Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Cybercrime involving personal data and electronic payment systems: challenges, threats, and prevention strategies

Bakhtiyor UMAROV[1]

General Prosecutor's Office of the Republic of Uzbekistan

ARTICLE INFO

Article history:
Received October 2025
Received in revised form
15 October 2025
Accepted 15 November 2025
Available online
05 December 2025

Keywords:
cybercrime,
personal data protection,
electronic payment systems,
data breaches,
cybersecurity,
digital fraud,
ransomware,
phishing,
online banking security,
cybercrime prevention
strategies.

ABSTRACT

The rapid development of information and communication technologies has fundamentally transformed modern society, creating new opportunities in the banking sector, public services, and various commercial sectors. However, digital transformation has simultaneously created vulnerabilities that are actively exploited by cybercriminals. This study examines the escalation of global cybercrime trends, with particular emphasis on personal data breaches and electronic payment system fraud. Analysis of international statistics reveals an alarming growth trajectory: in the US, a record number of cybercrimes were recorded in 2024 – 860,000 cases with losses amounting to $16.6 billion. Similar trends are observed in Russia and Uzbekistan, where the level of cybercrime has risen dramatically. In Uzbekistan, cybercrimes have increased nearly 70-fold over three years, accounting for almost half of all registered crimes with damages exceeding 1 trillion soums. The study proposes a comprehensive three-component system for countering cybercrime: technical measures, including data encryption and access control; legal and regulatory reforms that strengthen accountability; and organizational initiatives to establish specialized law enforcement units and interagency data integration systems.

2181-1415/© 2025 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol6- iss6-pp50-56

[1] Deputy Head of Department, General Prosecutor's Office of the Republic of Uzbekistan. E-mail: baxtiyor-7797@mail.ru

Shaxsiy ma’lumotlar va elektron to‘lov tizimlaridan foydalanilgan kiberjinoyatlar: muammolar, xavf-xatarlar va oldini olish yo‘llari

Kalit so‘zlar:
kiberjinoyatchilik,
shaxsiy ma’lumotlarni himoya qilish,
elektron to‘lov tizimlari,
ma’lumotlarning oshkor bo‘lishi,
kiberhavfsizlik,
raqamli firibgarlik,
tovlamachilik dasturlari,
fishing,
onlayn-banking xavfsizligi,
kiberjinoyatlarning oldini olish strategiyalari.

ANNOTATSIYA

Axborot-kommunikatsiya texnologiyalarining shiddat bilan rivojlanishi zamonaviy jamiyatni tubdan o‘zgartirib, bank sohasi, davlat xizmatlari va turli tijorat sektorlarida yangi imkoniyatlar yaratdi. Biroq, raqamli transformatsiya ayni paytda kiberjinoyatchilar tomonidan faol foydalanilayotgan zaifliklarni ham keltirib chiqardi. Ushbu tadqiqot shaxsiy ma’lumotlarning tarqalishi va elektron to‘lov tizimlari bilan bog‘liq firibgarliklarga alohida e’tibor qaratgan holda kiberjinoyatchilik global tendensiyasining kuchayishini ko‘rib chiqadi. Xalqaro statistik ma’lumotlar tahlili tashvishli o‘sish yo‘nalishini ko‘rsatmoqda: AQShda 2024-yilda 16,6 milliard dollar zarar bilan rekord darajadagi 860 000 ta kiberjinoyat qayd etilgan. Xuddi shunday tendensiyalar kiberjinoyatchilik darajasi keskin oshgan Rossiya va O‘zbekistonda ham kuzatilmoqda. O‘zbekistonda kiberjinoyatlar uch yil ichida qariyb 70 barobar ko‘payib, 1 trillion so‘mdan ortiq zarar yetkazgan holda barcha ro‘yxatga olingan jinoyatlarning deyarli yarmini tashkil etdi. Tadqiqot kiberjinoyatlarga qarshi kurashishning uch tarkibiy qismli kompleks tizimini taklif etadi: ma’lumotlarni shifrlash va kirishni nazorat qilishni o‘z ichiga olgan texnik choralar; javobgarlikni kuchaytiruvchi huquqiy va me’yoriy islohotlar; ixtisoslashtirilgan huquqni muhofaza qilish bo‘linmalari va idoralararo ma’lumotlarni integratsiyalash tizimlarini yaratish bo‘yicha tashkiliy tashabbuslar.

Киберпреступления с использованием персональных данных и электронных платежных систем: вызовы, угрозы и пути предупреждения

Ключевые слова:
киберпреступность,
защита персональных данных,
электронные платежные системы,
утечки данных,
кибербезопасность,
цифровое мошенничество,
программы-вымогатели,
фишинг,
безопасность онлайн-банкинга,
стратегии предупреждения киберпреступлений.

АННОТАЦИЯ

Стремительное развитие информационно-коммуникационных технологий коренным образом преобразовало современное общество, создав новые возможности в банковской сфере, государственных услугах и различных коммерческих секторах. Однако цифровая трансформация одновременно создала уязвимости, которые активно эксплуатируются киберпреступниками. Настоящее исследование рассматривает эскалацию глобальной тенденции киберпреступности с особым акцентом на утечки персональных данных и мошенничество с электронными платежными системами. Анализ международной статистики выявляет тревожную траекторию роста: в США в 2024 году зарегистрировано рекордное количество киберпреступлений

– 860 000 случаев с убытками в размере 16,6 млрд долларов. Аналогичные тенденции наблюдаются в России и Узбекистане, где уровень киберпреступности возрос драматически. В Узбекистане киберпреступления увеличились почти в 70 раз за три года, составив почти половину всех зарегистрированных преступлений с ущербом, превышающим 1 триллион сумов. Исследование предлагает комплексную трехкомпонентную систему противодействия киберпреступлениям: технические меры, включающие шифрование данных и контроль доступа; правовые и нормативные реформы, усиливающие ответственность; организационные инициативы по созданию специализированных правоохранительных подразделений и систем интеграции межведомственных данных.

Постепенное развитие информационно-телекоммуникационных технологий существенным образом изменило в лучшую сторону жизнь современного общества. Посредством применения информационно-коммуникационных технологий (ИКТ) появились новые общественные отношения в банковско-кредитной сфере, области оказания государственных и социальных услуг, в отрасли сервиса, в том числе доставки еды или такси, а также других.

При этом каждая сфера стремительно развивается с учетом потребностей пользователей и расширением зоны обслуживания интернет-связи. Однако, как и любое новшество, применение ИКТ имеет свои недостатки, что служит для использования этих недостатков в целях совершения правонарушений и преступлений.

Как справедливо отмечает профессор Оксфордского университета Федерико Варезе, «киберпреступность, как и все формы организованной преступности, имеет место в определенных контекстах, связанных с национальными характеристиками, такими как уровень образования, проникновение интернета, ВВП или уровень коррупции» [1]. Согласно Всемирному индексу киберпреступности, разработанному международной группой исследователей в рамках европейского проекта CRIMGOV в 2024 году, масштаб преступлений с применением ИКТ из года в год увеличивается в геометрической прогрессии по всему миру.

Согласно открытым данным, в США количество киберпреступлений в 2024 году побило все рекорды. Об этом говорится в ежегодном отчёте Центра жалоб на интернет-преступления (IC3), действующего при ФБР. За год ведомство получило почти 860 000 обращений – это на треть больше, чем в 2023 году [2].

Ущерб от действий мошенников и хакеров в 2024 году оценён в $16,6 миллиарда – самая крупная сумма с момента создания центра в 2000 году. Только за последние пять лет IC3 зарегистрировал 4,2 миллиона жалоб на общую сумму ущерба $50,5 миллиарда.

По мнению экспертов компании Cybersecurity Ventures, «если бы киберпреступность измерялась как страна, то ущерб в размере $9,5 триллиона USD глобально в 2024 году сделал бы её третьей по величине экономикой мира после США и Китая». Стив Морган, основатель и главный редактор Cybersecurity

Ventures, прогнозирует, что глобальные затраты на киберпреступность будут расти на 15 процентов ежегодно, достигнув $10,5 триллиона USD к 2025 году [3].

Фрод по-прежнему остаётся основным источником убытков, а среди угроз критической инфраструктуре первое место снова занял вымогательский софт. Жалобы, связанные с атаками программ-вымогателей, выросли на 9% и составили почти половину от всех зарегистрированных случаев в этой категории – 3 165 инцидентов.

Наиболее распространённой формой атак по-прежнему остаются фишинг и его разновидности – почти 200 000 жалоб. Наиболее уязвимой категорией остаются пожилые граждане: от людей старше 60 лет поступило 147 127 жалоб, совокупные потери которых достигли 4,8 миллиарда долларов.

Согласно данным Следственного департамента МВД Российской Федерации, за первые семь месяцев 2024 года ущерб от IT-преступлений в России уже достиг 99 млрд рублей, а преступления в сфере кибермошенничества составляют более 30% от общего числа [4].

Эксперты компании F.A.C.C.T. (ведущий российский разработчик технологий для борьбы с киберпреступлениями с 20-летним опытом исследований) отмечают, что в 2024 году количество атак программ-вымогателей выросло на 44% по сравнению с предыдущим годом. При этом в 10% подобных инцидентов целью киберпреступников был не выкуп, а диверсия для нанесения максимального ущерба жертве [5].

По данным аналитиков Positive Technologies, во втором квартале 2024 года было зафиксировано в 2,6 раза больше атак по сравнению с аналогичным периодом 2023 года. Исследователи подчеркивают, что «доля программ-шпионов среди всего вредоносного ПО, используемого в атаках на российские организации, составила 45%, при этом шифровальщики составили лишь 27%» [6].

В «группе риска» в 2024 году в первую очередь оказались ретейл и интернет-магазины, медицинские организации, образовательные центры. Как отмечают эксперты, «большинство похищенных баз данных выкладываются в публичный доступ, в основном в Telegram-каналах, бесплатно для нанесения наибольшего ущерба компаниям и их клиентам» [6].

В ноябре 2024 года Госдума Российской Федерации приняла законы, усиливающие ответственность за утечки персональных данных и их незаконное использование и передачу, введя уголовную ответственность и оборотные штрафы (до 3% совокупной выручки). По мнению экспертов, это окажет «огромное влияние» на отрасль, заставляя компании более системно подходить к информационной безопасности [7].

Масштабы и границы киберпреступлений неизмеримы и продолжают расти. Угрозы и атаки подобного характера имеются также в реалиях Узбекистана. Согласно статистическим данным, за последние три года количество киберпреступлений возросло почти в 70 раз, а в текущем году их удельный вес составил почти половину всех преступлений, материальный ущерб от которых превышает 1 трлн сумов [8].

Замминистра экономики и финансов Республики Узбекистан Ахадбек Хайдаров подчеркивает, что «рост цифровой экономики и онлайн-банкинга открывает новые возможности для киберпреступников». Согласно официальным

данным, в результате киберпреступлений в Узбекистане в 2021–2024 годах были похищены средства граждан на сумму свыше 1,9 трлн сумов, при этом 98% составляют преступления, связанные с банковскими картами [9].

Узбекские исследователи в области права отмечают важность комплексного подхода. Как указывается в научных публикациях Института законодательства и правовой политики при Олий Мажлисе, «борьба с киберпреступностью осложняется тем, что киберпреступники – это не обычные мошенники, а хорошо обученные программисты, которые скрываются за экраном своего компьютера». В связи с этим подчеркивается необходимость «проведения научных и социологических исследований для принятия мер по профилактике и предупреждению правонарушений с использованием современных технологий» [10].

При этом основную массу совершенных преступлений составляют мошенничества в сфере онлайн-кредитов. Однако не стоит недооценивать активность населения по использованию онлайн-услуг, учитывая их удобность и быстроту.

Профессора Бенуа Дюпон из Монреальского университета и Рутгер Лейкфелдт из Нидерландского института изучения преступности и правоприменения отмечают, что «киберпреступность в настоящее время представляет между 40 и 50% всех преступлений в индустриализованных обществах, что делает её основным типом преступности» [11].

Исследователи из Центра интернет-безопасности (CIS) подчеркивают эволюцию методов социальной инженерии: «Киберпреступники быстро адаптировали генеративный ИИ и большие языковые модели, что позволяет им создавать более персонализированные и убедительные атаки социальной инженерии». Они прогнозируют, что «2024–2025 годы станут периодом масштабного использования дипфейков голоса и видео против жертв» [12].

Эксперты компании KELA в своем отчете «Состояние киберпреступности 2025» отмечают трансформационный характер 2024 года: «От инфостилеров, компрометирующих миллионы учетных данных, до смены тактики вымогателей и роста киберпреступности на основе ИИ – злоумышленники находят новые способы эксплуатации уязвимостей» [13].

Аналитики SpyCloud обращают внимание на демократизацию киберпреступности: «Современная экосистема киберпреступности предлагает готовые решения – такие как Malware-as-a-Service – что делает легким для любого войти в игру. От криптеров до резидентных прокси, подпольный рынок демократизировал кибератаки, предоставляя инструменты взлома высокого уровня в руки менее квалифицированных пользователей» [14].

Учитывая вышеизложенное, в целях обеспечения защиты имущественных и неимущественных прав граждан, интересов общества и государства необходимо принять ряд неотложных комплексных мер в сфере защиты от киберпреступлений.

Принятие следующих технических мер представляется необходимым:

• Обеспечение безопасности персональных данных с применением методов шифрования и ведения реестра лиц, имеющих доступ к данным сведениям

• Установление обязательных правил по соблюдению требований кибербезопасности со стороны операторов, владеющих персональными данными

• Установление обязательного порядка отправления одноразового SMS-кода в зашифрованном виде при проведении онлайн денежных операций

• Установление соблюдения данных требований в качестве обязательных требований и условий лицензирования видов деятельности в данных отраслях

Учитывая недостаточность мер по предупреждению правонарушений в данной сфере, необходимо усиление ответственности за нарушение законодательства в сфере персональных данных:

• Предусмотреть порядок установления реальности изображения живого лица при проверке с помощью Face-ID контроля и взыскания ущерба вследствие несоблюдения требований обеспечения кибербезопасности со стороны оператора, владеющего персональными данными

• Ввести порядок возмещения материального ущерба по кибермошенничествам за счет банковско-кредитных и иных платежных организаций

• Внедрить оборотные штрафы для организаций, допустивших утечки персональных данных, по примеру законодательства Российской Федерации

Для реализации мер по предупреждению и раскрытию киберпреступлений следует:

• Создать новые подразделения по ресоциализации лиц, совершивших данные правонарушения, а также проводить научно-практические исследования по предупреждению киберпреступлений

• Обеспечить интеграцию баз данных правоохранительных органов с электронными базами банковско-кредитных организаций в целях обеспечения оперативности раскрытия подобных преступлений

• Расширить подготовку специализированных кадров в области кибербезопасности в Академии МВД, с учетом мнения замминистра экономики А. Хайдарова о необходимости «создать современную инфраструктуру и подготовить специалистов МВД и Генпрокуратуры»

• Обеспечить своевременное сообщение о совершенных киберпреступлениях и создание системы оперативного реагирования

Экспоненциальный рост киберпреступлений с использованием персональных данных и электронных платежных систем представляет собой критическую глобальную проблему, требующую немедленного комплексного вмешательства. Настоящее исследование демонстрирует, что масштаб и влияние киберпреступности продолжают расширяться как в развитых, так и в развивающихся странах, достигая беспрецедентных уровней ущерба.

Как справедливо отмечают международные эксперты, современная киберпреступность характеризуется профессионализацией, использованием искусственного интеллекта и демократизацией доступа к инструментам взлома. Предложенная трехкомпонентная система, объединяющая технические, правовые и организационные меры, предлагает холистический подход к предупреждению и обнаружению киберпреступлений.

Технические меры, сфокусированные на шифровании и контроле доступа, обеспечивают фундаментальную инфраструктуру безопасности. Правовые и нормативные реформы устанавливают необходимые рамки ответственности и механизмы компенсации жертвам. Организационные инициативы гарантируют эффективную реализацию через специализированные подразделения и межведомственное сотрудничество.

Реализация предложенных мер будет способствовать своевременному предупреждению и оперативному раскрытию киберпреступлений, в конечном итоге защищая права и интересы граждан в условиях все более цифровизирующегося общества. Будущие исследования должны быть сосредоточены на оценке эффективности внедренных мер и разработке адаптивных стратегий противодействия возникающим киберугрозам. Международное сотрудничество и обмен информацией между правоохранительными органами по всему миру остаются критически важными для решения транснационального характера киберпреступлений.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Varese F., Lavorgna A., Shortland A. The World Cybercrime Index // PLOS ONE. 2024. Vol. 19. № 4.
2. Federal Bureau of Investigation. Internet Crime Report 2024. Internet Crime Complaint Center (IC3), 2024.
3. Morgan S. Top 10 Cybersecurity Predictions and Statistics For 2024 // Cybersecurity Ventures. 2024.
4. Следственный департамент МВД Российской Федерации. Статистический отчет о IT-преступлениях в России. 2024.
5. F.A.C.C.T. Киберпреступность в России и СНГ, 2023–2024 гг. Тренды, аналитика, прогнозы. 2024.
6. Positive Technologies. Актуальные киберугрозы в странах СНГ 2023-2024. 2024.
7. Госдума Российской Федерации. Федеральный закон об усилении ответственности за утечки персональных данных. Ноябрь 2024.
8. Генеральная прокуратура Республики Узбекистан. Статистические данные о киберпреступлениях в Узбекистане. 2024.
9. Хайдаров А. Интервью телеканалу «Узбекистан 24» о киберпреступности. 2025.
10. Институт законодательства и правовой политики при Олий Мажлисе Республики Узбекистан. Перспективы правовой политики в области противодействия киберпреступности. 2024.
11. Dupont B., Fortin F., Leukfeldt R. Broadening our understanding of cybercrime and its evolution // Journal of Crime and Justice. 2024. Vol. 47. № 4. P. 435-439.
12. Center for Internet Security. 16 CIS Experts' Cybersecurity Predictions for 2024. 2024.
13. KELA. The State of Cybercrime 2025 Report. 2025.
14. SpyCloud. 2024 in Review: Cybercrime Deep Dive & Predictions for 2025. 2025.
15. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 № ЗРУ-764.