LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 2(2025) / ISSN 3030-3052 Available at www.uznauka.uz

ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ КИБЕРБЕЗОПАСНОСТИ ПОСТРОЕНИЯ ИНФРАСТРУКТУРЫ

Саидов Баходирходжа Насирходжаевич
Ведущий специалист Центра кибербезопасности Главного управления устрашения Национальной гвардии Республики Узбекистан
bahodirkhujasaidov@gmail.com

Аннотация: *В этой статье рассматриваются теоретические предпосылки кибербезопасности с точки зрения гражданского права. Киберугрозы становятся все более распространенными для инфраструктурных систем в результате быстрого развития цифровых технологий, что требует комплексной правовой базы для устранения этих опасностей. В статье рассматривается значение регулирующих органов и сотрудничества между государственным и частным сектором для повышения кибербезопасности. Результаты показывают, что разработка надежных правовых стратегий для защиты инфраструктурных учреждений от кибератак и обеспечения соблюдения гражданского права требует комплексного подхода.*

Ключевые слова: *кибербезопасность, гражданское право, защита инфраструктуры, правовая база, защита данных, управление рисками.*

PRACTICAL ASPECTS OF BUILDING INFRASTRUCTURE CYBER SECURITY IMPLEMENTATION

Saidov Bakhodirkhoja Nasirkhojaevich
The leading specialist of the Cyber Security Center of the Main Department of Intimidation of the National Guard of the Republic of Uzbekistan
bahodirkhujasaidov@gmail.com

Abstract: *the theoretical underpinnings of cyber security are examined in this essay within the framework of civil law. Infrastructure systems are becoming more susceptible to cyberattacks due to the quick growth of digital*

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 2(2025) / ISSN 3030-3052 Available at www.uznauka.uz

technology, necessitating a thorough regulatory framework to mitigate these risks. The function of regulatory agencies and the value of public-private sector collaboration in bolstering cyber security measures are covered in the essay. The results emphasize the necessity of a thorough strategy to creating strong legal defenses that shield infrastructure organizations from online attacks and guarantee adherence to civil law norms.

Keywords: *cyber security, civil law, infrastructure protection, legal framework, data protection, risk management.*

ВВЕДЕНИЕ

Киберпреступность и преступления в реальной жизни похожи. С другой стороны, он только создается в виртуальном пространстве. Тем не менее, мы знаем, как это влияет на реальную жизнь. Цифровизация в Узбекистане принесла свои плоды: многие предприятия активно работают над переводом информации в цифровой формат. Люди значительно облегчены, потому что им больше не нужно стоять в очереди в ЦОН и ходить в банк, чтобы сделать денежный перевод. Однако с упрощением появляется новая опасность со стороны киберпреступников. Киберугроза — это угроза. Законодательство по вопросу «Кибербезопасности» недостаточно даже в Узбекистане. потому что эта идея и подобные преступления в последнее время стали более распространенными. Олий Мажлис принял Закон Республики Узбекистан «О кибербезопасности», чтобы регулировать отношения в сфере кибербезопасности, предотвращать киберпреступления и защищать страну от кибератак. В эпоху быстрых технологических достижений и растущей зависимости от цифровой инфраструктуры кибербезопасность вышла за рамки простой технической проблемы и теперь

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 2(2025) / ISSN 3030-3052 Available at www.uznauka.uz

является юридической проблемой. По мере интеграции интеллектуальных технологий в инфраструктуру, такую как транспортные системы, электросети и сети связи, уязвимость перед киберугрозами растет. Эта изменчивость подчеркивает чрезвычайное значение всеобъемлющих правовых рамок для решения сложностей кибербезопасности в рамках гражданского права. Целью этой статьи является изучение теоретических основ кибербезопасности для инфраструктурных учреждений. Кроме того, он рассматривает, как существующие нормы гражданского права могут быть изменены для защиты от киберугроз. [1]

ОСНОВНАЯ ЧАСТЬ

Киберугроза включает в себя любую противоправную деятельность, от взлома личных страниц в социальных сетях до кражи больших данных. С помощью специальных вирусных программ киберпреступники могут взломать любое устройство, например мобильный телефон или компьютер. Преступникам не составит труда получить ваши данные, если пользователь установит нелицензионную программу или скачает файлы с вредоносными вирусами с подозрительных сайтов. Такие атаки могут затронуть как личные аккаунты, так и личные бренды. На это в основном влияют общественные деятели. Крупные предприятия часто подвергаются атакам киберпреступников. Они крадут данные, такие как базы данных клиентов, а затем используют их в своих целях. Другие кибермошенники могут вымогать деньги у неопытных людей, переводить деньги без разрешения владельца карты, а иногда даже совершать онлайн-покупки.

[1] Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 2(2025) / ISSN 3030-3052 Available at www.uznauka.uz

В современную цифровую эпоху кибербезопасность стала краеугольным камнем национальной безопасности, экономической стабильности и общественной безопасности. В условиях быстрой оцифровки общественной инфраструктуры и важнейших систем правовые рамки, регулирующие эти области, должны адаптироваться к меняющемуся ландшафту киберугроз. Гражданское право играет решающую роль в определении ответственности и обязательств организаций, осуществляющих управление инфраструктурой. Кибербезопасность — это методы, технологии и процессы, предназначенные для защиты систем, сетей и данных от киберугроз, таких как взлом, вирусы и утечка данных. Его важность невозможно переоценить, особенно с учетом того, что критически важные инфраструктурные сети, если они будут нарушены, могут иметь разрушительные последствия для общественного здравоохранения, безопасности и экономической стабильности. Эти отрасли включают коммунальные услуги, транспорт, связь и системы реагирования на чрезвычайные ситуации. Взаимосвязь между этими секторами усугубляет потенциальные риски и требует создания надежной системы кибербезопасности.[2]

Когда мы говорим о проблеме безопасности, мы прежде всего представляем себе понятие «война». Возникает паника, когда некоторые напуганные солдаты врываются с автоматами. На самом деле может показаться, что мирная эра родилась без таких войн. Никто не вешает пять пистолетов, не ревёт танками, не бомбит самолётами, не нарушает нашу границу, не мешает. Но это не значит, что мы полностью свободны от врагов.

[2] Amoroso, E. G., & Amoroso, E. (2012). Cyber attacks: protecting national infrastructure. Elsevier.

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 2(2025) / ISSN 3030-3052 Available at www.uznauka.uz

Сегодня мы живем мирно, но невооруженная война продолжается. Нынешняя война отличается от предыдущей войны. Современный мир живет в эпоху информационной войны. Основная особенность компьютерной, информационной и сетевой «войны» нового века заключается в том, что она не разделена на тыл и фронт, не имеет границ. Поэтому, хотя денег тратится меньше, чем в обычных войнах, риски и последствия очень высоки. Причина в том, что в этой войне человеческий ребенок часто становится застреленным, замученным, раненым, и даже если он не становится инвалидом, он становится более опасным, чем раньше. Излечить раны тела можно, но надо с самого начала понимать, что лечение ран психически и психически слабых обходится обществу очень дорого. Современные информационные технологии имеют множество преимуществ и преимуществ. Во-первых, скорость; во-вторых, эффективность и экономичность; в-третьих, возможность предоставления услуг на большом расстоянии; в-четвертых, целостность распространения и приема информации; в-пятых, широкий спектр возможностей для использования и потребления информации. Несмотря на эти преимущества, различные государственные услуги, реализуемые с помощью информационных технологий, также представляют собой серьезные риски. В результате необходимо обеспечить защиту от различных информационных угроз и проблем, чтобы поддерживать ритмичность полезной деятельности в обществе, уменьшать потенциальные потери и ущерб, повышать эффективность инвестиций и расширять возможности бизнеса. В общем, информационные угрозы неизбежны в наше сложное время. Кража и удаление данных с генерирующих устройств, решающих основные проблемы

страны, даже считается чрезвычайной ситуацией. Потому что такая ситуация серьезно наносит ущерб интересам государства, национальной безопасности, независимости и автономии. Поэтому информация является основным капиталом, координирующим нормальность работы, а также ценным имуществом и оборудованием конкретной организации, поэтому ее следует защищать. Раньше мы записывали информацию на бумаге, сохраняли ее и делились ею с другими. Сегодня широкое использование компьютеров и Интернета позволило хранить и распространять их как электронный онлайн-ресурс. Сегодняшняя информационная система очень сложна и синтетическа, поэтому иногда создает угрозы, отличные от человеческого фактора. Поскольку Интернет является средством связи и коммуникации современных стран мира, миллионы больших и малых систем взаимно зарегистрированы и подключены к нему. В результате экономится много времени и денег, но это также позволяет преступникам получать доход преступным путем. Кроме того, в Интернете широко распространено вредоносное ПО, вызывающее хаос. Поскольку в Интернете нет национальных границ и ограничений, проблема информационной безопасности – это не только проблема группы, региона, континента или отдельной страны. Действительно, это стало глобальной проблемой. Что же касается последствий компьютерной и информационно-сетевой войны, то это не что иное, как стихийное бедствие. Ее можно даже сравнить с угрозой атомного, ядерного оружия массового поражения. Мы знаем, что информация так же важна для военного командования, как и воздух. Ни одна великая команда с пятью пушками не сможет облажаться, если нет данных. Если это так, то вопросы безопасности компьютерных, информационных и сетевых систем займут большое место в

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 2(2025) / ISSN 3030-3052 Available at www.uznauka.uz

сфере обороны. В новом веке наука и техника вместе достигли высших точек развития. Возможность и скорость связи, обмена информацией возросли до максимума, а невидимая гигантская вселенная максимально «минимизировалась» на ладони. В результате максимально укрепились межгосударственные и межэтнические отношения.[3]

В начале 2020 года объем всех данных в Интернете достиг 44 зеттабайт. По оценкам, к 2025 году объем данных, производимых каждый день, достигнет 463 эксабайт. Однако эксперты обеспокоены давлением на СМИ. Потому что продюсера редакции «Radio Television Hong Kong» обвинили в нарушении правил дорожного движения при подготовке репортажа о восстании 2019 года. Кроме того, международная организация, выступающая за свободу прессы, «Репортеры без границ» сообщила, что Гонконг занимает 80-е место из 180 стран по уровню свободы СМИ, а значит, результат неудовлетворительный. В условиях процесса становления информационного общества в нашей стране информационно-коммуникационные технологии становятся основным ядром любой сферы общественной жизни. Информационные и коммуникационные технологии, как кровеносные сосуды политической системы, питают ее компоненты и элементы, обеспечивают их взаимодействие и движение. Иными словами, правильное функционирование политической системы и ее компонентов напрямую зависит от беспристрастности, корректности и своевременности предоставления информации. Поэтому независимо от форм государственного управления в любой стране роль информации как формообразующего, координирующего, коммуникативного фактора во всех компонентах ее

[3] Alpcan, T., & Başar, T. (2010). Network security: A decision and game-theoretic approach. Cambridge University Press.

политической системы (политических институтах, политических отношениях, политических нормах и принципах, политическом сознании и политической культуре) особенна и будет продолжать развиваться. Потому что с развитием информационных технологий, новых методов распространения информации, в том числе с развитием сети Интернет, которая сегодня в Узбекистане официально приравнена к средствам массовой информации, возродится коммуникативная деятельность политической системы. К данным нововведениям также проявили интерес государственные органы и органы управления, в результате чего родились такие новые проекты, как «электронное правительство», «электронное управление», «электронная партия», «электронный университет», институт информационно-коммуникационной политики. В то же время процесс производства и распространения информации, бурное развитие компьютерных технологий оказывают существенное влияние на структуру и механизмы государственного управления. Сегодняшний информационный поток стал постоянной силой, роль и место информации в обществе особенно возрастают в условиях формирования мирового информационного пространства. Это, в свою очередь, служит усложнению вопросов обеспечения информационной безопасности государства, общества и личности.

Законы о защите данных стали важной частью гражданского права по мере роста обеспокоенности по поводу утечки данных и нарушений конфиденциальности. Эти законы определяют, как организации собирают, хранят и обрабатывают личную и конфиденциальную информацию. Эти законы имеют огромное значение для кибербезопасности, поскольку

большинство киберугроз направлены на данные. Общий регламент по защите данных (GDPR) ЕС является основным законом о защите данных, связанным с кибербезопасностью. Согласно GDPR, организации обязаны принять соответствующие организационные и технические меры для защиты персональных данных. В связи с тем, что несоблюдение требований может привести к значительным штрафам, организациям очень важно вкладывать средства в надежные методы кибербезопасности.[4]

Хотя теоретические основы кибербезопасности прочно укоренились в гражданском праве, существуют проблемы с применением этих законов. Одной из важных проблем являются быстрые темпы технологических изменений. Киберугрозы развиваются с угрожающей скоростью, часто опережая возможности законодателей адаптировать существующие законы или принять новые правила. Это неравенство создает пробелы в правовой защите и делает организации уязвимыми для кибератак. Кроме того, юрисдикционные вопросы усложняют соблюдение законов о кибербезопасности. Кибератаки могут исходить из любой точки мира, что затрудняет определение применимых законов юрисдикции. Эта сложность затрудняет понимание организациями своих юридических обязательств и управление потенциальными обязательствами.

ЗАКЛЮЧЕНИЕ

Сегодня особое внимание уделяется реализации Закона Республики Узбекистан «О кибербезопасности». Киберщит — комплекс мероприятий, аппаратно-программных комплексов и проектов, реализуемых государственными органами в сфере информационной безопасности. В

[4] Brands, S. (2000). Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press.

рамках этой программы определены меры, направленные на безопасное использование информационных и коммуникационных технологий. Растущая частота и изощренность киберугроз против инфраструктурных учреждений подчеркивает необходимость создания надежной системы гражданского права, охватывающей кибербезопасность. В этой статье излагаются теоретические основы кибербезопасности в контексте гражданского права, выделяя такие ключевые принципы, как ответственность, управление рисками и защита данных. Поскольку инфраструктурные системы продолжают развиваться, правовые подходы, которые ими управляют, также должны гарантировать, что они эффективны в смягчении возникающих рисков. Кроме того, важно развивать сотрудничество между государственными органами, организациями частного сектора и практикующими юристами для разработки комплексных стратегий, усиливающих меры кибербезопасности.

ИСПОЛЬЗОВАННЫЕ ССЫЛКИ

1. Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.
2. Amoroso, E. G., & Amoroso, E. (2012). Cyber attacks: protecting national infrastructure. Elsevier.
3. Alpcan, T., & Başar, T. (2010). Network security: A decision and game-theoretic approach. Cambridge University Press.
4. Brands, S. (2000). Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press.