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

Information security and criminal law measures for the protection of critical infrastructure (Legal Mechanisms for Protecting State and Strategic Facilities from Cyberattacks)

Durbek DUSMATOV[1]

Tashkent City Prosecutor's Office

ARTICLE INFO

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

Keywords:
critical information infrastructure,
information security,
criminal law,
cyber threats,
law enforcement,
international agreements,
criminal liability.

ABSTRACT

The article analyzes threats targeting critical information infrastructure (CII) and evaluates criminal-legal measures applied for its protection. The study examines the legislative framework, law enforcement practices in the Republic of Uzbekistan, international approaches (such as the Budapest Convention), as well as steps being taken in the Republic of Uzbekistan. The effectiveness of these measures is assessed, and recommendations for improving legal mechanisms to counter cyber threats are presented.

2181-1415/© 2025 in Science LLC.
DOI: https://doi.org/10.47689/2181-1415-vol6- iss5-pp145-149

Ахборот хавфсизлиги ва муҳим ахборот инфратузилмаларни киберҳужумлардан ҳимоя қилишда жиноий-ҳуқуқий чоралар (Давлат ва стратегик объектларни киберҳужумлардан ҳимоя қилиш бўйича ҳуқуқий механизмлар)

Калит сўзлар:
муҳим ахборот инфратузилмалар,
ахборот хавфсизлиги,
жиноят ҳуқуқи,
киберхавфлар,

АННОТАЦИЯ

Ушбу мақолада муҳим ахборот инфратузилмалар (МАИ)га қаратилган таҳдидлар таҳлил қилиниб, уни ҳимоя қилишда қўлланилаётган жиноят-ҳуқуқий чора-тадбирлар баҳоланади. Ўзбекистон Республикасидаги қонунчилик базаси, ҳуқуқни қўллаш амалиёти, халқаро ёндашувлар

[1] 2nd class lawyer, Prosecutor of the Department in the field of counteraction shadow economy, Tashkent City Prosecutor's Office. E-mail: bk179971@gmail.com

ҳуқуқни қўллаш,
халқаро келишувлар,
жиноий жавобгарлик.

(масалан, Будапешт конвенцияси), шунингдек, Ўзбекистон Республикасида амалга оширилаётган чора-тадбирлар кўриб чиқилади. Киберхавфларга қарши курашда ҳуқуқий механизмларнинг самарадорлиги баҳоланиб, уларни такомиллаштириш бўйича тавсиялар илгари сурилади.

Информационная безопасность и уголовно-правовые меры защиты критической инфраструктуры (Правовые механизмы защиты государственных и стратегических объектов от кибератак)

Ключевые слова:
критическая информационная инфраструктура, информационная безопасность, уголовное право, киберугрозы, правоприменение, международные соглашения, уголовная ответственность.

АННОТАЦИЯ

В статье анализируются угрозы, направленные на критическую информационную инфраструктуру (КИИ), и оцениваются уголовно-правовые меры, применяемые для её защиты. Рассмотрены законодательная база, правоприменительная практика в Республике Узбекистан, международные подходы (например, Будапештская конвенция), а также предпринимаемые шаги в Республике Узбекистан. Дана оценка эффективности и представлены рекомендации по совершенствованию правовых механизмов противодействия киберугрозам.

С развитием цифровых технологий и расширением интернет-пространства киберпреступность становится все более актуальной угрозой для государств и общества. Республика Узбекистан, активно внедряющая цифровые решения в экономику и управление, также сталкивается с ростом преступлений в киберпространстве. Эффективное противодействие требует не только технических мер, но и выработки комплексной правовой политики, направленной на предупреждение, выявление и пресечение киберпреступлений.

Критическая информационная инфраструктура, включая системы управления энергией, водоснабжением, здравоохранением, связью и финансами, становится привлекательной целью кибератак. Особенно сейчас она слабо защищена, несмотря на возрастание числа инцидентов. Риски возрастают по мере внедрения цифровых технологий и отсутствия комплексной защиты. Необходимость уголовно-правового регулирования подтверждается государственными программами Узбекистана (Закон РУз «О кибербезопасности» 2022) и постановлением ПП–167 (2023).

Согласно данным Министерства внутренних дел Республики Узбекистан, количество преступлений, совершенных с использованием информационных технологий, выросло на 45% в 2023 году по сравнению с предыдущим периодом. Наиболее распространёнными являются случаи фишинга, мошенничества с использованием банковских карт, DDoS-атаки и несанкционированный доступ к информационным системам.

Узбекистан законодательство определяет объекты КИИ как «комплекс автоматизированных систем управления, информационных систем и ресурсов сетей имеющих стратегическое и социально-экономическое значение». Закон

выделяет категории объектов высокого, среднего и низкого уровня, что позволяет дифференцировать подходы к защите. Кибератаки на КИИ могут быть безобидными на первый взгляд, но привести к серьёзным последствиям – отключение электросетей, нарушение водоснабжения, сбои в здравоохранении.

Будапештской конвенция, принятая в 2001 году, является основным международным договором по борьбе с киберпреступностью. В ней четко прописаны правовые элементы, включая незаконный доступ, интерцепцию, вмешательство в системы (DATA INTERFERENCE), компьютерное мошенничество и др. С 2023 г. Римский статут и ICC рассматривает серьёзные кибератаки по критической инфраструктуре как возможные военные преступления, если они нарушают международные нормы. Например, кибератаки на больницы или энергосистемы могут быть квалифицированы как военные преступления.

Более того, имеются и другие примеры юрисдикции в Евросоюзе регулирования NIS2 и DORA предусматривают жесткие требования к защите КИИ и ответственность за их нарушение, в КНДР принят закон «Cybersecurity Law» регулирует безопасность ключевой инфраструктуры, включая интернет-провайдеров, энергетический сектор и госорганы, в США принят Акт «National Cybersecurity and Critical Infrastructure Protection Act (2013)» который устанавливает обязанности DHS и координацию с частным сектором для защиты КИИ.

Исходя из вышеизложенного, стоит отметить тот факт, что и в Республике Узбекистан, несомненно, уделяются огромное внимание со стороны государства на защиту КИИ, был принят Закон «О кибербезопасности» определяющий Службу государственной безопасности как уполномоченный орган по кибербезопасности. В ней регламентированы функции по оперативному реагированию и инцидентам, определен правовой статус КИИ, категоризация объектов, создание реестра и сертификация средств защиты инфраструктуры.

Законом СГБ предоставлены полномочия доступа в госорганы и объекты КИИ, проведение проверок, право на запросы и форсированный доступ, при этом регулируются уведомления прокуратуры и возмещение ущерба.

Более того, Президентом Республики Узбекистан подписано Постановление от 31.05.2023 г. № ПП–167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» где критической информационной инфраструктурой является комплекс автоматизированных систем управления, информационных систем и ресурсов сетей и технологических процессов, имеющих важное стратегическое и социально-экономическое значение.

В документе установлено, что информация о назначении работников, ответственных за обеспечение кибербезопасности, на должность и освобождении от нее, проведении аттестации передается в СГБ. Аттестация указанных работников проводится со стороны службы каждые 3 года.

Документом утверждено Положение о порядке обеспечения кибербезопасности объектов критической информационной инфраструктуры (КИИ). Оно определяет основные задачи системы кибербезопасности:

- предотвращение неправомерного использования, удаления, изменения, блокирования (ограничения), копирования, предоставления и распространения информации, обрабатываемой на объектах КИИ, а также иных неправомерных действий;

• недопущение воздействия на аппаратные, программные и программно--аппаратные средства обработки информации, способного вызвать нарушение и (или) остановку работы объектов КИИ;

• восстановление работы объектов КИИ путем резервирования телекоммуникационных сетей, информационных ресурсов и системы жизнедеятельности.

В постановлении также приведены общие требования кибербезопасности объектов КИИ.

Наряду с реформированием и модернизацией законодательства в сфере противодействия киберпреступности и вопросах по обеспечению КИИ, уголовно-правовых аспектах существуют пробелы и проблемы прямой ответственности.

На уровне Уголовного кодекса Республики Узбекистан пока отсутствует специализированная статья за незаконные действия против КИИ. В перспективе целесообразно предусмотреть ответственность за вмешательство в систему управления, создание угроз целостности, блокирование работы КИИ. Например, в КНР уголовная ответственность налагается на разрушение ключевой инфраструктуры, серьёзные перебои. Подобные подходы можно адаптировать и в Республике Узбекистан, предусмотреть ввод санкций за создание рисков или инцидентов.

При этом стоит отметить и пробелы в сборе доказательств, существует угроза доказуемости, то есть нужно фиксировать инциденты, сохранять лог-информацию, использовать систему журналирования, форензику. В Узбекистане уже предусмотрено для участников КИИ.

Исходя из вышеизложенного, предлагается предпринять меры по совершенствованию законодательства в сфере противодействия киберпреступности и создать правовые механизмы защиты критической информационной инфраструктуры, тем самым предлагается:

• **Разработать и принять в Уголовный кодекс Республики Узбекистан отдельную статью** за незаконное вмешательство в КИИ с дифференциацией санкций в зависимости от ущерба и субъективной стороны преступления.

• **Обеспечить соблюдение требований по сертификации и проведению аудита КИИ**, гарантирующей техническую, организационную, финансовую устойчивость.

• **Усилить ответственность операторов КИИ** за несообщение о киберинцидентах, внедрение простых, но надёжных регламентов.

• **Стимулировать сотрудничество гражданского и государственного секторов**, создавать совместные центры реагирования на инциденты, обмениваться разведывательными данными (THREAT INTELLIGENCE).

• **Укрепить международное сотрудничество** – присоединиться к Будапештской конвенции, применять стандарты ICC и NIS2/DORA, адаптировать опыт Китая и США.

• **В подготовке кадров** – проводить обязательные тренинги, курсы повышения квалификации, сертификация, форензик-экспертизы, проводить профилактические меры среди специалистов и пользователей КИИ.

В заключении стоит отметить, что информационная безопасность критической инфраструктуры – ключевой элемент национальной безопасности. Несмотря на меры, предпринятые государством, существуют и остаются пробелы в уголовно-правовом регулировании и на практике. Полноценная защита требует

принятия специализированной нормы в уголовный кодекс, проведения технического аудита, ответственности операторов, подготовки кадров и международной координации. Только такой комплексный подход позволит эффективно противостоять современным угрозам.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Министерство внутренних дел Республики Узбекистан. Годовой отчет о состоянии преступности в 2023 году. URL: https://mvd.uz (дата обращения: 19.05.2025).

2. Уголовный кодекс Республики Узбекистан. Принят 22 сентября 1994 года (в ред. от 2024 года).

3. Закон Республики Узбекистан «О кибербезопасности» от 15 апреля 2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан.

4. Постановление Президента Республики Узбекистан от 31 мая 2023 г. № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан».

5. Будапештская конвенция о киберпреступности от 23 ноября 2001 г. // Совета Европы. ETS No.185.

6. Бронников А.В. Информационная безопасность: правовые и организационные аспекты. – М.: Юрайт, 2020.

7. Дубов Д.В. Киберугрозы в сфере критической информационной инфраструктуры и подходы к их нейтрализации. // Информационное право. – 2022. – № 2. – С. 23–31.

8. Нечаев А.В. Уголовно-правовая охрана критически важной инфраструктуры: проблемы и перспективы. // Журнал российского права. – 2021. – № 9. – С. 44–52.

9. Политов С.В. Защита критической информационной инфраструктуры от киберугроз: международно-правовые аспекты. // Безопасность в цифровом мире. – 2023. – № 1(13). – С. 15–21.

10. Cybersecurity Law of the People's Republic of China (2017) // National People's Congress. https://npcobserver.com

11. National Cybersecurity and Critical Infrastructure Protection Act of 2013 // U.S. House of Representatives.

12. European Union Agency for Cybersecurity (ENISA). NIS2 Directive. – 2022. https://www.enisa.europa.eu

13. The International Criminal Court and Cyberwarfare // Wired Magazine. – 2023. https://www.wired.com

14. Gazeta.uz. В Узбекистане принят закон о кибербезопасности. – 18.04.2022. https://www.gazeta.uz/ru/2022/04/18/cyber-safety

15. Yuz.uz. Как в Узбекистане обеспечат кибербезопасность объектов критической инфраструктуры. – 10.05.2023. https://yuz.uz/ru/news/kak-v-uzbekistane-obespechat-kiberbezopasnost