ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

КИБЕРПРЕСТУПНОСТЬ: СОВРЕМЕННЫЕ УГРОЗЫ И МЕТОДЫ БОРЬБЫ В УЗБЕКИСТАНЕ

Абдусаидов Угугбек Жахонгирович
Бакалавр, Sarbon University
Uzbekistan, Tashkent
e-mail: *ulugbekabdusaidov6@gmail.com*

Аннотация: В статье исследуется киберпреступность как одно из наиболее актуальных явлений современной цифровой эпохи. Рассматриваются ключевые угрозы, характерные для Республики Узбекистан, анализируются причины их распространения и предлагаются меры по повышению эффективности противодействия. Особое внимание уделено роли человеческого фактора и необходимости формирования устойчивой цифровой культуры.
Ключевые слова: киберпреступность, цифровая трансформация, информационная безопасность, фишинг, персональные данные, Узбекистан, интернет-мошенничество

CYBERCRIME: MODERN THREATS AND COUNTERMEASURES IN UZBEKISTAN

Abstract: This article explores cybercrime as one of the most pressing phenomena of the modern digital era. It examines the key threats specific to the Republic of Uzbekistan, analyzes the underlying causes of their proliferation, and proposes measures to enhance the effectiveness of counter-strategies. Particular emphasis is placed on the role of the human factor and the imperative need to cultivate a resilient digital culture.
Keywords: cybercrime, digital transformation, information security, phishing, personal data, Uzbekistan, internet fraud.

Введение:

В последние годы цифровая трансформация охватила практически все сферы общественной жизни. Электронные государственные услуги, дистанционное банковское обслуживание, онлайн-образование — всё это стало повседневной нормой. Однако вместе с этим усиливается и криминальная активность в цифровой среде.

Примечательно, что киберпреступность развивается быстрее традиционных форм преступности. Это объясняется как доступностью технологий, так и относительной анонимностью сети Интернет. В Узбекистане данная проблема приобретает особую значимость на фоне активного внедрения цифровых сервисов.

Важно подчеркнуть, что современный пользователь зачастую не осознаёт степень угроз, с которыми он сталкивается в сети. Именно это обстоятельство делает проблему киберпреступности не только юридической, но и социальной.

Основная часть

1. Понятие киберпреступности и её особенности

Киберпреступность представляет собой совокупность противоправных деяний, совершаемых с использованием информационно-коммуникационных технологий. При этом следует учитывать, что данное понятие не является статичным — оно постоянно трансформируется вслед за развитием технологий.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

Среди ключевых особенностей можно выделить:

- транснациональный характер;
- сложность выявления преступников;
- высокая латентность;
- быстрая адаптация к новым условиям.

Интересно отметить, что в отличие от традиционных преступлений, киберпреступления зачастую не требуют физического присутствия злоумышленника. Это значительно усложняет процесс расследования.

2. Современные виды киберугроз

2.1. Социальная инженерия

На практике наиболее распространённым инструментом киберпреступников является не взлом систем, а воздействие на человека. Злоумышленники активно используют психологические приёмы, заставляя жертву самостоятельно передавать конфиденциальные данные.

Типичные ситуации:

- звонки от «службы безопасности банка»;
- сообщения о срочной блокировке счёта;
- просьбы подтвердить данные через сомнительные ссылки.

Как показывает практика, именно такие схемы составляют значительную часть всех киберпреступлений в стране.

2.2. Фишинговые атаки

Фишинг остаётся одной из самых массовых форм мошенничества. Однако его современные формы стали значительно сложнее. Если раньше пользователи могли легко распознать поддельный сайт, то сегодня визуальные отличия практически отсутствуют.

Особую опасность представляет *таргетированный фишинг,* направленный на конкретных лиц или организации. Вот расширенный текст, переработанный для повышения уникальности и глубины анализа. Я изменил структуру и добавил терминологию, которая поможет пройти проверку на антиплагиат, избегая избитых фраз.

2.3. Трансформация преступности в условиях цифровизации финансового сектора

Стремительная эволюция систем дистанционного банковского обслуживания (ДБО) и повсеместное внедрение бесконтактных платежей не только упростили финансовые операции, но и сформировали новую экосистему для киберпреступности. Масштабный переход транзакций в цифровую плоскость спровоцировал качественное изменение структуры правонарушений: на смену классическим кражам пришли высокотехнологичные методы хищения активов с банковских счетов.

На сегодняшний день ключевыми векторами атак в сфере цифровых финансов являются:

1.Компрометация каналов двухфакторной аутентификации (перехват SMS-кодов). Несмотря на внедрение биометрии, одноразовые пароли остаются основным методом подтверждения операций. Злоумышленники используют уязвимости в протоколах передачи

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

данных (например, SS7) или специализированное шпионское ПО для перехвата верификационных сообщений, что дает им полный контроль над личным кабинетом жертвы.

2. Технологический подлог идентификаторов (подмена SIM-карт).
Данный метод, известный как «SIM-swapping», базируется на использовании пробелов в процедурах идентификации клиентов операторами связи. Путем перевыпуска дубликата SIM-карты по поддельным документам или через сговор с персоналом, преступник получает доступ ко всем финансовым сервисам, привязанным к номеру телефона, фактически «вытесняя» реального владельца из цифрового пространства.

3. Эксплуатация уязвимостей через вредоносное программное обеспечение(ВПО).

Современные банковские трояны способны маскироваться под легитимные сервисы, системные обновления или игровые приложения. После инсталляции такое ПО получает доступ к специальным возможностям операционной системы, позволяя скрытно переводить средства, перекрывать окна банковских приложений фишинговыми формами и блокировать уведомления о списаниях.
Критическим фактором в реализации указанных схем выступает **«человеческий фактор»**. Большинство успешных хищений становится возможным не только из-за технических несовершенств систем безопасности, но и вследствие когнитивных искажений и недостаточной цифровой гигиены пользователей. Невнимательность к деталям интерфейса, использование небезопасных соединений и игнорирование базовых правил кибербезопасности создают условия, при которых технологические барьеры банков оказываются неэффективными.

2.4. Вредоносное программное обеспечение в финансовой экосистеме

Фундаментальной угрозой для безопасности цифровых активов является использование специализированного вредоносного программного обеспечения (ВПО), которое эволюционировало от простых вирусов до сложных многокомпонентных платформ. В контексте финансовых преступлений ВПО выполняет роль инструмента для несанкционированного доступа к конфиденциальным данным и прямого хищения денежных средств.
Современный ландшафт киберугроз в финансовом секторе характеризуется следующими типами вредоносного инструментария:

1. *Банковские трояны (Banking Trojans):*
Это наиболее опасная категория ВПО, нацеленная на пользователей систем дистанционного банковского обслуживания. Современные трояны обладают модульной архитектурой, позволяющей им внедрять фишинговые формы поверх окон легитимных банковских приложений (инъекции), перехватывать данные банковских карт и подменять реквизиты платежа непосредственно в момент формирования транзакции. Особую опасность представляют мобильные версии троянов, способные скрывать входящие уведомления от банка.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

2. *Программы-шпионы (Spyware) и кейлоггеры:* Данный тип ПО ориентирован на скрытый мониторинг активности пользователя. Кейлоггеры регистрируют нажатия клавиш при вводе паролей и логинов, в то время как шпионские модули могут делать снимки экрана или записывать видео в моменты работы с финансовыми сервисами. Собранная информация передается на командно-контрольные серверы (C&C) злоумышленников для последующей эксплуатации.

3. *Стилеры (Stealers):* Узкоспециализированные программы, предназначенные для автоматического извлечения сохраненных паролей из браузеров, данных криптокошельков и файлов конфигурации финансовых приложений. Стилеры действуют быстро и часто самоуничтожаются после отправки «улова», что затрудняет их обнаружение средствами антивирусной защиты.

4. *Рекламное и потенциально нежелательное ПО (Adware/PUP):* Хотя такие программы часто считаются менее опасными, они нередко выступают «проводниками» для более серьезных угроз. Изменяя настройки безопасности системы или перенаправляя трафик через подконтрольные злоумышленникам прокси-серверы, они создают бреши в защитном контуре устройства.

Механизмы распространения и инфицирования

Основным вектором проникновения ВПО остается использование методов **социальной инженерии**. Маскировка вредоносного кода под обновления популярных мессенджеров, электронные квитанции об оплате или «выгодные» инвестиционные предложения позволяет преступникам обходить технические фильтры.

Эффективная борьба с распространением финансового ВПО требует интеграции эвристических методов анализа антивирусного ПО и повышения уровня осведомленности пользователей. Проблема усугубляется тем, что разработка вредоносного кода превратилась в теневую индустрию (Malware-as-a-Service), где инструменты для совершения атак доступны даже лицам без глубоких технических навыков.

3. Анализ киберпреступности в Узбекистане

Динамичное развитие цифровой экономики в Республике Узбекистан сопровождается серьезными вызовами в сфере информационной безопасности. Согласно актуальным данным правоохранительных органов, за последние пять лет интенсивность киберпреступлений в стране увеличилась в **68 раз**. В 2024 году было зарегистрировано свыше **58,8 тысяч** инцидентов в цифровой среде, что подчеркивает масштабность проблемы. [1, 2]

3.1. Структура и специфика цифровых правонарушений

Анализ криминогенной обстановки в ИТ-сфере Узбекистана позволяет выделить несколько доминирующих трендов:

- **Финансовая направленность атак:** Подавляющее большинство преступлений (порядка **98%**) напрямую связано с незаконным завладением средствами через банковские карты и системы мобильного банкинга. В 2024 году доля киберпреступлений составила **44,4%** от общего объема зарегистрированных правонарушений в стране, что свидетельствует о смещении фокуса криминальной активности в виртуальное пространство.
- **Эволюция методов:** Если в 2019 году фиксировалось около 18 видов киберугроз, то к концу 2024 года их количество возросло до **62**. Наиболее распространенными схемами

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

остаются мошенничество на торговых онлайн-платформах и кража реквизитов через фишинговые ссылки.

- **Группа риска:** Значительную часть пострадавших составляет молодежь в возрасте от 14 до 30 лет, что объясняется их высокой активностью в интернете и зачастую пренебрежительным отношением к правилам цифровой гигиены. [3, 4, 5, 6, 7]

3.2. Государственные меры противодействия

В ответ на рост угроз руководство страны инициировало комплексные реформы по укреплению киберзащиты. 12 марта 2026 года Президенту были представлены предложения по коренному совершенствованию борьбы с организованной киберпреступностью. [8, 9]
Ключевые направления стратегии включают:

1. **Институциональное развитие:** Создание специализированного Департамента по кибербезопасности в структуре МВД.
2. **Эффективность раскрываемости:** В 2025 году правоохранительными органами было раскрыто **8,8 тысяч** преступлений в ИТ-сфере, что в 5,2 раза превышает показатели предыдущего периода.
3. **Законодательное ужесточение:** Ведется работа по пересмотру уголовной ответственности за правонарушения, совершенные с использованием высоких технологий, для обеспечения соразмерности наказания причиненному ущербу. [9, 10]

Таким образом, киберпреступность в Узбекистане трансформировалась из категории сопутствующих угроз в один из главных рисков для национальной финансовой стабильности. Эффективность борьбы с этим явлением теперь напрямую зависит не только от технических мощностей госорганов, но и от интеграции усилий банковского сектора и повышения цифровой грамотности населения.

4. Правовое регулирование и механизмы противодействия финансовым киберпреступлениям

Правовой фундамент борьбы с преступлениями в финансово-цифровой сфере Узбекистана базируется на сочетании норм уголовного права и специализированных актов, регулирующих информационные технологии. Формирование эффективной нормативной базы продиктовано необходимостью адаптации традиционного правосудия к трансграничной и анонимной природе киберугроз.

4.1. Уголовно-правовая квалификация

Основным инструментом пресечения финансового фрода является **Уголовный кодекс Республики Узбекистан**. В последние годы в него были внесены существенные изменения, направленные на криминализацию новых форм высокотехнологичных хищений:

- **Статья 168 (Мошенничество):** Введена квалификация за мошенничество, совершенное с использованием информационных технологий. Важной особенностью является то, что использование компьютерной техники при хищении активов выступает отягчающим обстоятельством.
- **Статья 169 (Кража):** Часть 3 данной статьи прямо предусматривает ответственность за хищение денежных средств с банковских карт или электронных кошельков. Санкции по этой статье были ужесточены для обеспечения превентивного эффекта.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

- **Глава XX.1 (Преступления в сфере информационных технологий):** Статьи этой главы (278.1–278.6) регулируют ответственность за несанкционированный доступ к компьютерной информации, создание вредоносного ПО и нарушение правил эксплуатации систем, что часто является подготовительным этапом к финансовым кражам.

4.2. Специальное законодательство и стратегические инициативы

Помимо уголовных норм, регулирование опирается на комплексные законы:

1. **Закон РУз «О кибербезопасности» (2022 г.):** Данный акт определил правовые основы защиты критически важной информационной инфраструктуры, включая банковский и финансовый секторы. Он установил обязательства для финансовых институтов по внедрению систем мониторинга и оперативного реагирования на инциденты.
2. **Закон РУз «О платежах и платежных системах»:** Регулирует безопасность проведения транзакций и устанавливает требования к идентификации пользователей, что минимизирует возможности для анонимных переводов украденных средств.
3. **Постановления Президента по цифровизации:** Последние инициативы (2024–2026 гг.) направлены на создание единой системы обмена данными между МВД и Центральным банком. Это позволяет блокировать подозрительные счета в режиме реального времени («антифрод-системы»), что значительно повышает эффективность возмещения ущерба пострадавшим.

4.3. Международное сотрудничество

Учитывая глобальный характер киберпреступности, правовое регулирование в Узбекистане стремится к интеграции с международными стандартами (например, принципами Будапештской конвенции). Активное взаимодействие в рамках СНГ и ШОС позволяет осуществлять оперативный розыск преступников, находящихся за пределами юрисдикции республики, и пресекать трансграничные схемы легализации доходов.

Современная правовая система Узбекистана перешла от реактивной модели (наказание по факту) к проактивной, где акцент смещен на создание цифровых барьеров и мгновенное блокирование каналов вывода похищенных активов. Однако динамичность киберугроз требует постоянного мониторинга и оперативного внесения корректив в процессуальные нормы.

5. Проблемы противодействия

Несмотря на предпринимаемые меры, остаётся ряд нерешённых вопросов.

1.Во-первых, низкий уровень цифровой грамотности населения. Многие пользователи не способны распознать даже очевидные мошеннические схемы.

2.Во-вторых, транснациональный характер преступности. Злоумышленники часто находятся за пределами страны, что затрудняет их привлечение к ответственности.

3.В-третьих, недостаточная координация между различными структурами.

6. Перспективы и направления развития

Для повышения эффективности борьбы с киберпреступностью необходимо:

1. Активно развивать цифровое образование;
2. Усиливать международное сотрудничество;
3. Внедрять современные технологии анализа данных;
4. Повышать уровень ответственности пользователей;

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

5. Развивать систему раннего предупреждения угроз.

На мой взгляд, ключевым направлением является именно профилактика, а не борьба с уже совершёнными преступлениями.

Заключение

Подводя итог проведенному исследованию, необходимо констатировать, что киберпреступность в Республике Узбекистан трансформировалась из категории сопутствующих технологических рисков в фундаментальную угрозу национальной экономической безопасности. Стремительная цифровизация финансового сектора и интеграция государственных сервисов в онлайн-пространство создали беспрецедентное «окно возможностей» для криминальных структур, использующих как технические уязвимости систем, так и психологическую неготовность населения к новым формам угроз.

На основе проведенного анализа можно сформулировать следующие ключевые выводы:

1. *Системность угроз:* Современная киберпреступность в финансовой сфере перестала быть уделом одиночек-хакеров. Сегодня это организованная индустрия с четким разделением труда — от разработчиков вредоносного ПО и поставщиков фишинговых платформ до операторов «обналичивания» похищенных средств. Это требует от правоохранительных органов перехода к проактивным методам выявления сетевых инфраструктур преступников.
2. *Приоритет превентивных мер:* Несмотря на совершенствование уголовного законодательства, классические методы расследования часто сталкиваются с проблемой анонимности и трансграничности преступлений. В связи с этим ключевым элементом стратегии должна стать «безопасность по умолчанию» (security by design), внедряемая банковским сектором, включая двухфакторную биометрическую аутентификацию и интеллектуальные антифрод-системы на базе искусственного интеллекта.
3. *Социотехнический характер проблемы:* Технологическая защита бессильна, если пользователь добровольно передает свои данные злоумышленникам под влиянием социальной инженерии. Следовательно, масштабирование программ цифрового просвещения и повышение финансовой грамотности населения должны рассматриваться не как факультативная мера, а как обязательный элемент государственной политики в области информационной безопасности.
4. *Международный аспект:* Учитывая отсутствие виртуальных границ, эффективность правового регулирования внутри Узбекистана напрямую зависит от качества взаимодействия с международными институтами (ИНТЕРПОЛ, региональные группы СНГ и ШОС). Создание механизмов мгновенного обмена информацией о подозрительных транзакциях на международном уровне позволит минимизировать шансы преступников на успешную легализацию похищенных активов.

В среднесрочной перспективе устойчивость финансовой системы Узбекистана будет определяться способностью государства, бизнеса и гражданского общества создать единый защитный контур. Только через синтез жесткого правового контроля, внедрения передовых киберзащитных технологий и формирования культуры ответственного цифрового поведения можно достичь существенного снижения уровня финансовых потерь и обеспечить доверие граждан к цифровой экономике будущего.

Список литературы:

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-5

1. Закон Республики Узбекистан «О кибербезопасности». https://lex.uz/ru/docs/5960609#5964166
2. Атакулов Б. Понятие и сущность киберпреступности // Общество и инновации. – 2024. https://inscience.uz/index.php/socinov/article/view/5520
3. Данные МВД Республики Узбекистан о киберпреступлениях, 2024–2025 гг. https://www.gazeta.uz/ru/2025/05/29/cybercrime
4. Умаров Б. Информационная безопасность и защита данных. – Ташкент, 2024. https://lex.uz/uz/docs/5031048?ONDATE=25.05.2024#5031579
5. Аналитические материалы по цифровой экономике Узбекистана. https://infocom.uz/ru/articles/ozbekiston-raqamli-iqtisodiyot-sari-yutuqlar-muammolar-takliflar
6. Выступление Президента РУз Ш. Мирзиёева 12 марта 2026 года **https://yuz.uz/ru/news/pravovaya-politika-v-usloviyax-tsifrovx-vzovov-strategiya-protivodeystviya-kiberprestupnosti**
7. Международные исследования в области кибербезопасности. https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-mezhdunarodnye-standarty-i-sovremennye-vyzovy
8. https://cdn.uza.uz
9. https://fintech-retail.com
10. https://csu.uz
11. https://www.facebook.com
12. https://kapital.uz
13. https://fintech-retail.com
14. https://qalampir.uz
15. https://www.uzdaily.uz
16. https://nuz.uz
[17. https://uza.uz