КИБЕРПРЕСТУПНОСТЬ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ: КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА, ДЕТЕРМИНАНТЫ И ИННОВАЦИОННЫЕ МЕТОДЫ ПРОФИЛАКТИКИ ПРАВОНАРУШЕНИЙ

Автор: *Адхамова Сугдиёна Ойбек кизи*

Место учёбы: *курсант Академии МВД Республики Узбекистан*

Аннотация: Настоящая статья посвящена системному криминологическому и уголовно-правовому анализу феномена киберпреступности как одной из наиболее динамичных угроз национальной и международной безопасности. В работе исследуются ключевые детерминанты цифровой преступности, специфика личности киберпреступника и особенности проявления цифровой виктимности. Особое внимание уделено анализу передового опыта, а также практической роли института «Махаллинской семерки» в реализации проактивных методов ранней профилактики киберправонарушений в рамках Стратегии «Узбекистан – 2030».

Ключевые слова: киберпреступность, информационная безопасность, цифровая гигиена, ранняя профилактика, социальная инженерия, фишинг, махаллинская семерка, искусственный интеллект.

1. ВВЕДЕНИЕ (INTRODUCTION)

Глобальная архитектура XXI века характеризуется тотальным проникновением информационно-коммуникационных технологий (ИКТ) во все страты жизнедеятельности государства, общества и личности. Переход к концепциям «Цифрового правительства», «Умного города» (Smart City) и форсированное развитие цифровой экономики, предусмотренное ***комплексной государственной программой «Цифровой Узбекистан - 2026»,*** открывают беспрецедентные возможности для социально-экономического прогресса. Однако обратной стороной технологической эволюции стало

зарождение и экспоненциальный рост киберпреступности — принципиально новой, высокотехнологичной формы противоправной деятельности, стирающей физические и юрисдикционные границы государств.

Президент Республики Узбекистан Шавкат Мирзиёев, обозначая ключевые приоритеты модернизации правоохранительной системы, подчеркивал:

«Обеспечение безопасности в киберпространстве, защита информационных систем государственных органов, бизнеса и, самое главное, защита личных данных и финансовых средств наших граждан от посягательств киберпреступников — это неотъемлемое условие стабильности Нового Узбекистана. Мы обязаны кардинально перестроить систему профилактики правонарушений, внедрив в неё интеллектуальные технологии и подходы опережающего реагирования» [1].

Современная киберпреступность перестала быть сугубо маргинальным явлением, реализуемым программистами-одиночками. Сегодня это высокоорганизованная, глубоко законспирированная и транснациональная индустрия, обладающая колоссальными финансовыми ресурсами и кооптирующая последние достижения науки: от генеративного искусственного интеллекта и дипфейк-технологий до распределенных реестров и методов скрытого сетевого шифрования.

Классические методы борьбы с преступностью, ориентированные на материальные следы преступления и локализованные пространственно-временные рамки, демонстрируют ограниченную эффективность в цифровой среде. В этой связи перед отечественной криминологической наукой встает императивная задача — переосмыслить каузальный комплекс киберпреступности, сформировать актуальную типологию цифровых девиаций и выстроить целостную, эшелонированную систему ранней профилактики.

2. МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ (RESEARCH METHODOLOGY)

Изучение столь сложного, динамичного и латентного феномена, как киберпреступность, потребовало применения диверсифицированного научно-методологического инструментария, находящегося на стыке юриспруденции, компьютерных наук, социологии и деликтологии. Применялся системно-структурный и криминологический анализ:для исследования внутренней архитектуры киберпреступности, выявления устойчивых связей между её элементами и моделирования каузальных комплексов, детерминирующих цифровые правонарушения. Статистико-компаративный метод позволил проанализировать эмпирическую базу данных Центра кибербезопасности МВД Республики Узбекистан, проследить динамику и структуру ИТ-преступлений за последние годы, а также сопоставить их с общемировыми тенденциями. Метод цифрового психологического профайлинга использовался для изучения поведенческих актов пользователей в сети, экспликации индикаторов манипулятивной уязвимости и признаков латентной цифровой виктимности. Сравнительно-правовой метод применялся для сопоставления нормативно-правовой базы Республики Узбекистан (в частности, Закона РУз «О кибербезопасности», Уголовного кодекса РУз) с международными конвенциями и стандартами (Будапештская конвенция о киберпреступности, регуляторные акты ЕС и ШОС).

3. ТЕОРЕТИКО-ПРАВОВАЯ РЕФЛЕКСИЯ КИБЕРУГРОЗ В ТРУДАХ УЧЕНЫХ АКАДЕМИИ МВД (LITERATURE REVIEW)

Теоретическое осмысление криминологических проблем информационного общества и уголовно-правовой охраны компьютерной информации получило глубокое развитие в трудах классиков узбекистанской юриспруденции — профессора И. Исмаилова [2] и академика М. Х. Рустамбаева [3]. Вопросы классификации составов преступлений против информационной безопасности и их отграничения от смежных

правонарушений детально исследованы в монографиях профессора Х. Р. Очилова [4].

Вместе с тем современные реалии требуют более узких, специализированных подходов, которые активно разрабатываются профессорско-преподавательским составом Академии МВД Республики Узбекистан. Начальник кафедры криминологии Академии МВД, профессор Ш. Т. Икрамов внес весомый теоретический вклад в изучение генезиса цифровой девиации. Профессор Ш. Т. Икрамов вводит в научный оборот концепт «виртуального криминогенного пространства», доказывая, что «цифровая среда функционирует по специфическим законам, где отсутствие прямого физического контакта между преступником и жертвой нивелирует классические механизмы психологического сдерживания (страх, эмпатию, стыд), что провоцирует стремительную криминализацию лиц, ранее не демонстрировавших девиантного поведения в реальной жизни» [5, с. 76].

Фундаментальное прикладное значение для построения действующей системы выявления и нейтрализации киберугроз на допреступной стадии имеют исследования старшего преподавателя Академии МВД Республики Узбекистан З. Шаумарова [6; 7; 8]. Специализируясь на цифровой юридической психологии и виктимологии, З. Шаумаров впервые детально описал когнитивные триггеры, используемые киберпреступниками при реализации методов социальной инженерии.

В своих научных изысканиях З. Шаумаров отмечает: «Успех киберпреступления в 80% случаев обусловлен не технологической изощренностью вредоносного софта, а эксплуатацией базовых психологических уязвимостей человеческой психики — дефицита времени, алчности, страха перед авторитетом власти или банального сострадания. Ранняя профилактика должна быть направлена не на блокировку железных серверов, а на формирование когнитивного иммунитета личности» [6, с. 63]. Разработанные автором методики психологического профайлинга интернет-

пользователей внедрены в практическую деятельность подразделений правоприменения и пробации [8, с. 104].

Административно-правовые рамки цифровой гигиены, регулирование деятельности интернет-провайдеров и алгоритмы межведомственного взаимодействия субъектов кибербезопасности получили подробное отражение в трудах доцента Академии МВД Б. Х. Пулатова [9, с. 147].

4. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА И КЛАССИФИКАЦИЯ КИБЕРПРЕСТУПЛЕНИЙ (TYPOLOGY OF CYBERCRIMES)

Научно обоснованная профилактика невозможна без четкой стратификации объекта воздействия. В современной криминологической доктрине киберпреступность классифицируется на три укрупненных блока. Во первых это цифровые корыстные преступления (Cyber-enabled crimes). К данной категории относятся преступления, где компьютерные сети выступают главным инструментом завладения чужим имуществом. Наиболее распространенными паттернами в Узбекистане являются **фишинг (phishing)** это создание точных цифровых дубликатов веб-ресурсов (банковских приложений, маркетплейсов, единого портала госуслуг), целью которых является перехват аутентификационных данных пользователей и **вишинг (vishing)** телефонное мошенничество с использованием методов социальной инженерии, когда злоумышленники маскируются под сотрудников службы безопасности банков («Халк Банк», «Асакабанк» и др.) или правоохранительных органов для получения SMS-кодов доступа к картам Humo и Uzcard. Преступления против информационной безопасности (Cyber-dependent crimes) это равонарушения, которые могут быть совершены исключительно в ИТ-сфере: несанкционированный доступ к охраняемой законом компьютерной информации, модификация данных, проведение разрушительных DDoS-атак на критическую информационную инфраструктуру, распространение вредоносного программного обеспечения

(включая вирусы-вымогатели семейства *Ransomware*). Киберпреступления против общественной безопасности и морали, то есть использование цифрового пространства для координации террористической деятельности, вербовки граждан в деструктивные религиозные секты, распространения порнографических материалов, пропаганды суицидального поведения среди несовершеннолетних, а также кибербуллинг и цифровое вымогательство.

5. ДЕТЕРМИНАНТЫ КИБЕРПРЕСТУПНОСТИ (CAUSAL COMPLEX)

Каузальный комплекс киберпреступности представляет собой сложную систему объективных и субъективных факторов, стимулирующих развитие данной криминальной сферы. Технологические детерминанты анонимизация и трансграничность, что означает использование технологий VPN, прокси-серверов, шифрованных браузеров (Tor) и анонимных криптовалютных транзакций (Monero, Bitcoin) создает у преступников чувство тотальной неуязвимости перед правосудием. Либо асимметрия защиты и нападения стоимость реализации кибератаки (покупка фишингового скрипта или аренда ботнета) несоизмеримо ниже, чем затраты государства и коммерческих структур на выстраивание комплексных систем информационной безопасности. Ещё и существуют социально-экономические детерминанты это может быть цифровой разрыв в правосознании темпы коммерциализации интернета опережают уровень правового воспитания граждан. Общество активно пользуется цифровыми финансовыми услугами, не обладая при этом элементарными навыками цифровой гигиены и высокая доходность при минимальных рисках что повышает возможность мгновенного обогащения за счет кражи средств с тысяч счетов одновременно привлекает в киберкриминал интеллектуальную молодежь, не нашедшую легальных способов высокооплачиваемой самореализации на рынке труда. Психолого-виктимологические детерминанты согласно исследованиям З. Шаумарова, ключевым фактором выступает «виртуальная инфантильность» жертв [7, с.

119]. Граждане в виртуальной среде демонстрируют уровень доверия к незнакомцам, который никогда бы не проявили в реальной жизни. Преступники успешно эксплуатируют такие триггеры, как «искусственный дефицит времени» (например: *«Ваша карта будет заблокирована через 2 минуты, если вы не назовете код»*) или «эффект авторитета» (*«Звонит старший следователь прокуратуры»*).

6. ИННОВАЦИОННАЯ СИСТЕМА РАННЕЙ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПЛЕНИЙ В РЕСПУБЛИКЕ УЗБЕКИСТАН (INNOVATIVE PREVENTION)

В соответствии с Концепцией общественной безопасности Республики Узбекистан, ранняя профилактика киберпреступлений строится на упреждении угроз и децентрализации превентивного воздействия. Модель разделена на три взаимосвязанных контура. Первый из них превентивный ИИ-мониторинг медиапространства, подразделения Центра кибербезопасности МВД РУз осуществляют непрерывный автоматизированный аудит национального сегмента сети Интернет. Развернутые нейросетевые алгоритмы способнывыявлять факты массовой автоматической регистрации подозрительных доменных имен, схожих до степени смешения с брендами банков и госорганов (предотвращение фишинга), блокировать в режиме реального времени автоматизированные рассылки вредоносных ссылок в мессенджерах и выявлять латентные интернет-сообщества, занимающиеся торговлей персональными данными граждан. Во вторых это экосистема «Махаллинской семерки» как первичный рубеж защиты. В рамках реализации Постановления Президента № ПП-10 от 20 января 2024 года, профилактика киберпреступлений была успешно интегрирована в общинную структуру махалли [12]. Были внедрены инспектор профилактики ОВД и Лидер молодежи, они осуществляют поквартирный обход, выявляя одиноких престарелых граждан и подростков — две наиболее уязвимые категории. Они проводят практический инструктаж по настройке двухфакторной

аутентификации в мессенджерах и разъясняют правила безопасности при использовании банковских приложений и женский активист махалли, которая фокусируется на выявлении фактов семейно-бытового кибершантажа, сталкинга и буллинга в отношении женщин в социальных сетях, организуя их своевременную правовую и психологическую защиту совместно с социальными работниками Центра «Инсон».

7. СИСТЕМНЫЕ ПРОБЛЕМЫ И БАРЬЕРЫ В СФЕРЕ КИБЕРПРЕВЕНЦИИ (SYSTEMIC PROBLEMS)

Несмотря на достигнутые успехи, криминологический мониторинг позволяет выделить ряд нерешенных проблем во первых это законодательное отставание от темпов развития технологий. Скорость появления новых модификаций киберпреступлений (например, использование технологии *Deepfake* для подделки биометрических данных или голоса близких родственников жертвы) превышает скорость криминализации данных деяний в Уголовном кодексе. Требуется непрерывная оптимизация диспозиций уголовно-правовых норм. Во вторых международно-правовой тупик деанонимизации. Поскольку большинство организаторов фишинговых платформ и операторов вирусов-вымогателей физически дислоцируются за пределами Республики Узбекистан, правоохранительные органы сталкиваются со сложными бюрократическими барьерами при попытках получения оперативной информации от зарубежных хостинг-провайдеров и регистраторов доменов. И в третих низкий уровень базовой ИТ-компетентности сотрудников первичного звена. Рядовые инспекторы профилактики на местах не всегда обладают достаточным уровнем технических знаний для квалифицированного консультирования граждан по сложным вопросам кибербезопасности, что обусловливает необходимость реформирования системы их переподготовки [5, с. 82].

8. ПЕРСПЕКТИВЫ РАЗВИТИЯ СИСТЕМЫ ЦИФРОВОЙ ПРОФИЛАКТИКИ (FUTURE PROSPECTS)

Для радикального снижения уровня киберпреступности в Новом Узбекистане авторами предлагается комплекс стратегических мер:

a. Создание государственной платформы «Антифишинг.уз» Необходимо запустить общенациональный интерактивный краудсорсинговый портал, куда любой гражданин Узбекистана в один клик сможет отправить подозрительную ссылку, SMS-сообщение или телефонный номер мошенника. Система на базе ИИ должна мгновенно проводить автоматический анализ ресурса и, в случае подтверждения угрозы, веерно блокировать доступ к нему со всех провайдеров республики в течение 5–10 минут.

b. Внедрение школьного компонента «Цифровая гигиена и медиаправо». Совместно с Министерством дошкольного и школьного образования необходимо разработать и внедрить в обязательную школьную программу предмет (или сквозной модуль), направленный на изучение основ информационной безопасности, ответственности за кибердевиации и развитие критического мышления.

c. Внедрение института обязательного кибер-страхования. Целесообразно разработать правовые механизмы стимулирования банковского и страхового секторов к внедрению доступных полисов страхования цифровых активов граждан от мошеннических посягательств, осуществленных с использованием методов социальной инженерии, что позволит снизить социальную напряженность и повысить доверие к цифровой финансовой системе.

9. ЗАКЛЮЧЕНИЕ (CONCLUSION)

Киберпреступность представляет собой сложный социотехнический вызов XXI века, требующий радикальной парадигмальной трансформации всей системы предупреждения правонарушений. Эволюция цифровых угроз демонстрирует, что борьба исключительно с последствиями совершенных кибератак является тупиковым путем. Основной вектор усилий государства должен быть смещен в сторону проактивной, ранней профилактики.

Благодаря системным реформам Президента Шавката Мирзиёева, в Узбекистане созданы уникальные условия для конвергенции научного потенциала и практического правоприменения. Интеграция передовых ИИ-технологий ведомственного мониторинга и беспрецедентного организационного потенциала «Махаллинской семерки» закладывает основу для формирования надежного «Цифрового щита» страны. Реализация предложенных в статье инициатив позволит Новой Республике Узбекистан не только эффективно минимизировать риски киберпреступности, но и выступить региональным лидером в сфере обеспечения цифровой безопасности общества.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ (REFERENCES)

1. Мирзиёев Ш. М. Обеспечение кибербезопасности и защита духовного пространства Нового Узбекистана — стратегическая задача государства // Официальный сайт Пресс-службы Президента Республики Узбекистан (www.press-service.uz).

2. Исмаилов И. Криминология в информационном обществе: Учебник для высших образовательных учреждений МВД РУз. — Ташкент: Академия МВД РУз, 2022. — 296 с.

3. Рустамбаев М. Х. Информационные преступления и деформация правосознания в эпоху глобализации. — Ташкент: «ILM ZIYO», 2023. — 324 с.

4. Очилов Х. Р. Проблемы детерминации киберпреступности и использования методов социальной инженерии // Юридический вестник. — Ташкент, 2024. — № 1. — С. 45–54.

5. Икрамов Ш. Т. Трансформация структуры правонарушений под влиянием социальных медиа: Монография. — Ташкент: Академия МВД Республики Узбекистан, 2023. — 210 с.

6. Шаумаров З. Психологические механизмы манипуляции сознанием молодежи в социальных сетях и их криминологическое значение //

Научный вестник Академии МВД Республики Узбекистан. — Ташкент, 2022. — № 1. — С. 60–68.

7. Шаумаров З. Актуальные вопросы разработки психологических методов противодействия киберпространственным девиациям // Научный вестник Академии МВД Республики Узбекистан. — Ташкент, 2023. — № 4. — С. 115–123.

8. Шаумаров З. Киберпрофайлинг и методы раннего выявления интернет-виктимности личности: Методическое пособие. — Ташкент: Академия МВД Республики Узбекистан, 2024. — 162 с.

9. Пулатов Б. Х. Организационно-правовое регулирование деятельности ОВД в сфере обеспечения кибербезопасности // Проблемы обеспечения правопорядка. — Ташкент, 2024. — № 4. — С. 142–151.

10. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан (www.lex.uz).

11. Закон Республики Узбекистан «О профилактике правонарушений» от 14.05.2014 г. № ЗРУ-371 // lex.uz.

12. Постановление Президента Республики Узбекистан № ПП-10 от 20 января 2024 года «О мерах по кардинальному совершенствованию системы работы с махаллями и внедрению концепции "Махаллинской семерки"» // lex.uz.

13. Ходжаев А. А. Социальные сети как катализатор девиантного поведения: опыт эмпирического исследования // Общество и правопорядок в Узбекистане. — Ташкент, 2024. — № 2. — С. 88–95.

14. Зуфаров У. С. Виртуальные криминальные сообщества: структура, иерархия и методы противодействия: Монография. — Ташкент: Фан, 2025. — 204 с.