АКТУАЛЬНЫЕ ВОПРОСЫ ПРЕДОТВРАЩЕНИЯ, ВЫЯВЛЕНИЯ, РАСКРЫТИЯ И РАССЛЕДОВАНИЯ IT-ПРЕСТУПЛЕНИЙ

Гуламов Суннатали Суннатали угли
Академия Министерства внутренних дел Республики Узбекистан Преподаватель кафедры Криминалистических экспертиз, капитан
E-mail: sunnatalig@mail.ru
https://doi.org/10.5281/zenodo.20538573

ARTICLE INFO

Qabul qilindi: 26-may 2026 yil
Ma'qullandi: 28-may 2026 yil
Nashr qilindi: 30-may 2026 yil

KEYWORDS

информационные технологии, киберпреступность, IT-преступления, информационная безопасность, кибербезопасность, расследование преступлений, цифровые доказательства, Республика Узбекистан, противодействие преступности, банковское мошенничество.

ABSTRACT

в данной статье рассматриваются вопросы, связанные с борьбой против преступлений в сфере информационных технологий (далее – ИТ). Автором изучаются технологии и методы при расследовании преступлений в сфере ИТ.

Стремительное развитие информационных технологий и цифровая трансформация всех сфер общественной жизни создали принципиально новые вызовы для системы уголовного правосудия. Преступления, совершаемые с использованием ИТ-технологий, превратились в одну из наиболее динамично растущих и трудно выявляемых категорий противоправных деяний в глобальном масштабе. Для Республики Узбекистан, находящейся на этапе интенсивной цифровизации государственного управления, экономики и социальной сферы, обеспечение эффективного противодействия ИТ-преступлениям приобрело стратегическое значение для национальной безопасности и устойчивого развития. Цифровизация общества сопровождается не только позитивными преобразованиями, но и ростом угроз кибербезопасности, требующих адекватной правовой и институциональной реакции [1].

[1] Правовая политика в условиях цифровых вызовов: стратегия противодействия киберпреступности // Yuz.uz. — 2026. — 2 апреля. — URL: https://yuz.uz/ru/news/pravovaya-politika-v-usloviyakh-tsifrovykh-vyzovov-strategiya-protivodeystviya-kiberprestupnosti (дата обращения: 06.05.2026)

Цели настоящей статьи заключаются в комплексном анализе современного состояния ИТ-преступности в Узбекистане, рассмотрение наиболее острых проблем в сфере предотвращения, выявления, раскрытия

и расследования подобных преступлений, а также в определении приоритетных направлений совершенствования правовых

и организационных механизмов противодействия данной категории деяний.

Анализ статистических данных демонстрирует катастрофический рост киберпреступности в Узбекистане в последние годы. По информации МВД республики, за период с 2019 по 2024 год количество киберпреступлений увеличилось с 863 случаев до почти 59 тысяч, то есть рост составил более чем в 68 раз [2]. За пять лет (2021–2025) число киберпреступлений возросло с 4 865 до 62 440, что представляет собой увеличение в 11 раз [3; 4]. В 2024 году доля киберпреступлений в общей структуре преступности достигла 44,4% – это означает, что практически каждое второе преступление в стране совершается с использованием информационных технологий. В Ташкенте в 2025 году зафиксировано более 16 тысяч киберпреступлений, что свидетельствует о высокой концентрации ИТ-угроз в столичном регионе [5].

Общий материальный ущерб граждан от киберпреступлений за 2021–2025 годы превысил 3,7 трлн сумов (около 309,5 млн долларов США), при этом половина этой суммы – 1 трлн 890 млрд сумов (156,8 млн долларов) – приходится лишь на 11 месяцев 2025 года [6;7]. Эти цифры убедительно доказывают, что проблема приобрела характер реальной угрозы экономическому благосостоянию населения. По данным Global Organized Crime Index [8] 2025, Узбекистан занял 108-е место из 193 стран, опустившись на восемь позиций относительно предыдущего рейтинга, при этом эксперты особо отметили резкое увеличение числа кибератак на государственные органы и бизнес-структуры [9].

Система противодействия IT-преступлениям в Узбекистане претерпела существенные изменения. Ключевым этапом стало принятие Постановления Президента № ПП-153 от 30 апреля 2025 года «О мерах, направленных на дальнейшее

---

2 «Киберпреступность в Узбекистане выросла в 68 раз за пять лет: ущерб превысил 1,9 трлн сумов» // Anhor.uz. – 2025. – 29 мая. – URL: https://anhor.uz/news/cyberattack-3-2/ (дата обращения: 06.05.2026)

3 URL: https://uza.uz/uz/posts/v-2025-godu-raskryto-88-tysyachi-kiberprestupleniy_830958 (дата обращения: 07.05.2026)

4 УзА (Uza.uz). – 2025. – 24 декабря. – URL: https://uza.uz/ru/posts/v-rezultate-kiberprestupleniy-grazhdanam-byl-nanesen-uscherb-prevyshayuschiy-37-trilliona-sumov_799702 (дата обращения: 07.05.2026)

5 // Nuz.uz. – 2026. – 27 января. – URL: https://nuz.uz/2026/01/27/ya-reshil-vse-voprosy-v-etom-napravlenii-dlya-mvd-i-prokuratury-gde-rezultat-prezident-ukazal-na-proval-v-borbe-s-kiberprestupnostyu/ (дата обращения: 07.05.2026

6 // Kun.uz. – 2025. – 24 декабря. – URL: https://kun.uz/ru/news/2025/12/24/uzbekistansam-za-11-mesyatsev-nanesen-ushcherb-kiberprestupleniyami-na-1-trln-890-mlrd-sumov (дата обращения: 07.05.2026)

7 // УзА (Uza.uz). – 2025. – 24 декабря. – URL: https://uza.uz/ru/posts/v-rezultate-kiberprestupleniy-grazhdanam-byl-nanesen-uscherb-prevyshayuschiy-37-trilliona-sumov_799702 (дата обращения: 07.05.2026)

8 Индекс, который измеряет и ранжирует страны по распространённости организованной преступности и их устойчивости к ней // URL: https://en.wikipedia.org/wiki/Global_Organized_Crime_Index/ (дата обращения 07.05.2026)

9 / К. Сайтжанов // Kursiv Media Uzbekistan. – 2025. – 21 ноября. – URL: https://uz.kursiv.media/2025-11-21/uzbekistan-opustilsya-na-108-e-mesto-v-rejtinge-organizovannoj-prestupnosti/ (дата обращения: 07.05.2026)

усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий» [10]. Данный документ впервые на уровне нормативного акта высшей юридической силы комплексно урегулировал вопросы противодействия киберпреступности.

Еще одним важным дополнением стало Постановление Президента № ПП-371 от 11 декабря 2025 года «О мерах по совершенствованию системы государственного контроля в сферах информации и цифровых технологий», направленное на дальнейшее усиление государственного регулирования ИТ-сферы [11].

В августе 2025 года Центральный банк Узбекистана утвердил минимальные требования к информационной и кибербезопасности коммерческих банков. Согласно этому документу, банки и их филиалы обязаны сформировать специализированные службы информационной

и кибербезопасности, запрещена передача ИТ-инфраструктуры и систем безопасности на аутсорсинг, а информационные активы, базы данных и серверы должны размещаться только в собственных или государственных дата-центрах [12].

На институциональном уровне в системе МВД создан Центр кибербезопасности, а в регионах – управления по борьбе с киберпреступлениями. В 2025 году Центр и региональные управления раскрыли 8,8 тыс. киберпреступлений, что в 5,2 раза превышает показатель 2024 года. В дальнейшем планируется создание департамента по кибербезопасности в системе министерства внутренних дел.

Несмотря на принятые меры, система борьбы с ИТ-преступлениями раскрывает крайне низкий процент киберпреступности. По неопубликованным данным МВД Республики Узбекистан, этот показатель не достигает даже 8%. Иными словами, из каждых 12–13 совершённых киберпреступлений раскрывается лишь одно. Такая ситуация дискредитирует саму идею уголовно-правовой защиты граждан в цифровой сфере и создаёт у преступников ощущение безнаказанности.

Можно выделить несколько значимых причин низкой эффективности раскрываемости преступлений в сфере информационных технологий. К ним относятся: уязвимость банковских систем, низкая цифровая грамотность населения [13], кадровый дефицит и недостаток квалифицированных сотрудников, сложности работы с цифровыми доказательствами (такие международные организации как Интерпол и Европол разработали сложные протоколы, технологии и правовые механизмы для работы с цифровыми доказательствами, которые могут быть адаптированы к условиям

10 Постановление Президента Республики Узбекистан от 30 апреля 2025 г. № ПП-153 (полный текст) // Lex.uz. – URL: https://lex.uz/ru/docs/7511168 (дата обращения: 07.05.2026)

11 Постановление Президента Республики Узбекистан от 11 декабря 2025 г. № ПП-371 // Национальная база данных законодательства Республики Узбекистан. – URL: https://lex.uz (дата обращения: 08.05.2026)

12 // Kapital.uz. – 2025. – 21 августа. – URL: https://kapital.uz/bankam-zapretili-peredavat-it/ (дата обращения: 08.05.2026)

13 Селиванов В.Ю. Теоретические и правовые основы профилактики кибермошенничества / В.Ю. Селиванов // Zenodo. – 2025. – 1 ноября. – DOI: 10.5281/zenodo.17501237 261 с.

Узбекистана [14]. Также можно начать проведение обучающих семинаров для судей по вопросам допустимости цифровых доказательств в уголовном процессе [15]), рост новых видов угроз (использование искусственного интеллекта, дипфейков, облачных технологий [16]. Правовое реагирование на преступления в социальных сетях также остаётся недостаточно эффективным ввиду анонимности, цифровых манипуляций и трансграничного характера таких деяний [17]).

Крайне низкая раскрываемость и колоссальный нанесенный ущерб, свидетельствует о системном кризисе правовой охраны в сфере кибербезопасности, в связи с чем, предлагаются рекомендации для повышения уровня расследования и борьбы с ИТ-преступностью.

Институциональное укрепление – создание в системе МВД департамента по кибербезопасности – верное решение, но одного создания структур недостаточно. Необходимо кардинальное увеличение штатной численности квалифицированных кадров, оснащение их современной компьютерной и криминалистической техникой, создание региональных лабораторий цифровой криминалистики.

Кадровая подготовка – расширение набора в академию МВД по специализации «Деятельность по противодействию преступлениям в сфере цифровых технологий» до 500 и более курсантов ежегодно; введение обязательного курса по расследованию IT-преступлений в программы повышения квалификации всех следователей и дознавателей; организация стажировок сотрудников в зарубежных центрах кибербезопасности.

Диверсификация методов работы – внедрение проактивного подхода, включая анализ Big Data для выявления трендов киберпреступности; использование систем на основе ИИ для обнаружения аномальной активности в Сети; активное сотрудничество с провайдерами
и разработчиками ПО.

Международное взаимодействие – присоединение к Будапештской конвенции о киберпреступности — стратегический шаг, позволяющий получать правовую помощь и обмениваться информацией с более чем 60 странами; заключение двусторонних соглашений с профильными ведомствами стран СНГ и дальнего зарубежья [18].

Научно-методическое обеспечение – разработка и внедрение методических рекомендаций по расследованию отдельных видов IT-преступлений; создание единой базы данных о способах совершения

---

14 Normurodova B.X. The experience of INTERPOL and EUROPOL in collecting and analyzing digital evidence: practical significance for Uzbekistan / B.X. Normurodova // Scienceproblems.uz. – 2025. – Ч. 8. – с. 230–236

15 // Правоохранительная академия Республики Узбекистан. – 2025. – URL: https://proacademy.uz/ru/news/view?alias=2873 (дата обращения: 08.05.2026)

16 // CSU.uz. – 2026. – 6 апреля. – URL: https://csu.uz/ru/news/raqamli-dunyo-xavf-ostida-2025-yilda-kiberjinoyatlar-qay-darajaga-yetdi (дата обращения: 08.05.2026)

17 Ахорова H.X. Zamonaviy o‘g‘irlik jinoyatlari: kompyuter vositalari orqali sodir etiladigan holatlarning jinoyat-huquqiy tahlili / H.X. Ахорова // Вестник НУУз. – 2025. – Т. 1. – № 1.4. – С. 58–60. – DOI: 10.69617/nuuz.v1i1.4.7177

18 Ахорова H.X. Zamonaviy o‘g‘irlik jinoyatlari: kompyuter vositalari orqali sodir etiladigan holatlarning jinoyat-huquqiy tahlili / H.X. Ахорова // Вестник НУУз. – 2025. – Т. 1. – № 1.4. – С. 58–60. – DOI: 10.69617/nuuz.v1i1.4.7177

киберпреступлений; реформирование системы цифровой криминалистики в экспертных подразделениях.

Цифровая трансформация Узбекистана должна сопровождаться надёжной правовой защитой граждан и бизнеса от киберугроз. Иначе достижения цифровизации могут быть сведены на нет страхом населения перед мошенничеством и потерей сбережений.

Заключение: Стремительная цифровизация Республики Узбекистан, наряду с очевидными социально-экономическими преимуществами, повлекла за собой критический рост угроз в сфере кибербезопасности. Статистические данные за 2019–2025 годы демонстрируют лавинообразное увеличение масштабов ИТ-преступности, доля которой в общей структуре правонарушений приблизилась к 50%, а нанесенный гражданам материальный ущерб исчисляется триллионами сумов. Несмотря на своевременную реакцию государства, выраженную в принятии профильных указов (ПП-153, ПП-371), ужесточении требований Центробанка к коммерческим банкам и создании Центра кибербезопасности МВД, текущая эффективность раскрытия таких преступлений остается критически низкой (менее 8%). Основными деструктивными факторами выступают уязвимость банковских систем, дефицит квалифицированных кадров, низкая цифровая грамотность населения, а также отставание методологии работы с цифровыми доказательствами от темпов развития ИТ-технологий (включая ИИ и дипфейки).

Для преодоления системного кризиса в сфере правовой охраны цифрового пространства необходим переход к проактивной стратегии, включающей:

- **Институциональное и кадровое усиление:** создание полноценного Департамента кибербезопасности МВД, кратное увеличение штата и масштабирование подготовки профильных специалистов в Академии МВД.
- **Технологическую модернизацию:** внедрение систем анализа Big Data и искусственного интеллекта для выявления аномальной сетевой активности, создание региональных цифровых лабораторий.
- **Международную интеграцию:** присоединение к Будапештской конвенции о киберпреступности для оперативного трансграничного взаимодействия.

Без реализации этих комплексных мер дальнейшее развитие цифровой экосистемы страны неизбежно столкнется с кризисом доверия со стороны населения и бизнеса, что ставит под угрозу экономическую стабильность и национальную безопасность государства в целом.

Литература:

1. Правовая политика в условиях цифровых вызовов: стратегия противодействия киберпреступности // Yuz.uz. — 2026. — 2 апреля. — URL: https://yuz.uz/ru/news/pravovaya-politika-v-usloviyakh-tsifrovykh-vyzovov-strategiya-protivodeystviya-kiberprestupnosti (дата обращения: 06.05.2026)
2. Киберпреступность в Узбекистане выросла в 68 раз за пять лет: ущерб превысил 1,9 трлн сумов» // Anhor.uz. – 2025. – 29 мая. – URL: https://anhor.uz/news/cyberattack-3-2/ (дата обращения: 06.05.2026)
3. URL: https://uza.uz/uz/posts/v-2025-godu-raskryto-88-tysyachi-kiberprestupleniy_830958 (дата обращения: 07.05.2026)

4. УзА (Uza.uz). – 2025. – 24 декабря. – URL: https://uza.uz/ru/posts/v-rezultate-kiberprestupleniy-grazhdanam-byl-nanesen-uscherb-prevyshayuschiy-37-trilliona-sumov_799702 (дата обращения: 07.05.2026)
5. // Nuz.uz. – 2026. – 27 января. – URL: https://nuz.uz/2026/01/27/ya-reshil-vse-voprosy-v-etom-napravlenii-dlya-mvd-i-prokuratury-gde-rezultat-prezident-ukazal-na-proval-v-borbe-s-kiberprestupnostyu/ (дата обращения: 07.05.2026
6. // Kun.uz. – 2025. – 24 декабря. – URL: https://kun.uz/ru/news/2025/12/24/uzbekistansam-za-11-mesyatsev-nanesen-ushcherb-kiberprestupleniyami-na-1-trln-890-mlrd-sumov (дата обращения: 07.05.2026)
7. // УзА (Uza.uz). – 2025. – 24 декабря. – URL: https://uza.uz/ru/posts/v-rezultate-kiberprestupleniy-grazhdanam-byl-nanesen-uscherb-prevyshayuschiy-37-trilliona-sumov_799702 (дата обращения: 07.05.2026)
8. Индекс, который измеряет и ранжирует страны по распространённости организованной преступности и их устойчивости к ней // URL: https://en.wikipedia.org/wiki/Global_Organized_Crime_Index/ (дата обращения 07.05.2026)
9. / К. Сайтжанов // Kursiv Media Uzbekistan. – 2025. – 21 ноября. – URL: https://uz.kursiv.media/2025-11-21/uzbekistan-opustilsya-na-108-e-mesto-v-rejtinge-organizovannoj-prestupnosti/ (дата обращения: 07.05.2026)
10. Постановление Президента Республики Узбекистан от 30 апреля 2025 г. № ПП-153 (полный текст) // Lex.uz. – URL: https://lex.uz/ru/docs/7511168 (дата обращения: 07.05.2026)
11. // Advice.uz. – 2026. – 13 марта. – URL: https://advice.uz/ru/news/3063 (дата обращения: 07.05.2026)
12. Постановление Президента Республики Узбекистан от 11 декабря 2025 г. № ПП-371 // Национальная база данных законодательства Республики Узбекистан. – URL: https://lex.uz (дата обращения: 08.05.2026)
13. // Kapital.uz. – 2025. – 21 августа. – URL: https://kapital.uz/bankam-zapretili-peredavat-it/ (дата обращения: 08.05.2026)
14. Селиванов В.Ю. Теоретические и правовые основы профилактики кибермошенничества / В.Ю. Селиванов // Zenodo. – 2025. – 1 ноября. – DOI: 10.5281/zenodo.17501237 261 с.
15. Normurodova B.X. The experience of INTERPOL and EUROPOL in collecting and analyzing digital evidence: practical significance for Uzbekistan / B.X. Normurodova // Scienceproblems.uz. – 2025. – Ч. 8. – с. 230–236
16. // Правоохранительная академия Республики Узбекистан. – 2025. – URL: https://proacademy.uz/ru/news/view?alias=2873 (дата обращения: 08.05.2026)
17. // CSU.uz. – 2026. – 6 апреля. – URL: https://csu.uz/ru/news/raqamli-dunyo-xavf-ostida-2025-yilda-kiberjinoyatlar-qay-darajaga-yetdi (дата обращения: 08.05.2026)
18. Ахорова Н.Х. Zamonaviy o‘g‘irlik jinoyatlari: kompyuter vositalari orqali sodir etiladigan holatlarning jinoyat-huquqiy tahlili / Н.Х. Ахорова // Вестник НУУз. – 2025. – Т. 1. – № 1.4. – С. 58–60. – DOI: 10.69617/nuuz.v1i1.4.7177