka.ru/article/n/analiz-sposobov-realizatsii-sistemy-mnogofaktornoy-autentifikatsii (дата обращения: 04.11.2025).

2. Абселямов А.А., Лагуткина Т.В. Исследование методов аутентификации на веб-сервисах. текущие тенденции и перспективы развития // Научный результат. Информационные технологии. 2024. №2. URL: https://cyberleninka.ru/article/n/issledovanie-metodov-autentifikatsii-na-veb-servisah-tekuschie-tendentsii-i-perspektivy-razvitiya (дата обращения: 04.11.2025).

3. Multifactor Authentication for E-Commerce. – NIST National Cybersecurity Center of Excellence (NCCoE). https://www.nccoe.nist.gov/multifactor-authentication-e-commerce

4. Henricks, A., & Kettani, H. (2019). On data protection using multi-factor authentication. Proceedings of the International Conference on Information System and System Management (ISSM), Rabat, Morocco. New York, NY: ACM. https://doi.org/10.1145/3394788.3394789

5. Safin, R., Abdiraman, A., Nurusheva, A., & Aldasheva, L. (2022). Comparison of information security methods of information-communication infrastructure: Multi-Factor Authentication. *Bulletin of L.N. Gumilyov Eurasian National University Technical Science and Technology Series*, *140*(3), 114–124. https://doi.org/10.32523/2616-7263-2022-140-3-114-124