УДК:347.7(045)(575.1)

АНАЛИЗ ВЛИЯНИЯ КИБЕРПРЕСТУПЛЕНИЙ НА ЭЛЕКТРОННУЮ КОММЕРЦИЮ В КОНТЕКСТЕ ВНЕДРЕНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Султонова Дурдона Шарофиддин кизи
Студент магистратуры Ташкентского Государственного Юридического Университета по направлению «Бизнес право»
Ташкент, Республика Узбекистан

Аннотация:

Передовые технологии представляют собой как значительные возможности для развития электронной коммерции в Узбекистане, так и серьезные вызовы в области кибербезопасности, что требует комплексного правового, технического и институционального исследования для обеспечения устойчивого роста цифровой экономики. Понимание сложного взаимодействия между передовыми технологиями, киберпреступностью и развитием электронной коммерции в Узбекистане является необходимым условием для выработки эффективных стратегий защиты цифровой экономики. Настоящее исследование направлено на анализ влияния киберпреступности на растущий сектор электронной коммерции Узбекистана, изучение двойственной роли передовых технологий — как толчок для экономического роста, так и инструментов для киберпреступников, а также оценку эффективности существующих правовых и технических механизмов защиты.

Ключевые слова: киберпреступления, электронная коммерция, цифровая экономика, правовая защита

ANALYZE OF THE IMPACT OF CYBERCRIME ON E-COMMERCE IN CONTEXT OF INNOVATIVE TECHNOLOGIES IN UZBEKISTAN

Sultonova Durdona Sharofiddin qizi
LLM Student, Tashkent State University of Law
Specialization: Business Law
Tashkent, Republic of Uzbekistan

Abstract:

Advanced technologies offer both significant opportunities for the development of e-commerce in Uzbekistan and serious challenges in the field of cybersecurity. This dual nature necessitates a comprehensive legal, technical, and institutional analysis to ensure the sustainable growth of the digital economy. Understanding the complex interplay between advanced technologies, cybercrime, and the development of e-commerce in Uzbekistan is essential for formulating effective strategies to protect the digital economy. This study aims to analyze the impact of cybercrime on Uzbekistan's growing e-commerce sector, examine the dual role of advanced technologies—as a driver of economic growth and as a tool exploited by cybercriminals—and assess the effectiveness of existing legal and technical protection mechanisms.

Keywords: *cybercrime, e-commerce, digital economy, legal protection*

I. Введение:

Цифровая трансформация экономики Узбекистана в последние годы значительно ускорилась, и электронная коммерция стала одной из ключевых сфер роста. Ожидается, что к концу 2027 года объем рынка электронной коммерции достигнет 2,2 миллиарда долларов США, что демонстрирует впечатляющий потенциал этого сектора в рамках развивающейся цифровой экономики страны.

Однако столь стремительное цифровое расширение сопровождается параллельным ростом киберугроз. В 2023 году, по данным Центра кибербезопасности, в Узбекистане было зафиксировано 11,2 миллиона кибератак, направленных на веб-ресурсы страны. Тревожная тенденция сохраняется и в настоящее время. По мере того как цифровая инфраструктура Узбекистана развивается, а граждане все активнее вовлекаются в онлайн-торговлю, уязвимость перед сложными киберугрозами становится серьезным препятствием для устойчивого экономического роста.

II. Методы

Настоящее исследование использует смешанный методологический подход, сочетающий как качественные, так и количественные методы для всестороннего анализа влияния киберпреступности на электронную коммерцию в Узбекистане с особым вниманием к роли передовых технологий.

Качественная составляющая исследования направлена на изучение контекстуальных факторов, субъективного восприятия и сложных взаимосвязей между киберпреступностью, передовыми технологиями и развитием электронной коммерции в Узбекистане. Это позволяет получить более тонкое представление о правовых, институциональных и культурных аспектах, формирующих ландшафт кибербезопасности. В

то же время количественная часть предоставляет статистические данные о частоте, масштабах и экономических последствиях кибер инцидентов, способствуя объективному измерению тенденций и закономерностей.

Количественные данные анализировались с использованием описательной и выводной статистики для выявления закономерностей и взаимосвязей. Применялись следующие процедуры:

Описательная статистика, выражаемая в расчёте частот, процентов, средних значений и стандартных отклонений.

Анализ тенденций, выражаемая в изучении динамики киберпреступности и показателей электронной коммерции.

Сравнительный анализ показателей Узбекистана с региональными и глобальными стандартами.

III. Результаты

A. Текущее состояние электронной коммерции в Республике Узбекистан

Сектор электронной коммерции Узбекистана демонстрирует стремительный рост в последние годы, укрепляя свои позиции как одного из самых быстрорастущих цифровых рынков Центральной Азии. Рынок электронной коммерции в Узбекистане за последние пять лет увеличился более чем в пять раз, что делает его самым быстрорастущим в регионе. Такая динамика объясняется благоприятным сочетанием факторов, включая последовательную государственную поддержку и устойчивый рост числа пользователей Интернета по всей стране.

Финансовые масштабы этого роста значительны. Исследование показало[1], что в 2021 году объем доходов от электронной коммерции в Узбекистане составил 1,39 миллиарда долларов США, что составляет

[1] Statista. (2023). The cybersecurity market in Uzbekistan. Statista Market Forecast. https://www.statista.com/outlook/tmo/cybersecurity/uzbekistan

90,2% от всех цифровых доходов страны, тогда как на цифровые медиа, электронные услуги и электронное здравоохранение приходится оставшиеся 9,8%. По прогнозу KPMG[2], к концу 2027 года объем рынка достигнет 2,2 миллиарда долларов США, при этом ожидается уровень проникновения электронной коммерции на уровне 9–11%. Это означает семикратный рост по сравнению с 2022 годом, когда объем рынка оценивался в 311 миллионов долларов.

Государственная политика также способствует развитию сектора. В частности, ставка налогообложения онлайн-доходов составляет всего 2% против 4% для традиционного бизнеса, что отражает стремление властей ускорить цифровую трансформацию экономики.

Международное сотрудничество также играет значимую роль. В октябре 2020 года Агентство по продвижению экспорта Узбекистана (на сегодняшний день - Компания развития торговли) заключило соглашение с китайской компанией Alibaba о создании раздела “Сделано в Узбекистане” на платформе Alibaba.com. Государство планирует финансово поддержать регистрацию более 300 местных компаний на этой платформе. Кроме того, в августе 2023 года администрация Наманганской области сообщила, что Alibaba откроет региональный центр в Намангане.

Анализ поведения потребителей и факторов доверия имеет решающее значение для оценки будущего развития электронной коммерции в Узбекистане. На уровень внедрения e-commerce влияют уровень цифровой грамотности, доступ к технологиям, предпочтения в оплате и доверие к онлайн-транзакциям.

B. Анализ воздействия киберпреступности

[2] KPMG. (2023, August 28). Uzbekistan e-commerce market is set to grow 7 times to 2.2 billion USD by 2027. PR Newswire. https://www.prnewswire.com/news-releases/uzbekistan-e-commerce-market-is-set-to-grow-7-times-to-2-2-billion-usd-by-2027-kpmg-301910649.html

Экономическое воздействие киберпреступлений на сектор электронной коммерции Узбекистана является значительным и многогранным, затрагивая сферу предпринимательской деятельности, потребителей и экономику в целом. Хотя точная количественная оценка финансовых потерь, вызванных киберпреступлениями в сфере электронной коммерции в Узбекистане, затруднена из-за ограниченности данных и низкого уровня отчетности, имеющиеся сведения указывают на наличие существенных прямых и косвенных затрат.

Прямые финансовые потери для бизнеса и потребителей включают похищенные средства в результате мошенничества с платежами, расходы, связанные с утечками данных, а также финансовое вымогательство посредством атак программ-вымогателей. Эти потери особенно тяжелы для малых субъектов предпринимательства (МСП), которые, как правило, не располагают достаточными ресурсами кибербезопасности и могут понести катастрофические финансовые последствия даже от одной серьезной атаки. Взаимосвязанная структура систем электронной коммерции означает, что уязвимость на одном этапе цепочки транзакций может повлечь цепную реакцию негативных последствий для множества участников.

Косвенные издержки киберпреступлений выходят за рамки немедленных финансовых потерь и включают в себя ущерб репутации, упущенные деловые возможности и расходы на восстановление. Для предприятий электронной коммерции такие косвенные издержки зачастую превышают прямые убытки. Согласно исследованию 2023 года[3] о влиянии киберпреступности на цифровую экономику, ущерб деловой репутации после инцидента с безопасностью, как правило, приводит к оттоку клиентов, снижению объемов транзакций и утрате

[3] AllahRakha, N. (2024). Impacts of cybercrimes on the digital economy. Uzbek Journal of Law and Digital Policy, 2(3), 29–36. https://doi.org/10.59022/ujldp.207

доверия со стороны инвесторов — последствия, которые могут сохраняться долго после устранения непосредственных технических проблем.

Утечки данных и нарушения конфиденциальности составляют еще одну важную категорию киберпреступлений, влияющих на сферу электронной коммерции[4]. Эти инциденты предполагают несанкционированный доступ к базам данных клиентов, что приводит к получению персональной и финансовой информации, которая может быть монетизирована путем прямого мошенничества или продажи на теневых онлайн-площадках. Растущие объемы потребительских данных, собираемых платформами электронной коммерции, делают их привлекательными целями для киберпреступников, стремящихся получить ценные персональные сведения.

С. Анализ правовой и нормативной базы, регулирующей борьбу с киберпреступностью в сфере электронной коммерции в Узбекистане

Правовая база Узбекистана, регулирующая вопросы киберпреступности и безопасности электронной коммерции, претерпела значительные изменения в последние годы, однако сохраняются существенные пробелы с реализацией принятых норм. До апреля 2022 года в стране отсутствовало специализированное законодательство, направленное непосредственно на обеспечение кибербезопасности; соответствующие нормы были фрагментарно распределены по различным законам в области телекоммуникаций, информационных технологий и положениям Уголовного кодекса. Такая фрагментация создавала правовые неопределенности и затрудняла эффективное реагирование на изменяющиеся киберугрозы.

[4] Litska S., Oswald M., Ryan D. Intangible harms: A comparative analysis of cybercrime victimization // *International Journal of Law, Crime and Justice*. – 2018. – № 55. – С. 1–12.

Ключевым событием стало принятие Закона Республики Узбекистан “О кибербезопасности”, от 15.04.2022 г. № ЗРУ-764, который стал первым всеобъемлющим законодательным актом в сфере кибербезопасности. Данный закон включил ряд важных положений, в том числе:

- формальное определение ключевых понятий и терминов в области кибербезопасности, что способствовало формированию общего юридического языка для борьбы с цифровыми угрозами.

- установление институциональной ответственности за надзор в сфере кибербезопасности, возложив функцию реализации государственной политики и программ в данной области на Президента Республики Узбекистан.

- введение требований к защите критической инфраструктуры, включая базовые стандарты безопасности для систем, обеспечивающих предоставление жизненно важных услуг.

- создание нормативной основы для отчетности об инцидентах и обмена информацией между заинтересованными субъектами.

Несмотря на значительный прогресс, эффективность применения закона ограничивается как структурными недостатками, так и проблемами реализации. Закон устанавливает общие принципы, но не содержит детализированных механизмов правоприменения и технических стандартов, необходимых для практической реализации.

Принятый в сентябре 2022 года обновленный закон об электронной коммерции также усилил правовую базу, устранив ряд проблем,

связанных с безопасностью в данной сфере. Ключевые положения включают:

- правовое положение и признание электронных чеков и счетов-фактур в качестве допустимых подтверждений оплаты товаров и услуг, что создает основу для безопасных цифровых транзакций.

- введение требований к защите персональных данных и конфиденциальности в контексте электронной коммерции, хотя эти нормы остаются достаточно обобщенными.

- установление гарантий для потребителей в цифровых сделках, включая право на получение достоверной информации и обеспечение защищенной оплаты.

Кроме того, Указ Президента № ПП-167 от 31 мая 2023 года[5] ввёл дополнительные требования по обеспечению кибербезопасности для компаний, что дополнительно укрепило нормативно-правовую базу для частного сектора, включая субъекты электронной коммерции.

Особую сложность представляют трансграничные преступления, влияющие на сферу электронной коммерции в Узбекистане. Транснациональный характер многих киберугроз порождает проблемы юрисдикции, расследования и судебного преследования. Например, по данным Центра кибербезопасности[6], в 2023 году Нидерланды неожиданно стали лидером по числу атак — более 759 000 атак были зафиксированы с IP-адресов этой страны, за ней следуют США, Россия,

[5] Постановление Президента Республики Узбекистан, от 31.05.2023 г. № ПП-167

[6] Центр кибербезопасности. Ежегодный доклад о кибербезопасности за 2023 год. – Ташкент: Правительство Республики Узбекистан, 2024.

Германия, Индия и Китай. Этот международный аспект требует эффективных механизмов сотрудничества, которые пока недостаточно развиты.

Ограниченное число соглашений о взаимной правовой помощи и экстрадиции по киберпреступлениям также затрудняет трансграничное правоприменение. Хотя Узбекистан участвует в некоторых региональных инициативах, они в основном ориентированы на традиционные формы преступности и не охватывают кибер специфику. Дополнительные сложности возникают при установлении личности злоумышленников, особенно при использовании сложных методов сокрытия источников атак.

Заключение

В ходе настоящего исследования были выявлены ключевые аспекты воздействия киберпреступлений на сферу электронной коммерции в Узбекистане, а также сложная роль, которую играют передовые технологии в данной области.

Во-первых, рынок электронной коммерции Узбекистана демонстрирует значительный потенциал роста. Рост стимулируется увеличением уровня проникновения интернета, государственными инициативами и расширением цифровых платежных инструментов. Однако стремительное цифровое развитие сопровождается ростом угроз в сфере кибербезопасности.

Во-вторых, воздействие киберпреступности на сферу электронной коммерции имеет многогранный характер: оно охватывает как прямые финансовые потери, так и репутационные издержки и подрыв доверия потребителей. Наиболее распространённой формой мошенничества являются платежные аферы. Эти угрозы создают существенные барьеры

на пути к более широкому внедрению электронной коммерции, особенно для малых и средних предприятий, обладающих ограниченными ресурсами для обеспечения кибербезопасности.

В-третьих, законодательная и нормативная база Узбекистана в области борьбы с киберпреступностью значительно укрепилась после принятия Закон Республики Узбекистан “О кибербезопасности”, от 15.04.2022 г. № ЗРУ-764 и внесения изменений в законодательство об электронной коммерции в сентябре 2022 года. Однако сохраняются серьёзные пробелы, особенно в сфере регулирования новых технологий, вопросов ответственности и международного сотрудничества. Дополнительные сложности создают ограниченные институциональные ресурсы, трудности с трансграничной юрисдикцией и недостаточная техническая оснащенность следственных органов.

Список использованной литературы

1. АллахРакха Н. Стратегия Узбекистана в области искусственного интеллекта: нормативная база, приоритеты и вызовы // *Международный журнал права и политики*. – 2023. – Т. 1, № 1.

2. АллахРакха Н. Киберпреступность и правовые и этические вызовы новых технологий // *Международный журнал права и политики*. – 2024. – Т. 2, № 5. – С. 28–36.

3. АллахРакха Н. Влияние киберпреступлений на цифровую экономику // *Узбекский журнал права и цифровой политики*. – 2024. – Т. 2, № 3. – С. 29–36.

4. Гулямов С. С., Эгамбердиев Э., Наим А. Практико-ориентированный подход к реформированию традиционной модели высшего образования с применением EdTech-технологий // *2024 4-я Международная конференция по технологиям, улучшающим обучение в высшем образовании (TELE)*. – IEEE, 2024. – С. 340–343.

5. Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан. Доклад о реализации Стратегии «Цифровой Узбекистан — 2030». – Ташкент: Правительство Республики Узбекистан, 2022.
6. Министерство инвестиций, промышленности и торговли. Стратегия развития электронной торговли в Узбекистане. – Ташкент: Правительство Республики Узбекистан, 2022.
7. Национальный комитет Республики Узбекистан по статистике. Показатели цифровой экономики за 2023 год. – Ташкент: Правительство Республики Узбекистан, 2024.