ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ: ОПЫТ РЕСПУБЛИКИ УЗБЕКИСТАН, ГОСУДАРСТВ СНГ, ЕВРОПЕЙСКОГО СОЮЗА И СОЕДИНЁННЫХ ШТАТОВ АМЕРИКИ.

Фарходов Жахонгир Фарходович
Курсант Академии МВД Республики Узбекистан.
А.А. Иминов
Научный руководитель: Начальник кафедры цифровых технологий и информационной безопасности Академии Министерства внутренних дел, кандидат физико-математических наук, подполковник.

https://doi.org/10.5281/zenodo.18458507

Annotatsiya. *Mazkur maqolada kiberxavfsizlikni ta'minlashning huquqiy asoslari qiyosiy-huquqiy tahlil asosida o'rganilgan. Tadqiqot doirasida O'zbekiston Respublikasi, Mustaqil Davlatlar Hamdo'stligi mamlakatlari, Yevropa Ittifoqi va Amerika Qo'shma Shtatlarida kiberxavfsizlik sohasini tartibga soluvchi normativ-huquqiy hujjatlar, milliy strategiyalar va institutsional mexanizmlar tahlil qilinadi. Maqolada axborot xavfsizligi, shaxsiy ma'lumotlarni himoya qilish, kiberjinoyatlarga qarshi kurashish hamda davlat va xususiy sektor o'rtasidagi hamkorlik masalalariga alohida e'tibor qaratilgan. Qiyosiy tahlil natijasida turli huquqiy tizimlarda kiberxavfsizlikni ta'minlashga bo'lgan yondashuvlarning o'xshash va farqli jihatlari aniqlanadi. Tadqiqot xulosalari O'zbekiston Respublikasida kiberxavfsizlik sohasidagi qonunchilikni takomillashtirish va ilg'or xorijiy tajribani milliy huquq tizimiga moslashtirishda ilmiy-amaliy ahamiyatga ega.*

Kalit so'zlar: *kiberxavfsizlik, huquqiy asoslar, qiyosiy tahlil, axborot xavfsizligi, kiberjinoyat, shaxsiy ma'lumotlar.*

Аннотация. *В данной статье рассматриваются правовые основы обеспечения кибербезопасности на основе сравнительно-правового анализа опыта Республики Узбекистан, государств Содружества Независимых Государств, Европейского союза и Соединённых Штатов Америки. В рамках исследования анализируются нормативно-правовые акты, национальные стратегии и институциональные механизмы в сфере защиты информационной безопасности, персональных данных и противодействия киберпреступности. Особое внимание уделяется вопросам взаимодействия государства и частного сектора, а также роли международных стандартов и сотрудничества в обеспечении кибербезопасности. В результате сравнительного анализа выявляются ключевые особенности и различия правовых подходов различных правовых систем, а также формулируются выводы и предложения, направленные на совершенствование законодательства Республики Узбекистан в сфере кибербезопасности.*

Ключевые слова: *кибербезопасность, правовые основы, сравнительный анализ, информационная безопасность, киберпреступность, защита персональных данных.*

Annotation. *This article examines the legal foundations of cybersecurity through a comparative legal analysis of the experience of the Republic of Uzbekistan, the Commonwealth of Independent States (CIS), the European Union, and the United States of America. The study analyzes legal frameworks, national cybersecurity strategies, and institutional mechanisms aimed at protecting information security, personal data, and combating cybercrime. Particular attention is paid to public–private cooperation and the role of international standards and cooperation in ensuring cybersecurity.*

The comparative analysis identifies key similarities and differences in legal approaches across various jurisdictions and provides conclusions and recommendations for improving the cybersecurity legislation of the Republic of Uzbekistan based on advanced international experience.

Keywords: *cybersecurity, legal foundations, comparative analysis, information security, cybercrime, personal data protection.*

Введение

Современное общество вступило в этап глубоких цифровых преобразований, охватывающих практически все сферы государственной и общественной жизни. Развитие информационно-коммуникационных технологий, расширение использования интернета, внедрение электронного правительства, цифровой экономики и автоматизированных систем управления существенно повысили эффективность социально-экономических процессов. Вместе с тем данные тенденции привели к возникновению новых угроз, связанных с нарушением информационной безопасности, ростом киберпреступности и уязвимостью критически важной информационной инфраструктуры.

В этих условиях обеспечение кибербезопасности становится одной из приоритетных задач современного государства и требует комплексного правового регулирования.

Киберпространство обладает рядом специфических особенностей, отличающих его от традиционных сфер общественных отношений. Оно характеризуется трансграничным характером, высокой динамичностью и сложностью идентификации субъектов противоправной деятельности. Кибератаки, утечки данных, несанкционированный доступ к информационным системам и распространение вредоносного программного обеспечения представляют угрозу не только для отдельных пользователей, но и для национальной безопасности государств.

В связи с этим правовые основы обеспечения кибербезопасности должны учитывать как национальные интересы, так и международные обязательства государств. Республика Узбекистан в последние годы активно реализует стратегию цифрового развития, направленную на модернизацию государственного управления, развитие электронных услуг и повышение прозрачности деятельности государственных органов.

Эти процессы объективно требуют создания эффективной системы правового обеспечения кибербезопасности, способной защитить информационные ресурсы, персональные данные граждан и устойчивость цифровой инфраструктуры.

В данном контексте особую актуальность приобретает изучение зарубежного опыта правового регулирования кибербезопасности, в частности практики государств СНГ, Европейского союза и Соединённых Штатов Америки. Сравнительно-правовой анализ позволяет выявить общие тенденции и особенности правового регулирования кибербезопасности в различных правовых системах, определить наиболее эффективные модели и инструменты противодействия киберугрозам.

Выбор указанных юрисдикций обусловлен их различным уровнем правового развития, институциональной организации и подходами к обеспечению информационной безопасности. Целью настоящей работы является комплексное исследование правовых основ обеспечения кибербезопасности с учетом опыта Республики Узбекистан, государств

СНГ, Европейского союза и США, а также формулирование научно обоснованных выводов и предложений по совершенствованию национального законодательства.

Основная Часть

Правовые основы обеспечения кибербезопасности в Республике Узбекистан формируются в рамках общей политики государства в сфере информационной безопасности и цифрового развития. Национальное законодательство направлено на защиту информационных ресурсов, обеспечение безопасности информационных систем и противодействие киберпреступности. Важное место в данной системе занимают нормы, регулирующие вопросы защиты персональных данных, электронного документооборота, функционирования государственных информационных систем и ответственности за преступления в сфере информационных технологий.

Особенностью узбекского подхода является постепенное формирование комплексной системы кибербезопасности, основанной на централизованной координации деятельности государственных органов. Создание специализированных подразделений, разработка национальных программ и стратегий, а также повышение требований к защите критической информационной инфраструктуры свидетельствуют о стремлении государства обеспечить устойчивость цифровой среды. Вместе с тем правовое регулирование продолжает развиваться и требует дальнейшей детализации, особенно в части разграничения полномочий, регулирования взаимодействия с частным сектором и внедрения механизмов оперативного реагирования на киберинциденты.

В государствах Содружества Независимых Государств правовое регулирование кибербезопасности имеет схожие черты, обусловленные общим историко-правовым наследием и сходством правовых систем. Для большинства стран СНГ характерен акцент на государственный контроль в сфере информационной безопасности и защиту национального сегмента интернета. Законодательство ориентировано на обеспечение суверенитета информационного пространства и предотвращение угроз национальной безопасности. Однако уровень развития правовых механизмов кибербезопасности в странах СНГ остается неоднородным. В одних государствах приняты комплексные стратегии и специализированные законы, в других – правовое регулирование носит фрагментарный характер. Отсутствие унифицированного подхода затрудняет международное сотрудничество и координацию действий в борьбе с трансграничной киберпреступностью.

В то же время накопленный опыт стран СНГ представляет практический интерес для Республики Узбекистан в части институциональной организации и правоприменительной практики. Европейский союз демонстрирует одну из наиболее развитых и системных моделей правового обеспечения кибербезопасности. Особенностью европейского подхода является наднациональный характер регулирования и гармонизация законодательства государств-членов. Кибербезопасность рассматривается как неотъемлемый элемент цифрового рынка и защиты фундаментальных прав человека.

Существенное внимание уделяется вопросам конфиденциальности и защиты персональных данных, что отражается в строгих требованиях к обработке информации.

В рамках ЕС сформирована разветвленная система институтов и механизмов координации, направленных на предотвращение и минимизацию последствий киберугроз.

Взаимодействие государственных органов, частного сектора и научного сообщества способствует повышению устойчивости информационных систем.

Европейский опыт представляет особую ценность с точки зрения баланса между обеспечением безопасности и соблюдением прав и свобод граждан, что является актуальным и для Республики Узбекистан. Соединённые Штаты Америки обладают одной из наиболее развитых и технологически продвинутых систем обеспечения кибербезопасности. Американская модель правового регулирования отличается децентрализованным характером и сочетанием федеральных, региональных и отраслевых норм. Существенную роль в обеспечении кибербезопасности играет частный сектор, который является ключевым владельцем и оператором критической инфраструктуры.

Правовое регулирование в США ориентировано на защиту национальных интересов и критически важных систем, а также на стимулирование инноваций в сфере киберзащиты. Высокий уровень взаимодействия между государством и бизнесом позволяет оперативно реагировать на новые угрозы и внедрять современные технологические решения. В то же время фрагментарность правового регулирования может создавать определенные сложности в обеспечении единых стандартов безопасности. Сравнительный анализ правовых основ обеспечения кибербезопасности показывает, что несмотря на различия в подходах, все рассматриваемые юрисдикции признают необходимость комплексного и многоуровневого регулирования данной сферы.

Для Республики Узбекистан особый интерес представляет европейский опыт защиты персональных данных и американская практика государственно-частного партнерства, а также координационные механизмы, применяемые в странах СНГ.

Заключение

Проведенное исследование свидетельствует о том, что правовые основы обеспечения кибербезопасности являются важнейшим элементом национальной безопасности и устойчивого развития государства. В условиях глобальной цифровизации и трансграничного характера киберугроз ни одна страна не может эффективно противостоять данным вызовам в изоляции. Именно поэтому развитие национального законодательства должно осуществляться с учетом международных стандартов и передового зарубежного опыта. Республика Узбекистан последовательно формирует правовую и институциональную базу обеспечения кибербезопасности, однако дальнейшее совершенствование законодательства остается актуальной задачей. Необходимо усилить системность правового регулирования, обеспечить четкое разграничение полномочий государственных органов и развивать механизмы взаимодействия с частным сектором.

Важным направлением является повышение правовой культуры и осведомленности населения в сфере информационной безопасности. Опыт государств СНГ, Европейского союза и Соединённых Штатов Америки показывает, что эффективная система кибербезопасности должна быть гибкой, адаптивной и основанной на сотрудничестве всех заинтересованных сторон. Внедрение лучших зарубежных практик с учетом национальных особенностей позволит Республике Узбекистан укрепить правовые основы обеспечения кибербезопасности и повысить устойчивость цифровой среды к современным угрозам.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Ахметов, Б.Р. *Профилактика преступлений среди женщин: теория и практика*. – Ташкент: Юридический университет, 2020.

2. Иванова, Е.В. *Социальная реабилитация ранее осуждённых женщин*. – Москва: Юрайт, 2019.
3. Петров, А.Н. *Психологические аспекты работы инспекторов профилактики*. – Санкт-Петербург: Питер, 2021.
4. Karimov, M. *Женская преступность и меры профилактики*. – Tashkent: Fan, 2018.