КИБЕРПРЕСТУПНОСТЬ В УЗБЕКИСТАНЕ

Боборахимов Сардор Уктамович
Студент 1 курса Университет Sarbon
Узбекистан
sardorboborahimov11@gmail.com

Аннотация. *В статье рассматриваются актуальные проблемы киберпреступности в Республике Узбекистан, анализируются основные виды преступлений в цифровой среде, а также действующие меры правового регулирования и противодействия киберугрозам. Особое внимание уделяется вопросам защиты персональных данных, совершенствованию уголовного законодательства и развитию международного сотрудничества в сфере кибербезопасности.*

Ключевые слова: *киберпреступность, кибербезопасность, цифровые технологии, Узбекистан, информационная безопасность, персональные данные, интернет-мошенничество.*

CYBERCRIME IN UZBEKISTAN

Sardor Uktamovich Boborahimov
First-year student Sarbon University
Uzbekistan
sardorboborahimov11@gmail.com

Abstract. *The article examines current issues of cybercrime in the Republic of Uzbekistan, analyzes the main types of crimes committed in the digital environment, and studies existing legal measures aimed at combating cyber threats. Particular attention is paid to the protection of personal data, improvement of criminal legislation, and development of international cooperation in the field of cybersecurity.*

Keywords: *cybercrime, cybersecurity, digital technologies, Uzbekistan, information security, personal data, internet fraud.*

Введение

В условиях стремительного развития цифровых технологий и расширения интернет-пространства проблема киберпреступности приобретает особую актуальность. В Республике Узбекистан активно развивается цифровая экономика, внедряются электронные государственные услуги, банковские онлайн-системы и современные информационные платформы. Вместе с тем рост цифровизации

сопровождается увеличением количества преступлений, совершаемых в киберпространстве.

Киберпреступность представляет серьёзную угрозу как для государства, так и для общества в целом, поскольку посягательства в цифровой среде могут причинять значительный материальный ущерб, нарушать права граждан и подрывать информационную безопасность страны. В связи с этим возникает необходимость совершенствования правовых механизмов противодействия киберугрозам и адаптации законодательства к современным технологическим реалиям.

Основная часть

На сегодняшний день в Узбекистане вопросам кибербезопасности уделяется значительное внимание на государственном уровне. Принимаются меры по укреплению информационной безопасности, развитию цифровой инфраструктуры и защите персональных данных граждан. Вместе с тем киберпреступность продолжает развиваться, приобретая всё более сложные формы.

Среди наиболее распространённых видов киберпреступлений можно выделить:

- интернет-мошенничество;
- незаконный доступ к компьютерной информации;
- кражу персональных данных;
- распространение вредоносного программного обеспечения;
- взлом банковских и электронных систем;
- кибератаки на государственные информационные ресурсы.

Особую опасность представляет интернет-мошенничество, связанное с хищением денежных средств через банковские карты, мобильные приложения и фишинговые сайты. В большинстве случаев преступники используют методы социальной инженерии, вводя пользователей в заблуждение с целью получения конфиденциальной информации.

Правовую основу противодействия киберпреступности составляют нормы Уголовного кодекса Республики Узбекистан, Закона Республики Узбекистан «О кибербезопасности», а также законодательства в сфере информационных технологий и защиты персональных данных. Однако существующие нормы не всегда способны эффективно регулировать быстро меняющиеся цифровые отношения.

Одной из ключевых проблем является сложность выявления и расследования киберпреступлений. Многие преступления совершаются анонимно, с использованием зарубежных серверов и технологий сокрытия личности. Это существенно затрудняет деятельность правоохранительных органов и требует развития международного сотрудничества в сфере борьбы с киберугрозами.

Кроме того, актуальной остаётся проблема недостаточной цифровой грамотности населения. Пользователи нередко становятся жертвами мошенников из-за незнания базовых правил информационной безопасности. В связи с этим важное значение

приобретает проведение профилактических мероприятий и повышение уровня киберкультуры общества.

Существенным направлением совершенствования законодательства является разработка более эффективных механизмов защиты персональных данных. В условиях активного использования цифровых сервисов возрастает риск утечки конфиденциальной информации, что требует усиления контроля за обработкой и хранением данных.

Перспективы развития системы противодействия киберпреступности связаны с внедрением современных технологий защиты информации, совершенствованием деятельности специализированных подразделений, а также развитием международного обмена опытом. Особое значение имеет подготовка квалифицированных специалистов в области кибербезопасности и цифрового права.

Заключение

Таким образом, киберпреступность является одной из наиболее серьёзных угроз современной цифровой эпохи. В условиях активной цифровизации Узбекистана возникает необходимость дальнейшего совершенствования законодательства и укрепления системы кибербезопасности. Несмотря на принимаемые меры, существующие правовые механизмы требуют дальнейшего развития и адаптации к новым видам цифровых угроз.

Эффективное противодействие киберпреступности возможно только при комплексном подходе, включающем совершенствование законодательства, развитие международного сотрудничества, повышение цифровой грамотности населения и внедрение современных технологий информационной защиты.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Уголовный кодекс Республики Узбекистан* : принят 22 сентября 1994 г. : введён в действие с 1 апреля 1995 г. – Ташкент : Министерство юстиции Республики Узбекистан. – (в ред. действующих изменений).
2. *О кибербезопасности* : Закон Республики Узбекистан от 15 апреля 2022 г. № ЗРУ-764 // Национальная база данных законодательства Республики Узбекистан. – Ташкент, 2022.
3. *О персональных данных* : Закон Республики Узбекистан от 2 июля 2019 г. № ЗРУ-547 // Национальная база данных законодательства Республики Узбекистан. – Ташкент, 2019.
4. Материалы Министерства цифровых технологий Республики Узбекистан [Электронный ресурс] / Министерство цифровых технологий Республики Узбекистан. – Режим доступа: https://mict.uz. – Дата обращения: 2024.

5. Международные документы и рекомендации в сфере кибербезопасности : [сб. документов] / Международный союз электросвязи (МСЭ) ; Организация Объединённых Наций. – Женева : МСЭ, 2020–2024.