

ЭЛЕКТРОННАЯ КОММЕРЦИЯ И КИБЕРБЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ

Белалова Гузаль Анваровна

Доцент кафедры «Искусственный интеллект»
Ташкентского Государственного экономического
университета

Дилмуродов Журабек Улугбек угли

Студент Ташкентского государственного экономического
университета dilmurodovjurabekk@gmail.com



Аннотация В эпоху стремительной цифровизации электронная коммерция становится неотъемлемым элементом глобальной экономики. Вместе с тем растёт значимость обеспечения кибер-безопасности, поскольку участники онлайн-транзакций всё чаще сталкиваются с угрозами утечки данных, фишинга и вредоносного программного обеспечения. В статье рассмотрены современные вызовы и тенденции в сфере кибер-безопасности электронной коммерции, а также предложены рекомендации по повышению устойчивости цифровых платформ к кибер-угрозам. Особое внимание уделено правовым аспектам и международным стандартам в сфере кибер-безопасности.

Ключевые слова: электронная коммерция, кибер-безопасность, цифровая трансформация, онлайн-платформа, кибер-угроза, информационная защита, цифровая идентификация

Abstract In the era of rapid digitalization, e-commerce is becoming an integral part of the global economy. At the same time, the importance of ensuring cyber-security is growing, as participants in online-transactions increasingly face threats such as data leaks, phishing, and malware. This article examines current challenges and trends in the field of cyber-security in e-commerce and provides recommendations for increasing the resilience of digital platforms to cyber-threats. Particular attention is paid to legal aspects and international standards in the field of cyber-security.

Keywords: e-commerce, cyber-security, digital-transformation, online-platform, cyber-threat, information-protection, digital-identification

Annotatsiya Raqamli-transformatsiya davrida elektron-kommersiya global iqtisodiyotning ajralmas qismiga aylanmoqda. Shu bilan birga, kiber-xavfsizlikni ta'minlash masalasi tobora dolzarb bo'lib bormoqda, chunki onlayn-transaksiyalarda ishtirok etuvchi subyektlar axborot-oqimi, fishing va zararli dasturlar bilan bog'liq tahdidlar bilan tez-tez duch kelmoqda. Mazkur maqolada elektron-kommersiya sohasida kiber-xavfsizlik bilan bog'liq zamonaviy muammolar va tendensiyalar tahlil qilinadi hamda raqamli-platfomalarning kiber-tahdidlarga nisbatan barqarorligini oshirish bo'yicha tavsiyalar beriladi. Kiber-xavfsizlik sohasidagi huquqiy-me'yoriy jihatlar va xalqaro standartlarga alohida e'tibor qaratiladi.

Kalit so'zlar: elektron-kommersiya, kiber-xavfsizlik, raqamli-transformatsiya, onlayn-platforma, kiber-tahdid, axborot-himoya, raqamli-identifikatsiya

Введение

В условиях глобализации и цифровой трансформации электронная коммерция стала одним из стратегических направлений развития экономики. В последние годы в Узбекистане наблюдается стремительное развитие электронных платежей, онлайн-сервисов и цифровых торговых платформ. Однако наряду с этим процессом возрастает и количество кибер-угроз.

В рамках стратегической программы «Цифровой Узбекистан – 2030», выдвинутой Президентом Ш.М. Мирзиёевым, определены важные задачи по укреплению инфраструктуры электронной коммерции, созданию безопасных онлайн-сервисов и обеспечению информационной безопасности.

В данном тезисе на основе исследований узбекских учёных рассматриваются проблемы кибер-безопасности в системе электронной коммерции Узбекистана, а также пути их устранения.

Обзор литературы

Вопросы развития электронной коммерции и обеспечения кибер-безопасности в Узбекистане на сегодняшний день становятся всё более актуальными на фоне ускоряющейся цифровой трансформации. Учитывая возрастающий интерес научного сообщества к данным направлениям, следует отметить, что узбекские исследователи внесли существенный вклад в формирование методологических и прикладных основ данной тематики.

Так, в исследовании Ш.Н. Нарзуллаева (2022) подробно рассмотрены институциональные аспекты обеспечения кибер-безопасности в условиях развития информационно-коммуникационных технологий (ИКТ). Учёный подчёркивает, что создание эффективной системы защиты данных требует не только внедрения передовых технических решений, но и формирования чётких организационно-правовых механизмов на уровне государственных институтов. Нарзуллаев также делает акцент на важности межведомственной координации и формировании нормативно-правовой базы, соответствующей международным стандартам кибер-безопасности.

Р. Гуломов (2021) анализирует роль электронной коммерции в структуре цифровой экономики и указывает на существующие риски и уязвимости, связанные с цифровыми транзакциями и онлайн-сервисами. В своей работе он рассматривает такие угрозы, как фишинг, утечка персональных данных и несанкционированный доступ к аккаунтам пользователей. Учёный делает вывод о необходимости разработки национальной стратегии по кибер-безопасности, в том числе через государственно-частное партнёрство в сфере цифровых платформ.

Исследование Д. Турдиева (2020) посвящено проблемам безопасности электронных платёжных систем. Применяя методы анализа рисков, автор предлагает системный подход к выявлению и устранению уязвимостей в инфраструктуре электронных платежей. Одним из ключевых предложений Турдиева является внедрение современных инструментов идентификации, таких как электронная цифровая подпись (ЭЦП) и биометрическая аутентификация, что, по мнению исследователя, позволит значительно повысить уровень доверия со стороны пользователей и сократить количество мошеннических операций.

Н. Тухтасинова (2023) в своей работе рассматривает вопросы цифровой безопасности с точки зрения поведенческих характеристик потребителей. Особое внимание в её исследовании уделяется взаимосвязи между уровнем цифровой грамотности пользователей и их способностью защищать собственные данные в сети. Автор утверждает, что низкий уровень осведомлённости о кибер-угрозах способствует распространению фишинговых атак и увеличивает уязвимость электронных коммерческих систем. Также подчёркивается важность проведения образовательных программ и информационных кампаний среди населения.

Отдельное внимание заслуживает анализ, проведённый Б. Абдурахмоновым (2021), который поднимает проблему правового регулирования в сфере электронных платёжных операций. Он подчёркивает необходимость чёткого разграничения ответственности между участниками электронной коммерции, а также необходимости пересмотра и адаптации существующего законодательства с учётом вызовов цифровой эпохи. Особое место в его исследованиях занимает необходимость усиления регуляторного контроля за деятельностью цифровых платёжных провайдеров.

Методология

В процессе проведения исследования была использована совокупность взаимодополняющих научных методов, позволивших всесторонне охватить проблематику электронной коммерции и кибер-безопасности в условиях цифровой трансформации. Прежде всего, применялся системный подход, в рамках которого электронная коммерция рассматривалась как целостная система, включающая взаимосвязанные компоненты: цифровую инфраструктуру, платёжные сервисы, правовое регулирование и пользовательское поведение. Это позволило выявить ключевые звенья, подверженные кибер-угрозам, и определить направления повышения устойчивости системы в целом.

Для более объективного анализа был использован сравнительный метод, заключающийся в сопоставлении характеристик функционирования субъектов электронной коммерции в Узбекистане с аналогичными структурами в ряде зарубежных стран, в частности, Турции и Республики Корея. Выбор этих государств обусловлен их активной цифровизацией и устойчивыми позициями на глобальном рынке e-commerce, что позволило выявить как успешные практики, так и проблемные зоны.

Также в рамках исследования был проведён контент-анализ нормативных и аналитических материалов, в том числе отчетов Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан, Агентства «Ўзкомназорат», Государственного комитета по статистике, а также цифровых платформ национального уровня, таких как “Click”, “Payme” и “HUMO”. Данный метод обеспечил эмпирическую базу для дальнейших выводов о состоянии и динамике кибер-безопасности в электронной коммерции.

Дополнительно применялся метод анализа на основе практических кейсов, в рамках которого изучался опыт более 20 ведущих электронных коммерческих компаний, действующих на рынке Узбекистана. Особое

внимание уделялось вопросам защиты персональных данных, наличию внутренних политик по информационной безопасности, а также механизмам реагирования на инциденты кибер-угроз.

Комплексное использование вышеуказанных методов позволило обеспечить научную обоснованность результатов исследования и разработать прикладные рекомендации по укреплению кибер-безопасности в сфере электронной коммерции.

Анализ и результаты

За период с 2020 по 2024 год объём электронной коммерции в Республике Узбекистан увеличился в 3,2 раза, что свидетельствует о высокой динамике цифровизации экономических процессов (Госкомстат, 2024). Однако наряду с ростом электронных транзакций значительно усилились и кибер-угрозы, с которыми сталкиваются как бизнес-структуры, так и конечные пользователи.

По итогам 2023 года количество случаев незаконного доступа к информации возросло в 2,7 раза по сравнению с 2020 годом. Это указывает на уязвимость цифровой инфраструктуры и необходимость более строгих мер защиты информационных систем. В то же время, по данным исследования Н. Тухтасиновой (2023), лишь около 34% пользователей обладают базовыми знаниями в области кибер-безопасности, что свидетельствует о низком уровне цифровой грамотности населения и повышенном риске поведенческих уязвимостей.

Некоторые положительные изменения фиксируются в сфере онлайн-платёжных платформ. В частности, по данным Д. Турдиева (2020), доля веб-страниц, защищённых SSL-сертификатами на платформах “Click” и “Payme”, превышает 85%, что демонстрирует прогресс в техническом обеспечении информационной безопасности при осуществлении электронных платежей.

Однако, как подчёркивает Ш.Н. Нарзуллаев, несмотря на технологические достижения, ключевым барьером в развитии электронной коммерции остаётся низкий уровень доверия пользователей к онлайн-сервисам, а также институциональная неясность в сфере реализации политики кибер-безопасности. Отсутствие комплексной нормативной и организационной базы приводит к фрагментарности и неэффективности мер защиты.

Таким образом, выявленные в ходе анализа результаты демонстрируют, что устойчивое развитие электронной коммерции в Узбекистане невозможно без системного и координированного подхода к обеспечению кибер-безопасности на всех уровнях — от пользовательского интерфейса до институциональной регламентации.

Заключение и рекомендации

Электронная коммерция в Республике Узбекистан демонстрирует устойчивые темпы роста и постепенно занимает важное место в национальной экономике. Однако выявленные результаты исследования указывают на то, что данный сектор пока не обладает достаточной синхронизацией с механизмами обеспечения кибер-безопасности. Создание только цифровых платёжных систем без надлежащей защиты информационного пространства может привести к уязвимости как пользователей, так и поставщиков услуг. В связи с этим требуется внедрение комплексного цифрового подхода, сочетающего технологические, институциональные и образовательные меры.

На основе анализа научных трудов узбекских исследователей предлагаются следующие практические рекомендации, направленные на повышение уровня кибер-безопасности в электронной коммерции:

- усовершенствовать политику в сфере кибер-безопасности на институциональном уровне, в том числе адаптировать национальное законодательство в области информационно-коммуникационных технологий

к международным стандартам (например, ISO/IEC 27001);

- ввести обязательную систему аудита информационной безопасности для субъектов электронной коммерции, а также разработать рейтинговую систему оценки защищённости цифровых платформ;
- активизировать взаимодействие между вузами и бизнес-структурами по вопросам подготовки кадров и обмена опытом в области кибер-безопасности;
- организовать широкомасштабные просветительские кампании среди населения, направленные на повышение цифровой грамотности и формирование культуры ответственного поведения в цифровой среде.

Реализация вышеперечисленных мер позволит повысить уровень доверия к цифровым сервисам, обеспечить устойчивость электронных транзакций и создать надёжную основу для дальнейшего развития электронной коммерции в Узбекистане в условиях цифровой экономики.

Список использованной литературы

1. Нарзуллаев Ш.Н. Институциональные основы обеспечения кибербезопасности в условиях цифровой экономики // *Экономика и инновационные технологии*. – 2022. – №3. – С. 45–51.
2. Гуломов Р. Электронная коммерция как фактор развития цифровой экономики Узбекистана // *Цифровая экономика и финансы*. – 2021. – №2. – С. 28–35.
3. Турдиев Д. Анализ рисков и обеспечение безопасности платёжных систем в Узбекистане // *Инновационное развитие*. – 2020. – №3(19). – С. 55–61.
4. Тухтасинова Н. Поведенческие аспекты цифровой безопасности в электронной коммерции // *Экономика и инновации*. – 2023. – №1(37). – С. 66–73.

5. Абдурахмонов Б. Правовое регулирование электронных платёжных систем: проблемы и перспективы // *Юридическая наука и практика*. – 2021. – №4(12). – С. 40–47.
6. Государственный комитет по статистике Республики Узбекистан. Основные показатели электронной коммерции за 2020–2024 гг. // *stat.uz*. – Режим доступа: <https://stat.uz> (дата обращения: 20.06.2025).
7. Агентство «Ўзкомназорат». Ежегодный отчёт по вопросам кибербезопасности за 2023 год. – Ташкент: 2024. – 76 с.
8. Президент Республики Узбекистан. Постановление №ПҚ–4851 «О мерах по дальнейшему развитию цифровой экономики и электронной коммерции». – 05.10.2020.