LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН: ПРАВОВЫЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ

Тухтасинов Искандар Туланбой Угли

Студент Ташкентского государственного юридического университета

Аннотация: *В статье рассматриваются актуальные вопросы профилактики киберпреступности в Республике Узбекистан в условиях ускоренной цифровой трансформации общества. Анализируются действующая нормативно-правовая база, институциональные механизмы противодействия киберугрозам, а также международный опыт. Предложены практические рекомендации по совершенствованию системы кибербезопасности страны.*

Ключевые слова*: киберпреступность, кибербезопасность, Узбекистан, цифровизация, профилактика, информационная безопасность, правовое регулирование.*

1. ВВЕДЕНИЕ

Стремительное развитие информационно-коммуникационных технологий (ИКТ) в XXI веке породило принципиально новый вид угроз — киберпреступность. По данным Cybersecurity Ventures, мировой ущерб от кибератак к 2025 году достиг астрономической отметки в 10,5 триллиона долларов США в год, что превышает совокупный ВВП большинства государств мира.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 4(2026) / ISSN 3030-3052 Available at www.uznauka.uz

Республика Узбекистан, активно реализующая масштабную программу «Цифровой Узбекистан — 2030», оказалась в эпицентре этих вызовов. Интенсивная цифровизация государственного управления, банковской сферы, здравоохранения и образования неизбежно расширяет поверхность атаки для злоумышленников. По оценкам Государственного центра кибербезопасности Узбекистана, в 2023 году в стране было зафиксировано свыше 140 000 кибератак на объекты критической информационной инфраструктуры.

Профилактика киберпреступности приобретает стратегическое значение для обеспечения национальной безопасности, устойчивого экономического развития и защиты прав граждан в цифровом пространстве. Именно поэтому данная проблематика требует глубокого научного осмысления и выработки системных практических решений.

2. ПОНЯТИЕ И КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ

Киберпреступность — это совокупность противоправных деяний, совершаемых с использованием компьютерных систем, сетей или против них, причиняющих ущерб физическим лицам, организациям или государству. Конвенция Совета Европы о киберпреступности (Будапештская конвенция, 2001) классифицирует киберпреступления по четырём основным категориям.

Первая категория — преступления против конфиденциальности, целостности и доступности компьютерных данных и систем: несанкционированный доступ (хакинг), перехват данных, вмешательство в работу систем. Вторая — компьютерные мошенничества и подлоги, включая

фишинг, создание вредоносного программного обеспечения, кражу персональных данных.

Третья категория охватывает преступления, связанные с содержанием: распространение запрещённых материалов, экстремистского контента, пропаганда терроризма в сети Интернет. Четвёртая — нарушения авторских и смежных прав в цифровой среде: незаконное копирование программного обеспечения, пиратство контента.

В Узбекистане наибольшую распространённость получили финансовые киберпреступления (интернет-мошенничество, кражи с банковских счетов), составляющие около 67% от общего числа зарегистрированных случаев. На втором месте — несанкционированный доступ к информационным системам (18%), на третьем — распространение вредоносного программного обеспечения (9%).

3. ПРАВОВАЯ ОСНОВА ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УЗБЕКИСТАНЕ

Правовой фундамент противодействия киберпреступности в Республике Узбекистан формировался поэтапно. Базовым документом является Закон Республики Узбекистан «Об информатизации» (1993, в редакции 2003 года), закрепивший основные понятия и принципы правового регулирования информационных отношений.

Принципиальным шагом вперёд стало принятие Закона «Об информационной безопасности» от 15 апреля 2022 года, который впервые в национальном законодательстве комплексно урегулировал вопросы защиты

критической информационной инфраструктуры, установил требования к субъектам кибербезопасности и определил полномочия уполномоченных органов. Законом введена обязательная сертификация средств защиты информации и лицензирование деятельности в сфере кибербезопасности.

Уголовный кодекс Узбекистана содержит специальную главу XXX «Преступления в сфере информационных технологий», включающую статьи 278–285, предусматривающие ответственность за неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ, нарушение правил эксплуатации ЭВМ и другие деяния. Санкции варьируются от штрафа до лишения свободы сроком до восьми лет.

Указом Президента Республики Узбекистан от 19 июля 2021 года №УП-6268 «О мерах по ускоренному развитию цифровой экономики в Республике Узбекистан» кибербезопасность признана приоритетом государственной политики, а Государственный центр кибербезопасности наделён дополнительными полномочиями по координации профилактической деятельности.

4. ИНСТИТУЦИОНАЛЬНЫЕ МЕХАНИЗМЫ ПРОФИЛАКТИКИ

Система институтов, осуществляющих профилактику киберпреступности в Узбекистане, включает несколько ключевых структур, каждая из которых выполняет специфические функции в едином координационном механизме.

Государственный центр кибербезопасности при Министерстве по развитию информационных технологий и коммуникаций является главным

оперативным органом в данной сфере. В его структуре функционирует национальная группа реагирования на компьютерные инциденты — CERT (UZ-CERT), осуществляющая мониторинг киберпространства в режиме 24/7 и координирующая реагирование на инциденты.

Министерство внутренних дел располагает специализированным Управлением по борьбе с преступлениями в сфере информационных технологий (Кибер МВД), которое занимается расследованием киберпреступлений и проводит профилактические рейды в интернет-кафе и публичных точках доступа.

Агентство по защите персональных данных, учреждённое в 2020 году, осуществляет контроль за соблюдением законодательства о персональных данных и проводит просветительские кампании для граждан и бизнеса. Важную роль в профилактике играют также коммерческие банки, обязанные внедрять многофакторную аутентификацию и системы антифрода в соответствии с требованиями Центрального банка Узбекистана.

5. АКТУАЛЬНЫЕ УГРОЗЫ И ТРЕНДЫ

Ландшафт киберугроз в Узбекистане и регионе в целом динамично эволюционирует. Эксперты выделяют несколько ключевых трендов, определяющих современный облик киберпреступности.

Во-первых, резкий рост атак на мобильный банкинг и платёжные системы. С распространением смартфонов и сервисов мобильных платежей злоумышленники переориентировались на кражу учётных данных мобильных приложений посредством поддельных приложений, SMS-

фишинга (смишинга) и атак типа SIM-swap. По данным Центрального банка, в 2023 году ущерб от мошенничества в системах электронных платежей составил более 45 миллиардов сумов.

Во-вторых, атаки с использованием программ-вымогателей (ransomware) на государственные организации и объекты критической инфраструктуры. Такие группировки, как LockBit и Clop, действуют глобально, и Центральная Азия не является исключением. Шифрование данных и требование выкупа ставит под угрозу непрерывность работы государственных сервисов.

В-третьих, использование технологий искусственного интеллекта для создания дипфейков и автоматизации фишинговых атак. Генеративный ИИ позволяет создавать убедительные поддельные голоса и видео для обмана граждан и руководителей организаций, что существенно снижает эффективность традиционных методов верификации.

6. МЕЖДУНАРОДНЫЙ ОПЫТ И СОТРУДНИЧЕСТВО

Эффективная профилактика киберпреступности невозможна без активного международного взаимодействия, поскольку киберпреступники действуют вне государственных границ. Узбекистан последовательно наращивает международное сотрудничество в данной сфере.

В рамках Шанхайской организации сотрудничества (ШОС) функционирует специализированная структура — Региональная антитеррористическая структура, в деятельность которой интегрированы вопросы противодействия киберэкстремизму. В 2022 году государства —

члены ШОС подписали Соглашение о сотрудничестве в области обеспечения международной информационной безопасности.

Узбекистан активно сотрудничает с Интерполом в рамках операций по противодействию киберпреступности. Участие в операциях GOLDFISH ALPHA и LYREBIRD позволило перенять передовые методики расследования и выработать эффективные механизмы трансграничного взаимодействия правоохранительных органов.

Значительный вклад в развитие потенциала страны вносит Агентство ЕС по кибербезопасности (ENISA), оказывающее техническую помощь и проводящее совместные учения. Программа USAID Digital Central Asia также направлена на укрепление кибербезопасности государств региона, включая Узбекистан.

7. РЕКОМЕНДАЦИИ ПО СОВЕРШЕНСТВОВАНИЮ ПРОФИЛАКТИКИ

На основании проведённого анализа можно сформулировать следующий комплекс рекомендаций по совершенствованию системы профилактики киберпреступности в Республике Узбекистан.

Первое направление — законодательное. Необходимо присоединение Узбекистана к Будапештской конвенции, что позволит гармонизировать национальное законодательство с международными стандартами и расширить возможности для получения доказательств из зарубежных юрисдикций. Также требуется разработка специального закона о

кибербезопасности критической инфраструктуры с чёткими требованиями к уведомлению об инцидентах.

Второе направление — образовательное. Внедрение обязательного курса «Цифровая гигиена и кибербезопасность» во всех общеобразовательных школах и вузах страны позволит сформировать культуру безопасного поведения в цифровой среде уже в молодом возрасте. Передовой мировой опыт убедительно демонстрирует эффективность данного подхода.

Третье направление — технологическое. Создание национальной платформы обмена информацией об угрозах для оперативного взаимодействия государственных органов, банков и телекоммуникационных компаний позволит существенно сократить время реагирования на инциденты. Внедрение системы раннего предупреждения на основе методов машинного обучения для выявления аномального сетевого трафика также является приоритетной задачей.

Четвёртое направление — просветительское. Регулярные национальные кампании по повышению осведомлённости граждан (по образцу Европейского месяца кибербезопасности), охватывающие все категории населения, создадут устойчивый иммунитет общества к социальной инженерии и фишингу.

8. ЗАКЛЮЧЕНИЕ

Профилактика киберпреступности в Республике Узбекистан является комплексной задачей, требующей синхронизированных усилий государства,

гражданского общества, бизнеса и международных партнёров. Страна обладает прочной нормативно-правовой базой и институциональными механизмами, однако стремительная эволюция угроз требует постоянной адаптации и опережающего развития.

Ключевыми приоритетами на среднесрочную перспективу должны стать: углубление международного сотрудничества, формирование культуры кибербезопасности через систему образования, технологическая модернизация систем защиты критической инфраструктуры и развитие национального кадрового потенциала в области кибербезопасности.

Убеждены, что последовательная реализация предложенных мер позволит Узбекистану занять достойное место в рейтинге Глобального индекса кибербезопасности МСЭ и обеспечить надёжную защиту цифровых активов государства, бизнеса и граждан в условиях четвёртой промышленной революции.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон Республики Узбекистан «Об информатизации» от 11 декабря 2003 г. № 560-II // Национальная база данных законодательства Узбекистана. — URL: https://lex.uz/docs/166693

2. Закон Республики Узбекистан «Об информационной безопасности» от 15 апреля 2022 г. № ЗРУ-764 // Национальная база данных законодательства Узбекистана. — URL: https://lex.uz/docs/5993218

3. Указ Президента Республики Узбекистан от 19 июля 2021 г. № УП-6268 «О мерах по ускоренному развитию цифровой экономики в Республике Узбекистан» // Национальная база данных законодательства Узбекистана. — URL: https://lex.uz/docs/5514949

4. Касымов О.Х. Классификация компьютерных преступлений в законодательстве Республики Узбекистан // Вестник ТашГЮУ. — 2022. — № 3. — С. 45–52.

5. Государственный центр кибербезопасности Республики Узбекистан. Ежегодный отчёт о состоянии кибербезопасности — 2023. — Ташкент, 2024. — 64 с. — URL: https://csec.uz

6. Агентство по защите персональных данных Республики Узбекистан. Отчёт о деятельности за 2022–2023 годы. — Ташкент, 2023. — 48 с.

7. Центральный банк Республики Узбекистан. Обзор рисков в сфере цифровых платежей за 2023 год. — Ташкент, 2024. — 36 с.

8. Council of Europe. Convention on Cybercrime (ETS No. 185). — Budapest, 2001. — URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

9. Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. — Cybercrime Magazine, 2020. — URL: https://cybersecurityventures.com

10. World Economic Forum. Global Cybersecurity Outlook 2024. — Geneva: WEF, 2024. — 56 p. — URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024/

11. ITU. Global Cybersecurity Index 2024. — Geneva: International Telecommunication Union, 2024. — 148 p. — URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

12. ENISA. European Cybersecurity Month 2023 Report. — Heraklion: ENISA, 2023. — 32 p. — URL: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-month

13. USAID. Digital Central Asia-South Asia Program. — 2023. — URL: https://www.usaid.gov/central-asia-regional/digital-casa

14. Шанхайская организация сотрудничества. Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. — Самарканд, 2022.