

ГЛОБАЛЬНЫЕ ВЫЗОВЫ КИБЕРПРЕСТУПНОСТИ И ЗАЩИТА ЦИФРОВЫХ ПРАВ ГРАЖДАН: МЕЖДУНАРОДНЫЕ СТАНДАРТЫ И НАЦИОНАЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО

Ахмаджужаев Шохруххон Зикирийёхон зода

Ферганский юридический техникум

Студенты 2 курса группы 44-24 направления

«Судебно-правовая деятельность»

Аннотация: В данной статье рассматриваются глобальные проблемы борьбы с киберпреступностью и механизмы обеспечения цифровых прав граждан в современную эпоху информационного общества. Анализируются международно-правовые подходы к противодействию правонарушениям в сети Интернет, включая Будапештскую конвенцию и инициативы ООН. Особое внимание уделяется развитию цифрового законодательства в Республики Узбекистан, вопросам модернизации Уголовного кодекса, защите персональных данных, а также роли молодых специалистов судебно-правовой системы в расследовании и судебном рассмотрении киберпреступлений.

Ключевые слова: киберпреступность, цифровые права, информационная безопасность, персональные данные, международное право, Уголовный кодекс, Республика Узбекистан, цифровая трансформация, судебно-правовая деятельность.

В эпоху стремительной цифровизации и построения глобального информационного общества традиционные институты права сталкиваются с принципиально новыми вызовами. Стремительное развитие интернет-технологий, искусственного интеллекта и электронной коммерции породило новую категорию угроз, не имеющих государственных границ — киберпреступность. Защита цифровых прав граждан, их конфиденциальности и личных данных в виртуальном пространстве стала одной из самых актуальных и масштабных задач для судебно-правовых систем всех государств мира.

Глобальный характер киберугроз требует от юридического сообщества выработки универсальных правовых дефиниций и механизмов взаимодействия. Преступления в сфере высоких технологий — от онлайн-мошенничества и кражи персональных данных до кибератак на критическую инфраструктуру — совершаются дистанционно и анонимно. В связи с этим традиционные методы расследования и сбора доказательств оказываются недостаточно эффективными, что стимулирует развитие нового направления в юриспруденции — цифрового права.

Следует отметить, что защита прав человека в цифровом пространстве является прямым продолжением фундаментальных прав и свобод, гарантированных международными пактами. Право на тайну переписки, неприкосновенность частной жизни и защиту чести и достоинства в сети Интернет требует создания надежного правового щита. Именно поэтому изучение международных стандартов кибербезопасности становится ключевым элементом подготовки юристов нового поколения.

В Республике Узбекистан, реализующей масштабную стратегию «Цифровой Узбекистан — 2030», вопросам ИТ-безопасности и защиты цифровых прав граждан уделяется приоритетное внимание. В условиях интеграции государственных услуг и финансовых сервисов в цифровые платформы, надежное правовое регулирование виртуальной среды выступает гарантом экономической стабильности и доверия населения к государственным институтам.

Особое значение в данном процессе имеет модернизация уголовного, уголовно-процессуального и административного законодательства страны. В последние годы в Узбекистане были существенно дополнены и детализированы нормы, предусматривающие ответственность за несанкционированный доступ к компьютерной информации, создание вредоносных программ и модификацию данных. Закрепление этих норм позволяет правоохранительным органам и судам более эффективно квалифицировать преступления в ИТ-сфере.

Понимание природы киберпреступлений критически важно для студентов юридических техникумов, обучающихся по направлению «Судебно-правовая деятельность». Будущим сотрудникам судов, прокуратуры и следственных органов придется ежедневно сталкиваться с цифровыми доказательствами (логами, IP-адресами, электронными документами). Освоение навыков работы с цифровой криминалистикой на этапе обучения закладывает прочную базу для их дальнейшей успешной профессиональной деятельности.

Одним из важнейших элементов международно-правового сотрудничества в этой сфере являются международные конвенции и стандарты ООН по борьбе с использованием информационно-коммуникационных технологий в преступных целях. Узбекистан активно поддерживает международные инициативы, направленные на создание единого безопасного цифрового пространства, и гармонизирует национальное законодательство с передовым зарубежным опытом.

Следует подчеркнуть, что важным шагом на пути защиты прав граждан стало принятие Закона Республики Узбекистан «О персональных данных». Данный нормативно-правовой акт жестко регламентирует процессы сбора, обработки и хранения личной информации государственными и частными

структурами, устанавливая юридическую ответственность за утечку данных. Это существенно повысило уровень цифровой защищенности населения.

Особую роль в снижении уровня киберпреступности играет правовое и цифровое просвещение граждан. Большинство преступлений в сети, таких как фишинг или социальная инженерия, совершаются из-за недостаточной цифровой грамотности жертв. Проведение правовых марафонов, семинаров и создание доступных образовательных ресурсов силами юридических клиник и студенческих сообществ способствует формированию у населения культуры безопасного поведения в интернете.

Кроме того, глобальные ИТ-вызовы требуют развития института экспертизы. В судебно-правовой практике Узбекистана активно развивается направление судебно-компьютерно-технической экспертизы, которая позволяет восстанавливать удаленную информацию, идентифицировать пользователей и устанавливать точную хронологию кибератак. Квалифицированное использование таких экспертиз является залогом вынесения справедливых судебных решений.

Важную роль в борьбе с киберпреступностью играют специализированные подразделения Министерства внутренних дел и Службы государственной безопасности Республики Узбекистан. Создание профильных центров по борьбе с киберпреступлениями позволяет оперативно реагировать на угрозы, блокировать мошеннические ресурсы и координировать действия с международными партнерами, такими как Интерпол.

В последние годы в стране также внедряются современные стандарты защиты прав детей в цифровой среде. Учитывая, что молодое поколение является наиболее активным пользователем интернета, законодательство Узбекистана предусматривает механизмы фильтрации контента, наносящего вред психическому и нравственному развитию несовершеннолетних, что соответствует международным конвенциям о правах ребенка.

Особую роль в практической подготовке будущих специалистов играет изучение реальных уголовных и гражданских дел, связанных с правонарушениями в интернете. Анализ судебных precedентов помогает студентам понять тонкости разграничения юрисдикции при трансграничных преступлениях, а также особенности применения обеспечительных мер, таких как арест цифровых активов или электронных счетов.

Следует отметить, что обеспечение кибербезопасности тесно связано с развитием электронной коммерции и защитой прав потребителей в сети. Четкие правовые алгоритмы возврата средств, верификации продавцов и защиты платежных систем стимулируют рост доверия к цифровой экономике и способствуют интеграции Узбекистана в мировое экономическое пространство.

Однако в сфере противодействия киберпреступности остаются определенные проблемы. К ним относятся высокая динамика изменения способов совершения преступлений (использование дипфейков, криптовалют для сокрытия доходов), дефицит кадров, обладающих одновременно глубокими юридическими и техническими знаниями, а также необходимость дальнейшего упрощения процедур международного запроса цифровых данных.

Для решения данных проблем необходимо внедрять специализированные междисциплинарные курсы по ИТ-праву в юридических учебных заведениях, укреплять техническую базу следственных и судебных органов, а также развивать государственно-частное партнерство между правоохранительными органами и ведущими технологическими компаниями.

Международный опыт показывает, что наиболее успешную модель борьбы с киберугрозами демонстрируют страны, создавшие гибкое законодательство, способное оперативно адаптироваться к технологическому прогрессу. Эффективная защита цифровых прав граждан является важнейшим показателем современности правовой системы и авторитета государства на международной арене.

Таким образом, глобальные вызовы киберпреступности требуют от судебно-правовой системы Узбекистана непрерывного совершенствования. Объединение международных стандартов, сильной национальной законодательной базы и высокого профессионализма молодых юристов позволит обеспечить надежную безопасность личности, общества и государства в цифровом веке.

Заключение

Подводя итог, можно сделать вывод о том, что противодействие киберпреступности и защита цифровых прав граждан представляют собой ключевой вектор развития современной юриспруденции. Международное сотрудничество и своевременная модернизация национального законодательства являются главными условиями построения безопасного цифрового пространства.

В Республике Узбекистан планомерная работа по укреплению информационной безопасности и защите персональных данных открывает новые стандарты правосудия в рамках Нового Узбекистана. Подготовка юристов, способных эффективно работать в условиях цифровой трансформации, выступает залогом успешной защиты прав граждан.

Для дальнейшего совершенствования системы борьбы с киберпреступностью необходимо:

- продолжить имплементацию международных стандартов и конвенций ООН в сфере кибербезопасности в национальное законодательство;

- разработать и принять комплексный Цифровой кодекс Республики Узбекистан;
- внедрять специализированные программы повышения квалификации для судей и следователей по работе с цифровыми доказательствами;
- повышать уровень цифровой и правовой грамотности населения для профилактики интернет-мошенничества;
- оптимизировать механизмы международного сотрудничества по вопросам выдачи киберпреступников и трансграничного обмена цифровыми данными;
- активно привлекать молодых специалистов и студентов юридических техникумов к разработке проектов в сфере ИТ-права и защиты прав пользователей.

Эффективное развитие правовых и технических механизмов в цифровой сфере будет способствовать надежной защите прав граждан, укреплению общественной безопасности и успешному развитию демократического правового государства в Республике Узбекистан.

Литература

1. Конституция Республики Узбекистан. — Ташкент, 2023.
2. Закон Республики Узбекистан «О персональных данных» от 02.07.2019 г. № ЗРУ-547.
3. Закон Республики Узбекистан «О кибербезопасности» от 15.04.2022 г. № ЗРУ-764.
4. Уголовный кодекс Республики Узбекистан (Глава XX¹ «Преступления в сфере информационных технологий»).
5. Конвенция ООН против транснациональной организованной преступности (2000 г.).
6. Мирзиёев Ш. М. Стратегия «Цифровой Узбекистан — 2030». — Ташкент, 2020.
7. Рустамбаев М. Х. Комментарий к Уголовному кодексу Республики Узбекистан. — Ташкент: Адолат, 2023. — 620 с.
8. Исмаилов А. А. Цифровое право и кибербезопасность: учебное пособие для юридических специальностей. — Ташкент: Юрист-медиа, 2025. — 190 с.
9. Официальный портал законодательства Республики Узбекистан — Lex.uz (дата обращения: 19.05.2026).