

КИБЕРПРЕСТУПНОСТЬ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ В ИНТЕРНЕТЕ

Абдуалимова Дилфуза Хикматовна

ведущий преподаватель Академического лицея при ТГЮУ им М.С.Васиковой

Абдуманнопова Шодиёна Музaffer кизи

учащийся 2-курса Академического лицея при ТГЮУ им М.С.Васиковой

Аннотация: В статье рассматриваются вопросы киберпреступности, её виды, причины и последствия для общества. Особое внимание уделено правовому регулированию интернет-пространства в Республике Узбекистан, анализу действующего законодательства и мер, принимаемых государством для защиты информационной безопасности.

Ключевые слова: киберпреступность, интернет, информационная безопасность, кибератака, правовое регулирование, Узбекистан, цифровизация.

В современном мире интернет стал неотъемлемой частью жизни человека. Развитие цифровых технологий способствует прогрессу во всех сферах, однако одновременно создаёт новые угрозы — киберпреступления. С каждым годом их количество увеличивается, и государствам необходимо разрабатывать эффективные правовые механизмы противодействия им. Республика Узбекистан не является исключением и активно формирует законодательную базу в области кибербезопасности.

Киберпреступность — это преступная деятельность, совершаемая с использованием информационно-коммуникационных технологий (ИКТ).

К основным видам киберпреступлений относятся:

несанкционированный доступ к компьютерным системам;

кража персональных данных и финансовых средств;

распространение вредоносных программ (вирусов);

кибермошенничество;

распространение запрещённой информации (экстремизм, фишинг, фейки);

атаки на государственные и банковские системы.

В Узбекистане, по данным Министерства внутренних дел и Агентства по кибербезопасности, ежегодно фиксируется рост числа подобных преступлений, особенно в финансовом секторе.

Правовое регулирование киберпространства в Узбекистане

Узбекистан предпринимает активные шаги по формированию нормативно-правовой базы в области кибербезопасности. Основные документы включают:

Закон Республики Узбекистан «Об информатизации» (новая редакция, 2020 г.) – регулирует порядок создания и защиты информационных систем.

Закон «О защите персональных данных» (2019 г.) – определяет механизмы хранения и обработки личной информации граждан.

Постановление Президента Республики Узбекистан №ПП-3832 от 3 июля 2018 года – о создании Центра кибербезопасности при Министерстве цифровых технологий.

Стратегия «Цифровой Узбекистан – 2030» – направлена на развитие цифровой экономики и повышение устойчивости к киберугрозам.

Также ведётся сотрудничество с международными организациями, такими как INTERPOL, ITU, OSCE, для обмена опытом и совершенствования законодательства.

Государственная политика и профилактика киберпреступлений

Государственные органы Узбекистана проводят масштабные мероприятия по защите населения от киберугроз.

Среди них:

внедрение систем мониторинга и реагирования на инциденты в киберпространстве;
повышение цифровой грамотности граждан;

создание специализированных подразделений по борьбе с киберпреступностью при МВД и СНБ;

организация тренингов и образовательных программ для молодёжи.

Важным направлением является развитие национальных программ по защите детей от опасностей в интернете, а также контроль за деятельностью социальных сетей.

Проблемы и перспективы

Несмотря на положительные результаты, остаются нерешённые вопросы:

недостаточный уровень правовой культуры пользователей;

быстрое развитие технологий, опережающее законодательство;

международный характер киберпреступлений.

В перспективе необходимо:

совершенствовать правовые нормы в соответствии с международными стандартами (Будапештская конвенция о киберпреступности);

развивать сотрудничество с другими странами;

внедрять национальные системы сертификации и защиты программного обеспечения.

Заключение, Киберпреступность представляет собой одну из ключевых угроз национальной безопасности в эпоху цифровизации. Узбекистан предпринимает последовательные шаги для формирования безопасного киберпространства, создавая правовые, технические и организационные механизмы защиты. Повышение цифровой культуры населения и международное сотрудничество остаются основными факторами успешной борьбы с киберпреступностью.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон Республики Узбекистан «Об информатизации». – Ташкент, 2020.
2. Закон Республики Узбекистан «О защите персональных данных». – Ташкент, 2019.
3. Постановление Президента Республики Узбекистан №ПП-3832 от 03.07.2018 г. «О мерах по совершенствованию системы обеспечения кибербезопасности Республики Узбекистан».

4. Стратегия «Цифровой Узбекистан – 2030». – Министерство цифровых технологий, Ташкент, 2020.
5. Агентство по кибербезопасности Республики Узбекистан – <https://cda.uz>
6. Интерпол. Отчёт о киберугрозах в Центральной Азии. – 2023.