EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
IF = 9.2 www.in-academy.uz/index.php/ejlfas

"LEGAL ASPECTS OF ENHANCING MEASURES TO PREVENT AND COUNTER CYBERCRIME IN THE REPUBLIC OF UZBEKISTAN"

Aybek Orazbaevich Xalmuratov

https://doi.org/10.5281/zenodo.19941840

ARTICLE INFO

Received: 24th April 2026
Accepted: 29th April 2026
Online: 30th April 2026

KEYWORDS

Cybercrime, legal regulation, early warning, IT specialists, digital economy.

ABSTRACT

This article analyzes the legal aspects of combating cybercrime in the Republic of Uzbekistan, examining issues in legal regulation and proposing solutions. Amid the development of digital technologies, cybercrime poses a threat to the economy and security. The study highlights several key areas for focus: improving early warning mechanisms, ensuring the certainty of punishment, implementing digital technologies, and recruiting highly qualified IT specialists into law enforcement agencies. These measures are aimed at strengthening security and fostering the development of the digital economy.

"ПРАВОВЫЕ АСПЕКТЫ СОВЕРШЕНСТВОВАНИЕ МЕР ПО ПРЕДУПРЕЖДЕНИЮ И ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКИ УЗБЕКИСТАН"

Айбек Оразбаевич Халмуратов
Самостоятельный соискатель Правоохранительной академии Республики Узбекистан
e-mail: bekbayevich@gmail.com

https://doi.org/10.5281/zenodo.19941840

ARTICLE INFO

Received: 24th April 2026
Accepted: 29th April 2026
Online: 30th April 2026

KEYWORDS

Киберпреступность, правовое регулирование, раннее предупреждение, IT-специалисты, цифровая экономика.

ABSTRACT

Статья анализирует правовые аспекты борьбы с киберпреступностью в Республике Узбекистан, рассматривая проблемы правового регулирования и предлагая меры для их решения. В условиях развития цифровых технологий киберпреступность представляет угрозу для экономики и безопасности. В исследовании выделены ключевые направления: улучшение механизмов раннего предупреждения, обеспечение неотвратимости наказания, внедрение цифровых технологий и привлечение высококвалифицированных IT-специалистов в правоохранительные органы. Эти меры направлены на укрепление безопасности и развитие цифровой экономики.

EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
IF = 9.2 www.in-academy.uz/index.php/ejlfas

“ЎЗБЕКИСТОН РЕСПУБЛИКАСИДА КИБЕРЖИНОЯТЧИЛИКНИНГ ОЛДИНИ ОЛИШ ВА УНГА ҚАРШИ КУРАШИШ ЧОРАЛАРИНИ ТАКОМИЛЛАШТИРИШНИНГ ҲУҚУҚИЙ ЖИҲАТЛАРИ”

Айбек Оразбаевич Халмуратов

https://doi.org/10.5281/zenodo.19941840

ARTICLE INFO

Received: 24th April 2026
Accepted: 29th April 2026
Online: 30th April 2026

KEYWORDS

Кибержиноятчилик, ҳуқуқий тартибга солиш, барвақт огоҳлантириш, АТ-мутахассислар, рақамли иқтисодиёт.

ABSTRACT

Мазкур мақолада Ўзбекистон Республикасида кибержиноятчиликка қарши курашишнинг ҳуқуқий жиҳатлари таҳлил қилинган, ҳуқуқий тартибга солиш муаммолари кўриб чиқилиб, уларни ҳал этиш чоралари таклиф этилган. Рақамли технологиялар ривожланаётган бир шароитда кибержиноятчилик иқтисодиёт ва хавфсизлик учун таҳдид солмоқда. Тадқиқотда асосий йўналишлар белгилаб берилган: барвақт огоҳлантириш механизмларини такомиллаштириш, жазонинг муқаррарлигини таъминлаш, рақамли технологияларни жорий этиш ҳамда ҳуқуқни муҳофаза қилувчи органларга юқори малакали ИТ-мутахассисларни жалб қилиш. Бу чоралар хавфсизликни мустаҳкамлаш ва рақамли иқтисодиётни ривожлантиришга қаратилган.

С развитием информационных технологий, которые охватывают все более широкие аспекты жизни общества, киберпреступность становится одной из самых опасных угроз для безопасности, экономики и прав личности. Эти преступления, как правило, выходят за рамки традиционного уголовного права [1] и требуют создания специальных правовых, технических и социальных механизмов для их предотвращения и минимизации ущерба.

Глобализация и бурное развитие цифровых технологий создают преступникам новые возможности для совершения противоправных действий. С каждым годом методы, применяемые киберпреступниками, становятся всё более сложными, что ставит перед правоохранительными органами задачу быстрого реагирования и постоянной адаптации методов борьбы с киберугрозами. Однако, несмотря на усилия по улучшению законодательства, остаются серьёзные проблемы, такие как недостаточная подготовленность специалистов, пробелы в правовом регулировании и недостаток современных технических ресурсов.

Для Республики Узбекистан, активно развивающей цифровую экономику и внедряющей новые технологии в различные сферы жизни, борьба с киберпреступностью становится одной из приоритетных задач. В последние годы наблюдается рост преступлений, совершённых с использованием информационных технологий, что делает вопрос

противодействия этим угрозам особенно актуальным. Для эффективного решения этих проблем необходимо внедрение комплексных стратегий, которые будут включать как правовые меры, так и инновационные технические решения, а также усилия по повышению осведомлённости и обучению населения.

Целью настоящего исследования является разработка рекомендаций по улучшению борьбы с киберпреступностью в Узбекистане. В частности, внимание уделяется четырём основным направлениям: усовершенствование механизмов раннего предупреждения киберпреступлений, обеспечение неотвратимости наказания за такие преступления, внедрение современных цифровых решений для оперативного выявления угроз и привлечение квалифицированных IT-специалистов в правоохранительные органы. Эти направления составляют основу необходимой комплексной стратегии для эффективного реагирования на вызовы, возникающие в киберпространстве.

Один из важнейших элементов эффективной борьбы с киберпреступностью – это создание **системы раннего предупреждения**, которая позволит снизить ущерб от преступлений, совершаемых с использованием цифровых технологий. В условиях динамично меняющейся цифровой среды, где преступники постоянно совершенствуют свои методы, традиционные способы реагирования становятся недостаточными. В связи с этим, крайне важным становится внедрение инновационных методов, которые должны сочетать как технические, так и социальные инструменты для своевременного обнаружения угроз.

Одним из ключевых факторов, обеспечивающих эффективную работу системы раннего предупреждения, является ***мониторинг общественного восприятия угроз***. Периодические опросы, направленные на изучение опыта граждан в сфере цифровой безопасности, помогают выявить наиболее распространённые виды преступлений, а также осознание потенциальных рисков. Это не только позволяет своевременно обнаружить угрозы, но и оперативно реагировать на новые формы преступной деятельности. В условиях увеличения числа пользователей Интернета это становится особенно актуальным.

Международная практика, например в США и странах ЕС, показывает, что проведение регулярных опросов среди населения и бизнеса способствует созданию динамичных и актуальных данных, которые помогают не только выявить ключевые угрозы, но и адаптировать меры борьбы с ними. Программа “Cyber Security Breaches Survey” в Великобритании является одним из примеров эффективного подхода, предоставляющего подробную информацию о состоянии киберзащищенности организаций [2].

Для Узбекистана критически важным является ***использование зарубежного опыта*** с учётом особенностей местных условий.

Эффективная система предупреждения должна не только выявлять риски, но и повышать осведомлённость населения о потенциальных угрозах. Внедрение опросов среди граждан позволит точнее оценить масштабы проблемы и создать действенные государственные инициативы, направленные на профилактику киберпреступлений. Это, в свою очередь, предполагает необходимость образовательных программ, которые помогут повысить уровень цифровой грамотности и информировать граждан о безопасном использовании технологий.

Для эффективного функционирования системы раннего предупреждения необходимо развивать ***инфраструктуру обмена информацией*** и мониторинга угроз. В этом контексте важно создавать межведомственные и международные платформы, которые позволят оперативно обмениваться данными о выявленных угрозах и инцидентах. Подобные инициативы уже реализуются в ряде стран, где такие платформы способствуют быстрому реагированию на угрозы и инциденты.

Для Узбекистана создание подобных платформ будет ключевым шагом в интеграции усилий государственных структур, частных организаций и гражданского общества для эффективной борьбы с киберпреступностью.

На фоне развития инфраструктуры необходимо также акцентировать внимание на ***образовательных инициативах***, направленных на повышение осведомлённости граждан и организаций о киберугрозах. Обучение должно не только повышать цифровую грамотность, но и обучать методам защиты от угроз. Пример успешных инициатив можно найти в Скандинавии, где различные обучающие программы значительно снизили уровень уязвимости населения перед киберугрозами.

Принцип неотвратимости наказания является краеугольным камнем в борьбе с киберпреступностью. В условиях быстрых изменений в цифровой среде, где преступники постоянно совершенствуют свои методы, крайне важно не только обновить правовую базу, но и сформировать ясную систему ответственности за преступления, совершённые с использованием информационных технологий. Наличие законодательных пробелов, нехватка квалифицированных специалистов и низкий уровень уголовной ответственности могут существенно снизить эффективность борьбы с такими преступлениями, что способствует их распространению.

Одной из основных проблем в области киберпреступности в Узбекистане является несовершенство законодательства, направленного на защиту от подобных угроз. Несмотря на существование ряда правовых актов, таких как Закон об информатизации [3] и положения Уголовного кодекса [1], остаются значительные пробелы в правовом регулировании новых форм

преступлений. Например, такие преступления, как фишинг, кибершантаж или различные виды онлайн-мошенничества, не всегда должным образом отражены в законодательстве. Быстрое развитие технологий требует своевременной адаптации законодательства, иначе существует риск, что правонарушители будут действовать с уверенностью в своей безнаказанности, что увеличивает угрозу для всей цифровой инфраструктуры.

Для эффективного решения вышеупомянутых проблем необходимо ***унифицировать нормы уголовной ответственности за преступления, совершенные в киберпространстве.*** Это предполагает создание чёткой классификации киберпреступлений и установление соответствующих санкций для каждого их типа. Важно, чтобы наказания были дифференцированы в зависимости от тяжести преступления, что позволит создать справедливую и предсказуемую систему правоприменения. Например, для преступлений, связанных с утечкой персональных данных или кибератаками на критически важные объекты, должны быть предусмотрены более жёсткие меры наказания.

Необходимым элементом правового регулирования является внедрение механизма учёта отягчающих обстоятельств при определении наказания. Это могут быть такие обстоятельства, как использование сложных методов хакерских атак или участие в организованных преступных группах. Важно, чтобы правоохранительные органы имели возможность оперативно выявлять и классифицировать такие преступления для применения соответствующих санкций. Также необходимо учитывать интересы жертв киберпреступлений, обеспечив защиту их прав и компенсацию ущерба, включая такие последствия, как утечка личных данных или финансовые потери [4].

Ключевым аспектом в эффективной борьбе с киберпреступностью является ***правоприменительная практика***. В Узбекистане наблюдается дефицит квалифицированных специалистов, способных эффективно расследовать преступления, связанные с использованием информационных технологий. Отсутствие необходимой подготовки у правоохранителей замедляет процесс расследования и снижает его результативность. Для решения данной проблемы необходимо не только обновить законодательство, но и повысить квалификацию сотрудников правоохранительных органов, обеспечив их доступом к современным технологиям и специализированным программным продуктам. Создание специализированных подразделений, занимающихся исключительно киберпреступлениями, позволит ускорить процесс расследования и повысить уровень компетенции в данной области.

Киберпреступность часто имеет транснациональный характер, что требует ***международного взаимодействия и координации усилий на глобальном уровне***. Узбекистану необходимо развивать сотрудничество с международными организациями, такими как Интерпол, Европол и другими государствами, для обмена информацией и проведения совместных расследований. Также необходимо участвовать в международных инициативах, направленных на унификацию стандартов борьбы с киберпреступностью. Подписание соглашений о взаимно-правовой помощи и участие в совместных расследованиях поможет улучшить координацию между государствами и обеспечит более эффективное преследование преступников, действующих через международные границы.

Современные цифровые технологии предоставляют новые возможности для повышения эффективности борьбы с киберпреступностью. Искусственный интеллект и машинное обучение особенно перспективны для анализа больших массивов данных и обнаружения аномалий в поведении пользователей. Эти технологии позволяют идентифицировать потенциальные угрозы на ранних стадиях, анализируя цифровые следы, такие как поведение пользователей и транзакции. Примером успешного применения таких технологий служат системы ИИ, используемые в странах с развитыми системами кибербезопасности, например в США и Великобритании, для мониторинга сетевого трафика и обнаружения подозрительных действий в реальном времени, что даёт возможность оперативно реагировать на кибератаки [5].

Блокчейн представляет собой распределённую базу данных, которая позволяет обеспечивать неизменность записей и высокий уровень защиты от фальсификации информации. В рамках борьбы с киберпреступностью блокчейн может использоваться для защиты цифровых транзакций, подтверждения их подлинности и повышения прозрачности процессов передачи и хранения данных. Внедрение блокчейн-технологий в Узбекистане для мониторинга финансовых операций и обеспечения подлинности информации может значительно уменьшить риски мошенничества и других незаконных действий, а также повысить доверие к цифровым платформам [6].

Одной из значимых преград для внедрения современных технологий в Узбекистане является недостаточная инфраструктура для их полноценного применения. Это касается как вычислительных мощностей, так и необходимости создания защищённых каналов связи для интеграции новых технологий в существующие государственные и частные системы. Для решения этой проблемы необходимо модернизировать инфраструктуру, а также активно инвестировать в исследования и разработки в области информационных технологий.

Создание благоприятных условий для стартапов и привлечение международных экспертов поможет ускорить внедрение инновационных решений и повысить уровень кибербезопасности в стране.

С учётом быстрого прогресса технологий и растущих угроз в киберпространстве, **привлечение квалифицированных IT-специалистов в правоохранительные органы** становится необходимым условием эффективной борьбы с киберпреступностью. Для эффективной работы в области борьбы с преступлениями, совершёнными с использованием информационных технологий, требуются специалисты с высокими знаниями и навыками в сфере цифровых технологий. Однако на пути привлечения таких кадров в государственные структуры существуют серьёзные препятствия, такие как недостаточные условия оплаты труда, отсутствие должной социальной и правовой защиты, а также ограниченные возможности для карьерного роста.

Основной проблемой является невысокая привлекательность работы в правоохранительных органах для IT-специалистов. В условиях высокой конкуренции на рынке труда, где частные компании предлагают более высокие зарплаты и лучшие условия для профессионального роста, государственные структуры сталкиваются с трудностью привлечения квалифицированных кадров. Работники частного сектора, особенно в области информационной безопасности, получают более выгодные условия труда, что создаёт серьёзные трудности для комплектования правоохранительных органов высококвалифицированными специалистами [7].

Для того чтобы эффективно решать эту проблему, необходимо предоставить в государственных органах конкурентоспособные условия труда, включая возможности для профессионального развития и карьерного роста. Важно предложить сотрудникам государственные тренинги, сертификационные программы и участие в международных проектах, что в свою очередь повысит мотивацию для работы в правоохранительных органах.

Для того чтобы эффективно привлекать и удерживать IT-специалистов в государственных структурах, необходимо создать систему социальной и правовой защиты их труда. Это включает в себя обеспечение достойных условий для жизни и работы, таких как конкурентоспособная заработная плата, медицинская страховка, пенсионные накопления и другие социальные гарантии, соответствующие важности их труда.

Особое внимание стоит уделить правовой защите сотрудников, столкнувшихся с угрозами или давлением со стороны преступных групп, занимающихся киберпреступлениями. Требуется разработать и внедрить законодательные меры,

направленные на защиту работников от внешних угроз, а также обеспечение безопасности их личных данных и информации, с которой они работают в процессе расследования.

Для привлечения и удержания IT-специалистов в государственном секторе необходимо создать систему долгосрочных стимулов, включающих не только конкурентоспособные зарплаты, но и возможности для личностного и профессионального роста. Важно, чтобы сотрудники правоохранительных органов могли участвовать в международных проектах, повышать свою квалификацию и заниматься научной деятельностью в области информационной безопасности. Участие в разработке новых методов борьбы с киберпреступностью и инновационных технологий станет мощным стимулом для долгосрочной работы в правоохранительных органах.

Кроме того, необходимо поддерживать инновационные идеи и инициативы, которые способствуют совершенствованию работы правоохранительных органов. Привлечение специалистов к разработке новых методов расследования и защиты информации создаст дополнительные возможности для их профессионального развития и обеспечит высокий уровень мотивации в долгосрочной перспективе.

С учётом постоянного развития технологий, важно организовывать непрерывное обучение и повышение квалификации IT-специалистов в правоохранительных органах. Специалисты должны быть в курсе последних тенденций в области кибербезопасности, информационных технологий и методов расследования. Образовательные программы, курсы повышения квалификации и семинары должны обновляться в соответствии с новыми достижениями в этой области.

Более того, важно развивать международные платформы для обмена опытом и знаниями между специалистами различных стран, что поможет не только совершенствовать существующие методики расследования, но и повышать эффективность работы с цифровыми доказательствами [8].

Поскольку киберпреступность имеет глобальный характер, международное сотрудничество в подготовке IT-специалистов становится важным аспектом эффективной борьбы с киберугрозами. Узбекистану необходимо активно развивать связи с международными организациями, такими как Интерпол и Европол, а также участвовать в международных образовательных и научных программах, что позволит повысить уровень подготовки специалистов в области кибербезопасности.

Создание международных тренингов, конференций и семинаров, организуемых с участием мировых экспертов, даст специалистам из Узбекистана доступ к передовым методам и технологиям, что поможет укрепить позиции страны в

глобальной борьбе с киберпреступностью.

Современные тенденции, связанные с быстрым развитием информационных технологий и их интеграцией в различные области человеческой деятельности, ставят перед государствами новые задачи в сфере безопасности. Киберпреступность, которая представляет собой серьёзную угрозу для экономики, правовой системы и личных данных граждан, требует комплексного подхода, направленного на её предупреждение и расследование. В Республике Узбекистан, как и в других странах, эта проблема требует скоординированных и своевременных решений, что подчеркивает необходимость выработки стратегии противодействия киберугрозам.

Проведённый анализ основных проблем и предложений по их решению позволяет выделить четыре ключевых направления для создания эффективной системы борьбы с киберпреступностью в Узбекистане. Эти направления включают: усовершенствование механизмов раннего предупреждения, обеспечение неотвратимости наказания, внедрение инновационных технологий для выявления преступлений и привлечение высококвалифицированных IT-специалистов в правоохранительные органы.

1. **Развитие механизмов раннего предупреждения** представляет собой важный шаг в профилактике киберпреступлений. Включение систем мониторинга общественного мнения, проведение регулярных опросов и использование международного опыта для адаптации превентивных мер позволит более оперативно выявлять возникающие угрозы и адаптировать законодательство под изменяющиеся условия в киберпространстве. Важно развивать инфраструктуру, которая обеспечит своевременное реагирование на новые риски и повысит осведомлённость граждан о потенциальных угрозах.

2. **Обеспечение неотвратимости наказания** за киберпреступления является важным элементом эффективного правоприменения. Создание чёткой классификации преступлений, а также унификация правовых норм по ответственности позволит улучшить систему правосудия, повысить доверие граждан к государственным институтам и оперативно реагировать на новые формы преступности в цифровой среде.

3. **Внедрение современных технологий** в расследование и профилактику киберпреступлений является важным инструментом для борьбы с цифровыми угрозами. Применение искусственного интеллекта, машинного обучения и блокчейн-технологий позволит правоохранительным органам оперативно выявлять и отслеживать угрозы в реальном времени, минимизируя ущерб от кибератак. Важным шагом является создание круглосуточных систем мониторинга,

которые обеспечат постоянную защиту от киберугроз.

4. **Привлечение высококвалифицированных IT-специалистов** в правоохранительные органы является необходимым условием для реализации вышеуказанных инициатив. Недостаток специалистов в области кибербезопасности в Узбекистане затрудняет эффективное реагирование на новые вызовы. Для привлечения специалистов необходимо создать конкурентоспособные условия труда, а также социальные гарантии и возможности для профессионального роста. Также важным аспектом является развитие международного сотрудничества в области подготовки специалистов и обмена опытом.

Таким образом, борьба с киберпреступностью требует интеграции правовых, технологических и социальных мер, а также повышения уровня осведомленности населения. Реализация предложенных шагов позволит создать эффективную систему защиты в киберпространстве, что, в свою очередь, будет способствовать стабильному развитию цифровой экономики и защите прав граждан. В дальнейшем необходима непрерывная адаптация государственной политики в сфере кибербезопасности с учётом новых вызовов и динамичного развития технологий.

References:

1. Уголовный кодекс Республики Узбекистан от 22.09.1994 г. // Национальная база данных законодательства Республики Узбекистан Lex.uz: [Электронный ресурс]. Режим доступа: https://lex.uz/docs/111453;
2. Taplin R. – Cyber risk, intellectual property theft and cyberwarfare. Великобритания: Taylor & Francis, 2020. – С. 22. [Электронный ресурс]. Режим доступа: https://www.taylorfrancis.com/books/mono/10.4324/9780429453199/cyber-risk-intellectual-property-theft-cyberwarfare-ruth-taplin;
3. Закон Республики Узбекистан от 11.12.2003 г. No 560-II "Об информатизации" // Национальная база данных законодательства Республики Узбекистан Lex.uz: [Электронный ресурс]. Режим доступа: https://lex.uz/docs/83472;
5. Jamal A., Iqbal J. Cyber Risk and Digital Finance: Ensuring Data Privacy, Fraud Detection, and Regulatory Compliance in Financial Institutions – [Электронный ресурс]. Режим доступа: https://www.researchgate.net/profile/Javid-Iqbal-14/publication/394478566_Cyber_Risk_and_Digital_Finance_Ensuring_Data_Privacy_Fraud_Detection_and_Regulatory_Compliance_in_Financial_Institutions/links/689dbaa8fc368579b82fd1e3/Cyber-Risk-and-Digital-Finance-Ensuring-Data-Privacy-Fraud-Detection-and-Regulatory-Compliance-in-Financial-Institutions.pdf;
6. Поламарасетти А., Вадисетти Р., Вангала С.Р. – Enhancing Cybersecurity in Industrial Through AI-Based Traffic Monitoring IoT Networks and Classification // International Journal of Artificial Intelligence and Data Science. – 2022. – С. 132.

[Электронный ресурс]. Режим доступа: https://reference-global.com/download/article/10.2478/kbo-2023-0072.pdf;
7. Anvarovich QS. – Cybercrimes Committed Through Phishing and Ransomware Attacks in Uzbekistan: Analysis and Protective Measures. – World Bulletin of Management and Law, 2023. – Стр. 23-40. [Электронный ресурс]. Режим доступа: https://www.neliti.com/publications/679058/cybercrimes-committed-through-phishing-and-ransomware-attacks-in-uzbekistan-anal;
8. Deflem M., Shutt J.E. Law enforcement and computer security threats and measures. – Dumitrudumbrava.wordpress.com, 2012. – [Электронный ресурс]. Режим доступа: https://dumitrudumbrava.wordpress.com/wp-content/uploads/2012/01/law-enforcement-and-computer-security-threats-and-measures.pdf;
9. Patreliuk D., Svoboda I., Kalancha I., Filashkin V. Effective Use of Electronic Systems for International Exchange of Evidence in Criminal Investigations // Pakistan Journal of Life Sciences. 2024. [Электронный ресурс] – Режим доступа: https://pjlss.edu.pk/pdf_files/2024_2/4811-4820.pdf