VOLUME:3 ISSUE:3

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ: НАЦИОНАЛЬНАЯ СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В ЦИФРОВОМ МИРЕ

Базарова Сарвинозхон Санжар кизи
Федерация профсоюзов Узбекистана Академия труда и социальных отношений Факультет управления трудовой сферой Направление «Юриспруденция» Студентка 4-го курса
Тел.: +998909008780
E-mail: sarvinozxonbazarova1@gmail.com

Аннотация. *В данной статье анализируются вопросы укрепления правового обеспечения кибербезопасности и противодействия новым угрозам в цифровом пространстве. В связи с быстрым развитием цифровых технологий информационные системы, государственное управление, экономика, а также персональные данные граждан подвергаются риску кибератак. В этом контексте в статье рассматриваются нормативно-правовая база Узбекистана в сфере кибербезопасности, международные стандарты и опыт, а также основные направления национальной стратегии безопасности.*
Ключевые слова: *кибербезопасность; киберпреступность; цифровые угрозы; информационная безопасность; информационные технологии; защита данных; кибератака; цифровая грамотность; противодействие кибератакам.*

Annotation. *This article analyzes the issues of strengthening legal support in the field of cybersecurity and combating new threats emerging in the digital space. As a result of the rapid development of digital technologies, information systems, public administration, the economy, and citizens' personal data are exposed to the threat of cyberattacks. In this regard, the article highlights the regulatory and legal framework of the Republic of Uzbekistan on cybersecurity, international standards and practices, as well as the main directions of the national security strategy.*
Key words: *cybersecurity; cybercrime; digital threats; information security; information technologies; data protection; cyberattack; digital literacy; cyber defense.*

ВВЕДЕНИЕ

В последние годы цифровые технологии проникли во все сферы жизни. Государственное управление, экономика, образование, здравоохранение и даже личная жизнь реализуются через цифровые платформы. В таких условиях надежность и безопасность информационных систем становятся неотъемлемой частью национальной безопасности. Государственные и частные структуры, а также граждане, работающие в цифровом пространстве, всё чаще сталкиваются с угрозами киберпреступности, кражи данных, кибератак и распространения ложной информации.

Обеспечение кибербезопасности не ограничивается только техническими мерами, оно требует правового регулирования, международного сотрудничества, повышения информационной культуры, а также последовательной реализации национальной стратегии. В этой связи в последние годы в Республике Узбекистан принимаются нормативно-правовые акты, направленные на правовое укрепление

кибербезопасности, защиту информационной инфраструктуры и обеспечение цифрового суверенитета.

В данной статье анализируются теоретические и практические аспекты правового обеспечения кибербезопасности, национальная стратегия противодействия угрозам в цифровой среде, а также вопросы изучения международного опыта и его внедрения в национальную систему.

Правовое обеспечение кибербезопасности и угрозы цифрового мира

XXI век с полным основанием можно назвать «цифровым веком». Сегодня почти все сферы жизни населения мира зависят от интернета и информационных технологий. Электронные государственные системы, интернет-банкинг, онлайн-торговля, цифровое образование, медицинские информационные базы — всё это облегчает человеческую деятельность, но одновременно создает новые риски. Быстрое распространение информации, развитие технологий и открытые сети создают благоприятные условия для киберпреступлений. Поэтому обеспечение кибербезопасности рассматривается не только как техническая, но и как стратегическая задача.

Сам термин «кибербезопасность» состоит из слов «кибер» (связанный с цифровыми сетями) и «безопасность» и подразумевает защиту информационных систем, компьютерных сетей и пользовательских данных от несанкционированного доступа, кражи, повреждения или уничтожения. Первоначально это понятие применялось только в техническом контексте, сегодня оно превратилось в сложную систему с политическим, экономическим и правовым значением.

В цифровом мире существует множество факторов, угрожающих безопасности. Одним из наиболее распространенных является киберпреступность. Она проявляется в различных формах: взлом банковских карт, фишинг через поддельные веб-сайты для кражи данных пользователей, распространение вредоносного ПО, атаки на государственные информационные системы, а также создание фальшивых изображений и видео с помощью искусственного интеллекта (deepfake) для манипуляции людьми. Иногда эти атаки наносят ущерб не только отдельным лицам, но и всей экономической системе или государственному управлению. Поэтому сегодня кибербезопасность признается неотъемлемой частью национальной безопасности.

Одним из ключевых факторов обеспечения цифровой безопасности является правовая база. Любая технологическая система защиты без закрепления законом не может быть устойчивой в долгосрочной перспективе. В Узбекистане в последние годы проведена значительная работа в этом направлении. Законы «Об

информатизации», «О персональных данных», «Об электронном правительстве» и «О кибербезопасности» формируют правовую основу в этой сфере. Эти нормативные акты четко определяют порядок защиты информационных ресурсов государства и частного сектора, а также правила сбора, хранения и обработки персональных данных пользователей.

Например, закон «О персональных данных» гарантирует каждому гражданину права в цифровой среде. Никто не имеет права собирать данные гражданина или передавать их третьим лицам без его согласия. Эта норма сохраняет конфиденциальность граждан и укрепляет доверие в цифровой среде. Кроме того, создан «Центр кибербезопасности», который ведет постоянную работу по выявлению уязвимостей государственных информационных систем, реагированию на угрозы и повышению уровня защиты.

Однако кибербезопасность не может быть решена только в пределах одной страны, поскольку интернет не знает границ. Пользователь, находящийся в Ташкенте, может подвергаться атаке киберпреступника с другой части света. Поэтому международное сотрудничество имеет решающее значение. Будапештская конвенция (2001) является одним из ключевых международных документов по борьбе с киберпреступностью. Многие страны присоединились к этой конвенции и создали системы обмена информацией для поиска и наказания преступников. Узбекистан также активно работает над укреплением сотрудничества с международными организациями и внедрением передового опыта в национальное законодательство.

Правовое обеспечение кибербезопасности должно включать не только механизмы наказания, но и профилактику. Это связано с повышением цифровой культуры населения, обучением правильному использованию интернета, избеганию опасных ссылок, применению надежных паролей и защите персональных данных. Часто киберпреступники используют психологические методы воздействия на человека — это так называемая «социальная инженерия». Поэтому наряду с техническими средствами защиты необходимо учитывать человеческий фактор.

Еще одним направлением укрепления кибербезопасности является подготовка квалифицированных специалистов. Развитие образовательных программ в области информационной безопасности, проведение соревнований по кибербезопасности среди молодежи и организация практических лабораторий позволяют готовить высококвалифицированные кадры. Для управления современными системами необходимы знания и опыт.

Сегодня одной из глобальных проблем является огромное количество данных и сложность их управления. Ежедневно миллиарды данных обмениваются через интернет, поэтому каждый пользователь сети несет ответственность за собственную безопасность. Государство управляет этим процессом через законы, политику и системы контроля.

Цифровой мир несет как возможности, так и угрозы. Правовое обеспечение кибербезопасности является одним из важнейших направлений защиты современного общества. Только при сочетании правовой базы, технических средств защиты, международного сотрудничества и цифровой культуры населения возможно построение безопасного цифрового будущего. Кибербезопасность — это не просто техническая задача, это система, защищающая интересы человека, общества и государства, обеспечивающая мирную и стабильную жизнь.

Рекомендации по защите от кибератак:

1. Политика надежных паролей и управление паролями
   Создавайте уникальные пароли для каждой учетной записи, длиной не менее 12 символов, с использованием комбинации заглавных и строчных букв, цифр и специальных символов. Не сохраняйте пароли в браузере, рекомендуется использовать надежный менеджер паролей.
2. Двухфакторная (двухкомпонентная) аутентификация
   Включите подтверждение входа не только через логин и пароль, но и через телефон или приложение-аутентификатор. Это значительно усложняет злоумышленникам доступ к системе даже при известном пароле.
3. Регулярное обновление программного обеспечения и систем
   Периодически обновляйте операционные системы, приложения, серверы и прошивки маршрутизаторов — это позволяет закрывать уязвимости типа zero-day и другие.
4. Резервное копирование (backup) и шифрование данных
   Внедрите политику автоматического резервного копирования критически важных данных; храните резервные копии в безопасных местах, изолированных от сети. Используйте шифрование данных и трафика (TLS, шифрование дисков и баз данных), чтобы снизить риск кражи информации.
5. Защита сети: firewall и сегментация
   Устанавливайте современные межсетевые экраны, IDS/IPS-системы для управления внешним и внутренним трафиком. Сегментирование внутренней сети по уровням ответственности или степени риска ограничивает распространение ущерба в случае компрометации.

6. Правовая и политическая база: политики безопасности и механизмы
   Документально закрепите внутри организации политику информационной безопасности, правила конфиденциальности и обработки данных; установите обязательные для сотрудников правила и санкции за их нарушение.
7. Периодический анализ рисков и проверка уязвимостей (pentesting, аудит)
   Проводите внутренние и внешние оценки рисков, автоматизированное и ручное сканирование уязвимостей, а также независимое тестирование на проникновение для выявления и устранения слабых мест.
8. План оперативного реагирования на инциденты (Incident Response)
   Разработайте документ, в котором четко прописано, кто и какие действия выполняет при киберинциденте, где хранятся данные, какие каналы связи используются и порядок восстановления. Проводите регулярные учения (tabletop/real drills).
9. Обучение пользователей и тренинги по противодействию социальной инженерии
   Обучайте сотрудников методам фишинга, смс- и голосового мошенничества (smishing, vishing) и другим методам социальной инженерии; проводите симуляции и совершенствуйте меры защиты на основе полученных результатов.
10. Ролевой доступ и принцип минимальных прав
    Предоставляйте каждому пользователю только те права, которые необходимы для выполнения его задач (least privilege). Не используйте учетные записи администратора для повседневных операций.
11. Логирование, мониторинг и SIEM-системы
    Передавайте логи систем и приложений в централизованную систему, используйте автоматический анализ и корреляцию для выявления аномалий и настройки уведомлений.
12. Безопасность цепочки поставок (supply chain)
    Проверяйте сторонние сервисы и поставщиков; включайте требования по безопасности в контракты и проводите регулярные аудиты.
13. Классификация и защита данных (data classification)
    Классифицируйте данные по степени чувствительности и определяйте для каждого класса отдельные меры хранения и защиты (например: открытые, внутренние, конфиденциальные, строго конфиденциальные).
14. Физическая и экологическая безопасность

Ограничьте физический доступ к серверным, обеспечьте видеонаблюдение, биометрический контроль доступа, контроль за электропитанием и климатом — интегрированная защита в рамках кибербезопасности.

15. Использование искусственного интеллекта и автоматизированных средств обнаружения

    Применяйте AI/ML-инструменты для автоматического выявления аномалий, прогнозирования инцидентов и быстрого реагирования, сочетая их с контролем со стороны человека.

16. Юридическая подготовка и международное сотрудничество

    При совершении киберпреступлений наладьте оперативное взаимодействие с правоохранительными органами, участвуйте в международных конвенциях и механизмах поддержки.

17. Постоянный аудит и обновление перспективной политики

    Технологии и угрозы постоянно изменяются, поэтому ежегодно или по мере необходимости пересматривайте политику безопасности и технические требования.

ВЫВОД

В цифровую эпоху кибербезопасность рассматривается не только как техническая, но и как правовая и социальная проблема. Рост числа киберпреступлений напрямую угрожает национальной безопасности стран. Поэтому защита информационных систем, повышение цифровой грамотности пользователей и разработка эффективных правовых механизмов противодействия киберпреступлениям являются актуальными задачами современности. Только при сочетании сильного законодательства, технических средств защиты и международного сотрудничества возможно формирование устойчивой системы кибербезопасности.

Использованная литература:

1. Указ Президента Республики Узбекистан «Цифровой Узбекистан – 2030».
2. Закон «Об информатизации», 2003 г. (с последними изменениями).
3. Каримов С. (2022). Основы кибербезопасности и методы защиты информационных систем. Ташкент: Изд-во ТАТУ.
4. Нурматова Н. (2023). Цифровая безопасность и борьба с киберпреступлениями. Ташкент: Изд-во «Инновация».
5. National Institute of Standards and Technology (NIST). (2021). Cybersecurity Framework.
6. ISO/IEC 27001:2022 — Information Security Management Systems.