КИБЕРПРЕСТУПЛЕНИЯ ПРОТИВ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ УЗБЕКИСТАНА: ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ, СОВРЕМЕННЫЕ УГРОЗЫ И ПУТИ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ

Жололидинова Дилара Зовки кизи,
студентка факультета «Бизнес-право и судебная защита»,
Ташкентского государственного юридического университета
Email:dilarajololidinova@gmail.com

АННОТАЦИЯ

В статье рассматриваются киберпреступления против государственных информационных систем Узбекистана как одна из наиболее актуальных угроз цифровому государству. Исследуются история развития национального законодательства в данной сфере, современное состояние правового регулирования, статистические показатели роста киберпреступности, а также институциональные меры, принимаемые государством для защиты государственных информационных ресурсов. Особое внимание уделено уголовно-правовой охране государственных информационных систем, роли Закона Республики Узбекистан «О кибербезопасности», нормам Уголовного кодекса о преступлениях в сфере информационных технологий, а также актам Президента и Кабинета Министров, направленным на защиту объектов критической информационной инфраструктуры. В работе проанализированы практические кейсы, включая мошеннические действия с использованием имени портала my.gov.uz, что демонстрирует уязвимость не только технической инфраструктуры, но и доверия граждан к цифровым государственным сервисам. На основе исследования выявлены основные проблемы квалификации, доказывания и предупреждения таких преступлений, а также предложены пути совершенствования законодательства и правоприменительной практики.

Ключевые слова: *киберпреступления, государственные информационные системы, кибербезопасность, Узбекистан, электронное правительство, my.gov.uz, критическая информационная инфраструктура, цифровые доказательства, уголовно-правовая защита.*

ANNOTATSIYA

Mazkur maqolada O‘zbekiston davlat axborot tizimlariga qarshi sodir etilayotgan kiberjinoyatlar raqamli davlatga tahdid soluvchi eng dolzarb xavflardan biri sifatida tahlil qilinadi. Tadqiqotda ushbu sohadagi milliy qonunchilikning

rivojlanish tarixi, huquqiy tartibga solishning hozirgi holati, kiberjinoyatchilikning o‘sishiga oid statistik ko‘rsatkichlar hamda davlat axborot resurslarini himoya qilish bo‘yicha ko‘rilayotgan institutsional chora-tadbirlar o‘rganilgan. Davlat axborot tizimlarini jinoyat-huquqiy muhofaza qilish, “Kiberxavfsizlik to‘g‘risida”gi Qonunning o‘rni, Jinoyat kodeksining axborot texnologiyalari sohasidagi jinoyatlarga oid normalari, shuningdek, tanqidiy axborot infratuzilmasi obyektlarini himoya qilishga qaratilgan Prezident va Vazirlar Mahkamasi hujjatlariga alohida e’tibor qaratilgan. Ishda my.gov.uz portali nomidan foydalanilgan firibgarlik holati misolida amaliy holatlar ham tahlil qilinib, bunda nafaqat texnik infratuzilma, balki fuqarolarning davlat raqamli xizmatlariga bo‘lgan ishonchi ham xavf ostida ekanligi ko‘rsatilgan. Tadqiqot natijasida bunday jinoyatlarni kvalifikatsiya qilish, isbotlash va oldini olishdagi asosiy muammolar aniqlanib, qonunchilik va huquqni qo‘llash amaliyotini takomillashtirish yo‘llari taklif etilgan.

Kalit so'zlar: *kiberjinoyatchilik, davlat axborot tizimlari, kiberxavfsizlik, O'zbekiston, elektron hukumat, my.gov.uz, muhim axborot infratuzilmasi, raqamli dalillar, jinoiy himoya.*

ABSTRACT

This article examines cybercrimes against state information systems of Uzbekistan as one of the most pressing threats to the digital state. It explores the historical development of national legislation in this field, the current state of legal regulation, statistical indicators of cybercrime growth, and institutional measures undertaken by the state to protect public information resources. Particular attention is paid to the criminal law protection of state information systems, the role of the Law of the Republic of Uzbekistan “On Cybersecurity,” the provisions of the Criminal Code concerning crimes in the sphere of information technologies, as well as presidential and governmental acts aimed at protecting critical information infrastructure. The paper also analyzes practical cases, including fraudulent schemes involving the name of the my.gov.uz portal, demonstrating the vulnerability not only of technical infrastructure but also of public trust in digital government services. Based on the findings, the study identifies major problems of legal qualification, proof, and prevention of such crimes and proposes ways to improve legislation and law enforcement practice.

Keywords*: cybercrime, government information systems, cybersecurity, Uzbekistan, e-government, my.gov.uz, critical information infrastructure, digital evidence, criminal defense.*

ВВЕДЕНИЕ

Цифровизация государственного управления в Узбекистане в последние годы приобрела системный характер. Государственные услуги переводятся в электронную форму, расширяется деятельность Единого портала интерактивных государственных услуг, развиваются межведомственные информационные системы, электронная идентификация, цифровой документооборот и иные элементы электронного правительства. Закон Республики Узбекистан «Об электронном правительстве» закрепляет организационные основы цифрового взаимодействия государства и граждан, а также определяет полномочия государственных органов в этой сфере.[1] Это означает, что государственные информационные системы сегодня являются не вспомогательным техническим инструментом, а полноценной основой современной публичной администрации.

Одновременно с этим рост цифровизации усиливает и криминальные риски. Чем больше государственных функций переносится в электронную среду, тем выше вероятность незаконного доступа, вмешательства в работу систем, подмены данных, использования фишинга, вредоносного программного обеспечения и иных форм киберпреступной деятельности. По данным МВД Республики Узбекистан, если в 2019 году посредством информационных технологий было совершено 863 преступления 18 видов, то в 2024 году зарегистрировано уже 58 800 преступлений 62 видов, а причиненный гражданам ущерб превысил 1 трлн 909 млрд сумов.[2] Эти цифры показывают, что киберпреступность перестала быть узкой технической проблемой и превратилась в самостоятельную угрозу общественной и государственной безопасности.

Правовое развитие этой сферы в Узбекистане происходило поэтапно. Вначале законодательство решало общие задачи информатизации и защиты информации, однако по мере усложнения цифровой среды возникла необходимость специального регулирования кибербезопасности. Важным шагом стало принятие Закона Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 года, который определил правовые и организационные

[1] Закон Республики Узбекистан «Об электронном правительстве» от 09.12.2015 г. № ЗРУ-395 [Электронный ресурс]. Режим доступа: https://lex.uz/ru/docs/2833855 Дата обращения: 07.04.2026

[2] Министерство внутренних дел Республики Узбекистан. Если в 2019 году посредством информационных технологий было совершено 863 преступления 18 видов, то в 2024 году зарегистрировано 58 800 преступлений 62 видов; ущерб превысил 1 трлн 909 млрд сумов [Электронный ресурс]. Режим доступа: https://gov.uz/ru/iiv/news/view/57775 Дата обращения: 07.04.2026.

основы защиты объектов информатизации и киберпространства.[3] Следующим значимым этапом стало принятие постановления Президента № ПП-167 от 31 мая 2023 года, утвердившего порядок обеспечения кибербезопасности объектов критической информационной инфраструктуры. [4] Тем самым государство закрепило, что отдельные информационные системы имеют повышенное значение и требуют специального режима защиты.

Актуальность темы обусловлена не только ростом числа преступлений, но и особенностью объекта посягательства. Если атака направлена на государственную информационную систему, вред причиняется не только конкретной базе данных или серверу. Под угрозой оказываются предоставление государственных услуг, стабильность публичного управления, сохранность персональных данных, доверие граждан к цифровым сервисам и в отдельных случаях элементы национальной безопасности.[5][6][7]

Именно поэтому киберпреступления против государственных информационных систем требуют отдельного научного и правового анализа.

Степень изученности темы пока нельзя признать достаточной. В научной литературе чаще исследуются общие вопросы киберпреступности, защиты персональных данных, цифровых доказательств и информационной безопасности, тогда как именно посягательства на государственные информационные системы в условиях Узбекистана рассматриваются фрагментарно. Кроме того, в открытом доступе ограничено количество развернутых судебных решений по таким делам, что осложняет анализ правоприменительной практики. В таком случае особую ценность приобретают нормы законодательства, официальные государственные сообщения,

[3] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 [Электронный ресурс]. Режим доступа: https://lex.uz/ru/docs/5960609 Дата обращения: 07.04.2026.

[4] Постановление Президента Республики Узбекистан от 31.05.2023 г. № ПП-167 «О дополнительных мерах по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» [Электронный ресурс]. Режим доступа: https://lex.uz/docs/6479197 Дата обращения: 08.04.2026.

[5] Закон Республики Узбекистан «Об электронном правительстве» от 09.12.2015 г. № ЗРУ-395 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/2833855 (дата обращения: 07.04.2026);

[6] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL:https://lex.uz/ru/docs/5960609 (дата обращения: 07.04.2026);

[7] Постановление Президента Республики Узбекистан от 31.05.2023 г. № ПП-167 «О дополнительных мерах по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL:https://lex.uz/docs/6479197 (дата обращения: 07.04.2026). Эти акты в совокупности закрепляют связь государственных информационных систем с оказанием электронных государственных услуг, защитой информационных ресурсов и обеспечением устойчивости объектов критической информационной инфраструктуры.

статистика и конкретные кейсы, связанные с государственными цифровыми сервисами.[8]

Вместе с тем основная научно-правовая проблема заключается не только в самом росте киберпреступности, но и в том, что действующее уголовное и информационное законодательство Республики Узбекистан не в полной мере учитывает особый статус государственных информационных систем как объекта повышенной правовой охраны. Действующие нормы в основном ориентированы на защиту компьютерной информации и информационных систем в общем виде, тогда как посягательство именно на государственную информационную систему затрагивает не только сферу информационной безопасности, но и стабильность публичного управления, доступ граждан к государственным услугам, защиту персональных данных и доверие к цифровому государству. Кроме того, правоприменение сталкивается со сложностями квалификации, доказывания и оценки степени общественной опасности таких посягательств, а ограниченность открытой судебной практики затрудняет формирование единых подходов. Именно в этом заключается центральная правовая интрига настоящего исследования.

Цель настоящей статьи состоит в комплексном исследовании киберпреступлений против государственных информационных систем Узбекистана, выявлении пробелов в действующем уголовном и информационном регулировании, анализе основных трудностей квалификации и доказывания, а также формулировании предложений по совершенствованию законодательства и правоприменительной практики.

Методы

При подготовке статьи использовались формально-юридический, сравнительно-правовой, системный и аналитический методы исследования.

Формально-юридический метод применялся для изучения действующего законодательства Республики Узбекистан, прежде всего Закона «О кибербезопасности», Закона «Об электронном правительстве», а также Уголовного кодекса Республики Узбекистан, включая нормы главы XX[1] о преступлениях в сфере информационных технологий. С помощью этого метода исследовались содержание правовых норм, их цели, предмет регулирования и соотношение между собой.[9]

[8] Ташкентский городской суд. Электронные данные в суде: роль цифровых доказательств // Официальный сайт судебных органов Республики Узбекистан [Электронный ресурс]. URL: https://toshkent.sud.uz/электронные-данные-в-суде-роль-цифров/ (дата обращения: 07.04.2026).

[9] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/5960609 (дата обращения: 07.04.2026).

Сравнительно-правовой метод использовался для оценки того, насколько узбекская модель уголовно-правовой охраны государственных информационных систем соответствует общим международным подходам к криминализации незаконного доступа, вмешательства в данные, вмешательства в работу систем и использования специальных средств для совершения киберпреступлений. Хотя статья ориентирована прежде всего на национальное право, анализ строился с учетом того, что современные киберугрозы по своей природе трансграничны и не могут эффективно исследоваться изолированно.[10]

Системный метод позволил рассмотреть государственные информационные системы не только как технические объекты, но и как элементы цифрового государства, взаимодействующие с административным правом, уголовным правом, информационным правом и сферой национальной безопасности.

Эмпирической базой исследования выступили официальные статистические материалы, сообщения государственных органов и открытые публикации о киберинцидентах. В частности, использованы данные МВД о динамике киберпреступности, сведения UZCERT о количестве выявленных киберинцидентов, киберугроз и уязвимостей в 2025 году, а также публикации о мошеннических схемах, связанных с my.gov.uz.

На сайте UZCERT указано, что в 2025 году было выявлено 247 киберинцидентов, обнаружено более 2 миллионов киберугроз, выявлено более 700 уязвимостей на веб-сайтах и устранено свыше 67 миллионов кибератак.[11]

Практический кейс, связанный с февральской утечкой персональных данных из государственных систем, имеет центральное значение для исследования. В начале февраля 2026 года в публичном пространстве появились сообщения о компрометации центрального OAuth-сервера цифрового правительства, через который осуществлялась аутентификация в ряде государственных и связанных с ними систем. Первоначально злоумышленник заявил о продаже более 15 миллионов записей, однако эта цифра не была верифицирована. По данным анализа C7 Cybersecurity, опубликованного Spot, были подтверждены отдельные массивы данных: свыше 5522 записей с единого OAuth-сервера E-Gov, более 24 фотографий сотрудников МВД, 15 874 записи из массива Национального агентства социальной защиты и 446 записей компании по рефинансированию ипотеки.

[10] United Nations. Convention against Cybercrime (2024) // Официальный сайт ООН [Электронный ресурс]. URL: https://www.unodc.org/unodc/en/cybercrime/convention/home.html (дата обращения: 07.04.2026).
[11] UZCERT. Официальная статистика киберинцидентов и киберугроз за 2025 год // Официальный сайт [Электронный ресурс]. URL: https://uzcert.uz (дата обращения: 07.04.2026).

Среди категорий скомпрометированных данных фигурировали ПИНФЛ, ФИО, даты рождения, номера телефонов и паспортные данные. Позднее министр цифровых технологий Шерзод Шерматов сообщил, что распространённая цифра в 15 миллионов не подтвердилась, а предварительная оценка показала компрометацию примерно 60 тысяч уникальных персональных данных и затрагивание трёх государственных систем в период с 27 по 30 января 2026 года. По реконструкции C7 Cybersecurity, первоначальный доступ, вероятно, был получен через уязвимость Log4Shell, а сам инцидент носил характер атаки на цепочку поставок, поскольку компрометация центрального сервера аутентификации создавала риск для доверяющих ему систем.

После инцидента на платформе OneID доступ к персональным данным был ограничен по умолчанию, а пользователям предоставлена возможность самостоятельно разрешать или запрещать передачу своих данных организациям через раздел управления персональными данными. Дополнительным механизмом превенции выступает сервис my.gov.uz по установлению запрета на заключение кредитного договора, позволяющий пользователю снизить риск мошеннического оформления кредита при компрометации его данных. Одновременно гражданам рекомендовано проявлять повышенную бдительность к мошенническим звонкам и сообщениям, использовать дополнительные средства защиты, а государству проводить ротацию токенов и учётных данных, аудит Java-приложений, сегментацию сетей и пересмотр архитектуры OAuth-доверия.

С правовой точки зрения данный инцидент выявляет сразу несколько проблем. Во-первых, он показывает, что компрометация одного узлового элемента государственной цифровой инфраструктуры способна затронуть не одну отдельную базу данных, а целый комплекс взаимосвязанных государственных и связанных с ними систем, что существенно повышает общественную опасность такого посягательства. Во-вторых, подобные случаи ставят вопрос о том, насколько действующие уголовно-правовые конструкции позволяют в полной мере учесть многообъектный характер причиняемого вреда, когда одновременно затрагиваются информационная безопасность, персональные данные, устойчивость оказания государственных услуг и доверие к цифровому государству. В-третьих, такие инциденты демонстрируют практические сложности доказывания: установление способа первоначального доступа, определение масштаба компрометации, разграничение несанкционированного доступа, последующего использования данных и возможных мошеннических действий, а также точная фиксация цифровых

следов требуют высокого уровня технической и процессуальной подготовки. Тем самым кейс с OneID и центральным OAuth-сервером подтверждает, что посягательства на государственные информационные системы нуждаются не только в техническом реагировании, но и в более точной уголовно-правовой и процессуальной проработке.

Следовательно, практический кейс подтверждает, что основная трудность заключается не только в наличии киберугроз как таковых, но и в недостаточной адаптированности правового механизма к случаям, когда объектом посягательства выступают централизованные элементы государственной цифровой инфраструктуры. Таким образом, данный кейс демонстрирует, что посягательства на государственные информационные системы обладают повышенной общественной опасностью и требуют не только технического реагирования, но и дальнейшего совершенствования уголовно-правовых механизмов защиты.

Результаты

Проведенное исследование позволяет сделать вывод о том, что в Республике Узбекистан уже сформирована базовая нормативная и институциональная основа защиты государственных информационных систем, однако действующая модель правового регулирования остается фрагментарной, недостаточно дифференцирует посягательства на государственные и негосударственные системы и в большей степени ориентирована на реакцию на киберинциденты, чем на их опережающее предупреждение.

Во-первых, исследование показывает, что кибербезопасность в Узбекистане уже признана самостоятельным направлением публично-правового регулирования. Однако при этом нормативное закрепление защищенности объектов информатизации пока не сопровождается столь же четким уголовно-правовым выделением государственных информационных систем как особого объекта повышенной охраны. Закон «О кибербезопасности» устанавливает правовые и организационные основы обеспечения защищенности объектов информатизации и киберпространства, а также предусматривает оценку уровня обеспечения кибербезопасности и специальные требования к объектам критической информационной инфраструктуры.[12] Это означает, что законодатель отказался от восприятия киберугроз как побочной проблемы информатизации и выделил их в отдельную сферу публичного управления.

[12] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/5960609 (дата обращения: 07.04.2026).

Во-вторых, действующее регулирование усиливает охрану наиболее значимых цифровых ресурсов через механизм критической информационной инфраструктуры, однако сама по себе принадлежность системы к государственному сектору еще не всегда означает наличие специального уголовно-правового акцента на повышенной общественной опасности посягательства на нее. Постановление Президента № ПП-167 от 31 мая 2023 года утвердило Положение о порядке обеспечения кибербезопасности объектов критической информационной инфраструктуры и общие требования к их защите.[13] Из этого следует, что отдельные государственные и иные значимые системы рассматриваются как инфраструктура повышенной значимости, нарушение функционирования которой может причинить серьезный вред общественным и государственным интересам.

В-третьих, уголовное законодательство Узбекистана уже содержит специальный блок составов, относящихся к преступлениям в сфере информационных технологий. Глава XX[1] Уголовного кодекса включает такие составы, как нарушение правил информатизации, незаконный доступ к компьютерной информации, модификация компьютерной информации, компьютерный саботаж, создание и распространение вредоносных программ и другие формы противоправного воздействия на компьютерные системы и данные. [14] Следовательно, действующее право в целом позволяет квалифицировать многие формы посягательств на государственные информационные системы.

В-четвертых, статистические данные свидетельствуют о резком росте киберугроз и киберпреступности. Рост с 863 преступлений в 2019 году до 58 800 в 2024 году показывает, что масштабы проблемы изменились качественно.[15] При этом сведения UZCERT за 2025 год подтверждают высокий уровень ежедневной угрозы для национального цифрового пространства. [16] Таким образом, развитие законодательства объективно происходит как реакция на резкое усложнение криминальной обстановки в киберсреде.

[13] Постановление Президента Республики Узбекистан от 31.05.2023 г. № ПП-167 «О дополнительных мерах по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/docs/6479197 (дата обращения: 07.04.2026).
[14] Уголовный кодекс Республики Узбекистан // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/acts/1295264 (дата обращения: 07.04.2026).
[15] Министерство внутренних дел Республики Узбекистан. Официальные данные о росте киберпреступности // Официальный сайт [Электронный ресурс]. URL: https://gov.uz/ru/iiv/news/view/57775 (дата обращения: 07.04.2026).
[16] UZCERT. Официальная статистика киберинцидентов и киберугроз за 2025 год // Официальный сайт [Электронный ресурс]. URL:https://uzcert.uz (дата обращения: 08.04.2026).

В-пятых, в последние годы государство усиливает институциональное противодействие преступлениям, совершаемым с помощью информационных технологий. В 2025 году было принято постановление Президента № ПП-153, направленное на дальнейшее усиление деятельности по борьбе с такими преступлениями. [17] Это подтверждает, что проблема киберпреступности признается не эпизодической, а системной и требует организационной перестройки правоохранительной деятельности.

Существенным институциональным шагом стало и создание Государственного университета «Cyber university». **Постановлением Президента Республики Узбекистан от 20 января 2025 года № ПП-14** было поддержано предложение Министерства цифровых технологий и Службы государственной безопасности о создании данного университета[18]. В документе прямо указано, что университет создается для подготовки высококвалифицированных кадров, а также для решения задач в сферах защиты информации, информационной и кибербезопасности и цифровых технологий.

Практическое значение Cyber university для противодействия киберпреступности состоит в том, что государство формирует не узко техническую, а междисциплинарную кадровую базу. По официальному сайту университета среди направлений подготовки присутствуют не только информационная безопасность, кибербезопасность, программная инженерия и искусственный интеллект, но и **«Юриспруденция: Киберправо», «Юриспруденция: Цифровая криминалистика», а также «Менеджмент: Управление кибербезопасностью» и «Экономика: Цифровая экономика».** Это означает, что для защиты государственных информационных систем государство ориентируется не только на подготовку специалистов по защите, но и на подготовку юристов, цифровых криминалистов, управленцев и экспертов, способных работать на стыке права, технологий и расследования.

Следовательно, Cyber university следует рассматривать как долгосрочный механизм противодействия киберпреступности: через него государство создает кадровую и аналитическую основу для защиты цифровой инфраструктуры,

[17] Постановление Президента Республики Узбекистан от 30.04.2025 г. № ПП-153 «О мерах по усилению борьбы с преступлениями, совершаемыми с использованием информационных технологий» // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/7511168 (дата обращения: 07.04.2026).
[18] Постановление Президента Республики Узбекистан от 20.01.2025 г. № ПП-14 «О создании Cyber University».

расследования киберпреступлений и правового регулирования цифровой среды.[19]

Обсуждение

Отдельного внимания заслуживает международно-правовой аспект противодействия киберпреступности. Узбекистан уже подписал Конвенцию ООН против киберпреступности: по данным UN Treaty Collection, подпись была поставлена 25 октября 2025 года. Участие в данной Конвенции усиливает универсальную основу международного сотрудничества, в том числе по вопросам обмена электронными доказательствами и расследования преступлений, носящих трансграничный характер.

Вместе с тем Узбекистан не является участником Будапештской конвенции о киберпреступности. В правовом профиле Совета Европы по Узбекистану прямо указано, что подписание Конвенции отсутствует. Между тем именно Будапештская конвенция содержит один из наиболее детализированных международных механизмов сотрудничества по киберделам, включая ускоренное сохранение данных, ускоренное раскрытие трафиковых данных и сеть круглосуточных контактных пунктов 24/7. Присоединение к ней могло бы усилить способность Узбекистана оперативно сохранять и получать электронные доказательства по делам, где данные и исполнители находятся за пределами страны.

При этом отсутствие участия в Будапештской конвенции не означает отсутствия международного сотрудничества вообще. Узбекистан является членом Интерпола с 28 сентября 1994 года, а Национальное центральное бюро в Ташкенте взаимодействует с другими государствами через систему I-24/7. По линии Интерпола возможно направление запросов, обмен полицейской информацией, а также инициирование Red Notice для установления местонахождения и временного задержания разыскиваемого лица. Однако Red Notice не является международным ордером на арест и не заменяет специализированные механизмы быстрого получения и сохранения электронных доказательств.

Кроме того, Узбекистан участвует в более широких международных инструментах сотрудничества, включая Конвенцию ООН против транснациональной организованной преступности и Конвенцию ООН против коррупции. Эти договоры не заменяют специальные киберконвенции, однако укрепляют общую основу международной правовой помощи, экстрадиции,

[19] C7 Cybersecurity. Анализ утечки данных OneID / OAuth (опубликовано на Spot). URL: https://www.spot.uz

поиска лиц и взаимодействия по делам, где киберпреступление связано с организованной преступностью, финансовым мошенничеством или коррупционными схемами.

ВЫВОДЫ

Проведенное исследование позволяет сделать несколько итоговых выводов.

Во-первых, киберпреступления против государственных информационных систем Узбекистана представляют собой одну из наиболее опасных форм современной киберпреступности, поскольку они затрагивают не только информационные ресурсы как таковые, но и функционирование государства, устойчивость публичных сервисов и доверие граждан к цифровому управлению.

Во-вторых, в Узбекистане уже создана нормативная основа для противодействия таким преступлениям. Ее ключевыми элементами являются Закон «Об электронном правительстве», Закон «О кибербезопасности», положения Уголовного кодекса о преступлениях в сфере информационных технологий, а также акты Президента, направленные на защиту критической информационной инфраструктуры.[20]

В-третьих, официальная статистика показывает стремительный рост киберпреступности, а практические кейсы, включая использование имени my.gov.uz в мошеннических схемах, подтверждают, что угроза носит как технический, так и социальный характер.[21]

В-четвертых, действующего регулирования пока недостаточно для полного и точного отражения особенностей посягательств именно на государственные информационные системы. Основными проблемами остаются отсутствие специального акцента на государственном характере объекта посягательства, сложности доказывания, ограниченность открытой судебной практики и слабая превентивная составляющая.

В-пятых, перспективы совершенствования связаны с усилением уголовно-правовой охраны государственных систем, развитием механизмов работы с цифровыми доказательствами, повышением уровня прозрачности судебной практики и укреплением превентивной киберзащиты. В итоге можно сделать вывод, что защита государственных информационных систем должна

[20] Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/5960609 (дата обращения: 08.04.2026).

[21] Kun.uz. Мошенники рассылают фейковые письма от имени my.gov.uz и звонят через Telegram // [Электронный ресурс]. URL: https://kun.uz/ru/news/2026/03/25/moshenniki-rassylayut-feykovyye-pisma-ot-imeni-mygovuz-i-zvonyat-cherez-telegram (дата обращения: 07.04.2026).

рассматриваться не как узкотехническая задача, а как одно из центральных направлений обеспечения правопорядка и устойчивости цифрового государства в Узбекистане.

ЛИТЕРАТУРА / REFERENCES

1. Закон Республики Узбекистан «Об электронном правительстве» от 09.12.2015 г. № ЗРУ-395 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/2833855 (дата обращения: 07.04.2026).
2. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/5960609 (дата обращения: 07.04.2026).
3. Уголовный кодекс Республики Узбекистан // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/acts/1295264 (дата обращения: 07.04.2026).
4. Постановление Президента Республики Узбекистан от 31.05.2023 г. № ПП-167 «О дополнительных мерах по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/docs/6479197 (дата обращения: 07.04.2026).
5. Постановление Президента Республики Узбекистан от 30.04.2025 г. № ПП-153 «О мерах по усилению борьбы с преступлениями, совершаемыми с использованием информационных технологий» // Национальная база данных законодательства Республики Узбекистан [Электронный ресурс]. URL: https://lex.uz/ru/docs/7511168 (дата обращения: 07.04.2026).
6. Министерство внутренних дел Республики Узбекистан. Официальные данные о росте киберпреступности // Официальный сайт [Электронный ресурс]. URL: https://gov.uz/ru/iiv/news/view/57775 (дата обращения: 07.04.2026).
7. UZCERT. Официальная статистика киберинцидентов и киберугроз // Официальный сайт [Электронный ресурс]. URL: https://uzcert.uz (дата обращения: 07.04.2026).
8. Kun.uz. Мошенники рассылают фейковые письма от имени my.gov.uz и звонят через Telegram // [Электронный ресурс]. URL: https://kun.uz/ru/news/2026/03/25/moshenniki-rassylayut-feykovyye-pisma-ot-imeni-mygovuz-i-zvonyat-cherez-telegram (дата обращения: 07.04.2026).

9. Ташкентский городской суд. Электронные данные в суде: роль цифровых доказательств // Официальный сайт судебных органов Республики Узбекистан [Электронный ресурс]. URL: https://toshkent.sud.uz/электронные-данные-в-суде-роль-цифров/ (дата обращения: 07.04.2026).
10. United Nations. Convention against Cybercrime (2024) // Official website [Electronic resource]. URL: https://www.unodc.org/unodc/en/cybercrime/convention/home.html (дата обращения: 07.04.2026).