Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Combating cybercrime as a crucial element in the development of modern information society in Uzbekistan

Bekhruza BAKHRIDDINOVA[1]

Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan

ARTICLE INFO

Article history:
Received August 2025
Received in revised form
15 September 2025
Accepted 15 October 2025
Available online
25 November 2025

Keywords:
information society,
cybercrime,
digitalization of law,
security strategy,
digital court proceedings,
training of specialists.

ABSTRACT

The article outlines modern measures to combat cybercrime as an integral component of developing an information society in the Republic. Based on international experience (the USA, Germany, the United Kingdom, Korea, China, Kazakhstan), organizational and legal recommendations are substantiated for strengthening anti-cybercrime measures and forming an information society.

DOI: https://doi.org/10.47689/2181-1415-vol6- iss5-pp122-127

O‘zbekistonda kiberjinoyatlarga qarshi kurash zamonaviy axborot jamiyati rivojlanishining muhim tarkibiy qismi sifatida

Kalit so‘zlar:
axborot jamiyati,
kiberjinoyatlik,
huquqni raqamlashtirish,
xavfsizlik strategiyasi,
raqamli sud jarayonlari,
mutaxassislar tayyorlash.

ANNOTATSIYA

Maqolada Respublika axborot jamiyatini rivojlantirishda muhim komponent sifatida kiberjinoyatlarga qarshi kurash bo‘yicha zamonaviy choralar yoritilgan. Xalqaro tajriba (AQSh, Germaniya, Buyuk Britaniya, Koreya, Xitoy, Qozog‘iston) asosida tashkilot-huquqiy tavsiyalar asoslangani ta’kidlangan; bu tavsiyalar kiberjinoyatlikka qarshi choralarni kuchaytirish va axborot jamiyatini shakllantirish bo‘yicha strategik yondashuvni taqdim etadi.

[1] Doctoral student, Institute of Legislation and Legal Policy under the President of the Republic of Uzbekistan
E-mail: bexruza.baxriddinova@mail.ru

Противодействие киберпреступности как важный компонент развития современного информационного общества в Узбекистане

Ключевые слова:
информационное общество, киберпреступность, цифровизация права, стратегия безопасности, цифровое судопроизводство, подготовка специалистов.

АННОТАЦИЯ

В статье представлен обзор современных мер по противодействию киберпреступности как важного компонента развития современного информационного общества в Республике Узбекистан. На основании международного опыта (США, Германия, Великобритания, Корея, Китай, Казахстан) обоснованы организационно-правовые рекомендации по укреплению мер по противодействию киберпреступности и формирования информационного общества в Республике.

Формирование в Узбекистане информационного общества развивается ускоренными темпами: с 2020 года реализуется стратегия **«Цифровой Узбекистан – 2030»**, задающая долгосрочные ориентиры цифрового развития государства [1].

По данным ООН, по итогам очередного цикла оценки электронного правительства Узбекистан вошёл в группу стран с очень высоким индексом развития e-government [2]. Одновременно растёт нагрузка на правоохранительную систему: киберпреступность выделена руководством страны в число наиболее актуальных угроз, требующих системных межведомственных и международных решений [3]. В ответ государство формирует правовую и институциональную базу противодействия киберпреступности, включая принятие специального законодательства и актов Президента, направленных на координацию усилий компетентных органов и укрепления правовых основ современной концепции информационного общества.

Стремительная цифровизация услуг, экономики и социальной сферы повышает «площадь атаки» и стимулирует миграцию традиционной преступности в онлайн-среду. Официальные данные показывают кратный рост числа преступлений, совершаемых с использованием ИКТ, за последние годы. В публичных выступлениях и материалах госорганов подчёркивается, что доля киберпреступлений в структуре регистрируемых деяний стала одной из наибольших.

Нормативная база последовательно развивается. Принят закон «О кибербезопасности», который определяет понятия, субъектов и основы обеспечения кибербезопасности [4]. Указом Президента от 30 апреля 2025 г. № ПП-153 Министерство внутренних дел определено уполномоченным координатором практики борьбы с преступлениями, совершаемыми с использованием информационных технологий, с задачей организации адресного межведомственного взаимодействия. В судебной системе последовательно накапливается массив дел по преступлениям в сфере информационных технологий: официальная платформа публикации судебных актов (public.sud.uz) отражает формирование и поиск единообразной практики по вопросам цифровых доказательств и квалификации новых составов.

Институционально в борьбе с киберпреступностью задействованы органы прокуратуры, МВД, СГБ, специализированные научно-образовательные структуры (в том числе НИИ цифровой криминалистики при Академии правоохранительных органов). В подготовке кадров участвуют Правоохранительная академия (программы магистратуры «Правовое обеспечение кибербезопасности»), ТАТУ (направление «Кибербезопасность»), Академия МВД (бакалавриат по противодействию преступности в сфере цифровых технологий), ТГЮУ (магистратура по киберправу).

Проблемные аспекты правоприменения и управления:

1) Отсутствие единой превентивной стратегии. В настоящее время не утверждён национальный стратегический документ, который бы комплексно определил цели, принципы, приоритеты и индикаторы эффективности профилактики и пресечения киберпреступности. Отсюда – фрагментарность терминологии в смежных актах, неравномерность профилактических мер, преобладание реактивной модели (реагирование post factum), сложности объективной оценки результативности. Утверждение единой межведомственной Стратегии противодействия киберпреступности на горизонте до 2030 года позволило бы задать общую «рамку» для отраслевого нормотворчества, криминалистической методики и ресурсного планирования.

2) Координация и распределение полномочий. Постановление Президента № ПП-153 закрепило общую координаторскую роль МВД [5], но в практической плоскости требуется детализация постоянных процедур обмена данными, регламент быстрой межведомственной реакции, понятные «маршруты» взаимодействия с банками, платёжными организациями, провайдерами и CERT-структурами, а также встроенные каналы к международным платформам (Europol/INTERPOL). Это позволит уйти от ситуационного формата реагирования и повысить устойчивость системы к крупным инцидентам.

3) Судебная адаптация к цифровым делам. Переход значительной части споров и преступлений в цифровую среду предъявляет особые требования к оценке электронных доказательств, атрибуции сетевой активности, учёту особенностей пользовательских соглашений и трансграничных элементов. Отдельные сложности судебной практики (разночтения в квалификации, неодинаковое понимание новых терминов) фиксируются самой системой правосудия [6]. Необходима устойчивая специализация судей и экспертов, а также регламент цифрового судопроизводства (удалённое участие, процессуальные гарантии, стандарты допустимости электронных доказательств).

4) Кадровые разрывы и методическое единство. При наличии разветвлённой сети образовательных программ остаются задачи: межведомственная координация учебных результатов (единая «матрица компетенций» для следователя / прокурора / судьи / эксперта), преемственность «бакалавриат-магистратура-повышение квалификации», «сквозные» практикумы по полному циклу: выявление – фиксация – экспертиза – процесс – исполнение. Оптимально закрепить единые стандарты подготовки и развивать национальную платформу цифровой криминалистики с общими полигонами и лабораториями [7].

США. Национальная стратегия кибербезопасности 2023 г. определяет курс на упреждающее пресечение киберугроз и усиление ответственности злоумышленников, предусматривая комплекс мер государства в сотрудничестве с частным сектором и партнёрами по кибероперациям [8].

Германия. «Стратегия кибербезопасности для Германии 2021» институционализирует борьбу с киберпреступностью как приоритет национальной киберполитики, развивает сеть специализированных подразделений полиции и прокуратуры, а также постоянные «точки контакта» для бизнеса и граждан [9].

Великобритания. Национальная киберстратегия 2022г. и инфраструктура NCA/NCCU задают проактивную модель расследования киберпреступлений, взаимодействие с провайдерами и платёжным сектором, акцент на «тёмный веб» как логистическую базу преступности [10].

Республика Корея. В 2023 г. ообновлена государственная стратегия реагирования на киберпреступность. Стратегия консолидирует меры пресечения трансграничных атак и сотрудничество с международными организациями [11].

Китай. Судебная система КНР апробировала специализированные «Интернет-суды» (начиная с Ханчжоу, 2017): официальные судебные документы фиксируют цифровой формат процесса, использование блокчейн-идентификации доказательств и обязательную переподготовку судей по цифровым делам [12].

Казахстан. Концепция кибербезопасности «Киберщит Казахстана» 2017г. закрепляет отдельное направление – борьбу с киберпреступностью, с целями правового и институционального укрепления на среднесрочный период [13].

Общий знаменатель указанных моделей: наличие утверждённой национальной стратегии; специализированного координационного ядра; формализованного международного обмена; устойчивых образовательных контуров (включая судей и прокуроров); процессуальной «цифровизации» правосудия.

Узбекистан уже создал базовые элементы правовой и организационной системы противодействия киберпреступности. Следующий шаг – переход от фрагментарной реактивности к стратегически выверенной, превентивной и координированной модели, встроенной в международную сеть обмена данными и методиками. Утверждение национальной Стратегии, регламента цифрового судопроизводства, создание координационного центра и института подготовки кадров, а также судебная специализация обеспечат устойчивость правоприменения, защиту прав граждан и бизнеса и усилят доверие к цифровой среде. Это соответствует приоритетам «Цифрового Узбекистана – 2030», международным лучшим практикам и задачам обеспечения верховенства права в условиях цифровой экономики.

Предложения организационно-правового характера для Республики Узбекистан:

1. Утвердить Концепцию и Стратегию противодействия киберпреступности до 2030 года. Документы должны определить: цели, принципы, терминологию, приоритеты (защита детей онлайн; защита платёжной инфраструктуры; охрана критической ИКТ-инфраструктуры), систему KPI, механизмы межведомственной координации и международного взаимодействия. Базой может стать межведомственная рабочая группа (Генпрокуратура, Верховный суд, МВД, СГБ, Минюст, Минцифры, Академия правоохранительных органов, профильные НИИ).

2. Принять Регламент цифрового судопроизводства. Закрепить процессуальные стандарты использования видеоконференций, удалённого участия, обращения с электронными доказательствами, цифровой идентификации участников и обеспечительных мер, а также интеграцию судебной ИТ-инфраструктуры с ведомственными системами (в пределах процессуальной тайны и персональных данных).

3. Учредить Национальный координационный центр киберпреступности при МВД. Функции: ситуационно-аналитический мониторинг; оперативно-розыскная координация; цифровая криминалистика; единый шлюз международного обмена (Europol, INTERPOL, запросы о трансграничной помощи); взаимодействие с банками, платёжными организациями, операторами связи и национальными CERT. Для центра – нормативный регламент обмена данными, SLA реагирования, протоколы эскалации.

4. Ввести судебную специализацию («судья по цифровым делам») и профильные составы. Этап 1 – пилот в г. Ташкенте (городская/межрайонная юрисдикция), этап 2 – тиражирование в регионы. Параллельно – постоянные курсы повышения квалификации по цифровым доказательствам и трансграничной правовой помощи (MLA, экстрадиция).

5. Утвердить Концепцию подготовки кадров по противодействию киберпреступности. Единая матрица компетенций для следователя, прокурора, судьи, эксперта; непрерывная траектория «бакалавриат-магистратура-повышение квалификации»; единые практикумы по полному циклу расследования и судебного рассмотрения. Развивать совместные программы с международными академиями (INTERPOL, EU-CyberNet) – на основе межведомственных соглашений.

6. Создать Национальный институт цифрового правосудия и противодействия киберпреступности. На базе НИИ цифровой криминалистики – с функциями научно-методического центра, обучения судей / прокуроров / следователей / экспертов, аккредитации учебных программ, апробации отечественных средств цифровой криминалистики, проведения «киберучений» и моделирования инцидентов.

Сноски/Iqtiboslar/References:

1. Постановление Президента Республики Узбекистан от 05.10.2020 № ПП-6079 «О мерах по реализации Стратегии “Цифровой Узбекистан – 2030”».

2. United Nations E-Government Survey 2024 (EGDI). Департамент по экономическим и социальным вопросам ООН (UN DESA).

3. Выступления и официальные сообщения Президента Республики Узбекистан (в т.ч. по вопросам киберпреступности и правопорядка), официальный сайт Президента Республики Узбекистан.

4. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 года.

5. Постановление Президента Республики Узбекистан от 30.04.2025 № ПП-153 «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с использованием информационных технологий».

6. Официальная платформа публикации судебных актов Республики Узбекистан – public.sud.uz**.**

7. Нормативные и организационные материалы Правоохранительной академии Республики Узбекистан, Ташкентского университета информационных технологий, Академии МВД, ТГЮУ (о программах подготовки кадров в сфере кибербезопасности и киберправа).

8. The White House. National Cybersecurity Strategy (2023) – официальный документ администрации США.

9. Bundesministerium des Innern und für Heimat (BMI). Cybersicherheitsstrategie für Deutschland (2021) – Стратегия кибербезопасности для Германии.

10. HM Government. National Cyber Strategy (2022); National Crime Agency (NCA) / National Cyber Crime Unit (NCCU) – официальные правительственные документы и материалы о противодействии киберпреступности в Великобритании.

11. Правительственные материалы Республики Корея о государственной стратегии реагирования на киберпреступность (обновление 2023 г.).

12. Supreme People's Court of the PRC – официальные судебные документы о создании и функционировании Интернет-судов (начиная с Hangzhou Internet Court, 2017).

13. Постановление Правительства Республики Казахстан «Об утверждении Концепции кибербезопасности "Киберщит Казахстана"» (2017).