ПРОФИЛАКТИКА КИБЕРПРЕСТУПНОСТИ: НЫНЕШНЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

на основе изучения национального и зарубежного законодательства

Рахманов Дмитрий Каландарович
Главный научный сотрудник Института парламентских исследований при Законодательной палате Олий Мажлиса Республики Узбекистан

Аннотация. *В статье рассматриваются актуальные вопросы обеспечения кибербезопасности в Республике Узбекистан и в ряде стран мира. Анализируется законодательная база Узбекистана в сфере кибербезопасности, проводится сравнительный анализ законодательной базы зарубежных стран, рассматриваются основные направления профилактики киберпреступности и предлагаются меры по совершенствованию системы обеспечения кибербезопасности в Узбекистане.*
Ключевые слова: *кибербезопасность, информационная безопасность, киберпрес-тупность, законодательство, Узбекистан, международный опыт, профилактика, критическая информационная инфраструктура.*

Abstract. *The article examines current issues of cybersecurity in the Republic of Uzbekistan and worldwide. It analyzes the legislative framework of Uzbekistan in the field of cybersecurity, including recently adopted legal acts. A comparative analysis of cybersecurity legislation in several foreign countries is conducted. The main directions of cybercrime prevention are considered, and measures to improve the cybersecurity system in Uzbekistan are proposed.*
Keywords: *cybersecurity, information security, cybercrime, legislation, Uzbekistan, international experience, prevention, critical information infrastructure.*

Противодействие использованию информационных сетей в целях совершения противоправных деяний, а также защита важнейших для государства и общества информационных инфраструктур от кибератак имеют ключевое значение для внешней и внутренней безопасности нашей страны. Использование электронного информационного пространства и средств интернет-коммуникаций преступными группами, специализирующимися на вымогательстве, мошенничестве, кражах, совершении преступлений в сфере компьютерной информации, актуализирует необходимость принятия решительных мер противодействия, как в масштабах отдельных государств, так и в рамках межгосударственного сотрудничества.

Решение этой задачи предполагает совместную работу правоохранительных и иных государственных органов, выстраивание оптимальной стратегии сотрудничества и обмена информацией на национальном и межгосударственном уровне, а также разработку и реализацию комплекса нормативно-правовых и организационных мер по противодействию деятельности организованных преступных формирований и сообществ.

Необходимость совершенствования нормативно-правовой базы по вопросам обеспечения кибербезопасности в Республике Узбекистан связана с возрастающими в настоящее время вызовами, рисками и угрозами в киберпространстве, резким ростом киберпреступности, увеличением кибератак в сети, непредсказуемой динамикой развития киберпространства в мире.

Как известно, кибербезопасность – это один из разделов информационной безопасности, который изучает состояние защищенности интересов личности, общества и государства от внутренних и внешних угроз в киберпространстве. Однако сам термин «кибербезопасность» и его производные (киберпространство, кибербезопасность, кибератаки и т.д.) не имеют международно признанного юридического определения.

В связи с развитием современных технологий увеличилось и количество

киберпреступлений. Так, согласно статистической информации на территории Узбекистана[1] количество преступлений в сфере информационных технологий, совершенных в 2020 году составило 106, в 2021 году – 2.281, а в 2022 году увеличилось в 2 раза и составило 4.332 факта. Из них 2.747 преступлений составили киберкражи, 625 – кибермошенничество, 874 – преступления, связанные с наркотиками, совершенные с помощью информационных технологий.

Мировая статистика киберпреступлений выглядит следующим образом:

Ущерб от киберпреступлений: 6,6 триллиона долларов США.

Прогноз на 2025 год: 10,5 триллиона долларов США.

Количество опасных кибератак:

- Ежедневно: 2 328 атак
- Еженедельно: 16 384 атаки
- Ежемесячно: 70 000 атак
- Ежегодно: 840 000 атак

- Распределение кибератак по сферам:
  - Финансы: 33%
  - Здравоохранение: 24%
  - Государственный сектор: 22%
  - Розничная торговля: 17%
  - Энергетика: 4%[2]

В настоящее время Республика Узбекистан активно развивает и внедряет цифровые технологии, как в государственном, так и в частном секторе. Помимо преимуществ и новых возможностей для всех сфер человеческой деятельности, существует ряд потенциальных рисков для устойчивого функционирования информационных систем и ресурсов государственного сектора, и соответственно для обеспечения прав, свобод и законных интересов личности, которые могут представлять реальную угрозу общественным интересам, здоровью и благополучию общества и граждан.

В этой связи в 2022 году был разработан и принят Закон «О кибербезопасности». Закон направлен на минимизацию административных и временных затрат в случае возникновения новых фундаментальных угроз в цифровой среде, в нем четко определены:

основные принципы обеспечения кибербезопасности;

полномочия, права и обязанности уполномоченного государственного органа в сфере обеспечения кибербезопасности;

требования к обеспечению кибербезопасности информационных систем и ресурсов государственных органов и организаций;

меры реагирования на инциденты кибербезопасности и другие вопросы.

В законе определены понятия: кибербезопасность, киберугроза, киберзащита, кибератака, критическая информационная инфраструктура и другие. Меры по обеспечению кибербезопасности, включают в себя следующее:

- Защита информационных систем, сетей и данных;
- Предотвращение киберпреступлений и кибератак;
- Расследование инцидентов кибербезопасности;
- Восстановление информационных систем, сетей и данных в случае кибератаки;
- Повышение осведомленности о кибербезопасности.

Законом определены полномочия государственных органов в сфере кибербезопасности:

- Разработка и реализация государственной политики в сфере кибербезопасности;
- Координация деятельности субъектов кибербезопасности;
- Контроль и надзор за обеспечением кибербезопасности;
- Международное сотрудничество в сфере кибербезопасности.

Закон “О кибербезопасности” является важным шагом на пути к обеспечению кибербезопасности в Узбекистане.

31мая 2023 года Президентом подписано Постановление №ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан». Постановлением утверждено Положение о

[1] *Брифинг, посвященный теме: «Виды преступлений и способы защиты в сфере информационных технологий» //https://iibb.uz/ru/news/v-glavnom-upravlenii-vnutrennih-del-stolitsy-sostojalsja-brifing-*

[2] *Отчет о киберугрозах за 2023 год https://www.statista.com/study/134738/cyber-threat-report-2023/*

порядке обеспечения кибербезопасности важнейших объектов информационной инфраструктуры Республики Узбекистан, которое определяет порядок обеспечения кибербезопасности важных объектов информационной инфраструктуры Республики Узбекистан. Кроме того, Постановлением утверждены Общие требования по обеспечению кибербезопасности важнейших объектов информационной инфраструктуры Республики Узбекистан:

Справочно: критическая информационная инфраструктура – комплекс автоматизированных систем управления, информационных систем и ресурсов сетей и технологических процессов, имеющих важное стратегическое и социально-экономическое значение.

Положение о порядке обеспечения кибербезопасности объектов критической информационной инфраструктуры (КИИ) определяет основные задачи системы кибербезопасности:

· предотвращение неправомерного использования, удаления, изменения, блокирования (ограничения), копирования, предоставления и распространения информации, обрабатываемой на объектах КИИ, а также иных неправомерных действий;

· недопущение воздействия на аппаратные, программные и программно-аппаратные средства обработки информации, способного вызвать нарушение и (или) остановку работы объектов КИИ;

· восстановление работы объектов КИИ путем резервирования телекоммуникационных сетей, информационных ресурсов и системы жизнедеятельности.

В постановлении также приведены общие требования кибербезопасности объектов КИИ.

Изучение зарубежного опыта.

Закон «О кибербезопасности» был разработан и принят на основе изучения и анализа состояния правового регулирования информационной и кибербезопасности в зарубежных странах (Грузии, Казахстана, Украины, Российской Федерации, Китая, Сингапура, США и других государств).

Основным нормативным правовым документом Грузии в сфере обеспечения информационной безопасности является Закон «Об информационной безопасности». Этот закон устанавливает права и обязанности государственного и частного секторов в области информационной безопасности, а также определяет механизмы государственного контроля за реализацией поли-тики информационной безопасности.

Закон “Об информационной безопасности” способствовал созданию Бюро кибербезопасности при Министерстве обороны, отвечающего за обеспечение кибербезопасности военных объектов и организаций страны, а также Агентства по обмену информацией при Министерстве юстиции, которое занимается вопросами информационной и кибербезопасности в государственном секторе, поддерживает и контролирует исполнение Закона “Об информационной безопасности”, а также составляет список важных информационных систем, разрабатывая минимальные требования и стандарты для их защиты от кибератак.

Агентство по обмену информацией, также отвечает за управление группой реагирования на компьютерные инциденты (CERT), в состав которой входят ИТ-специалисты, занимающиеся технической поддержкой по предотвращению кибератак и борьбе с ними. Кроме того, при Министерстве внутренних дел создан Отдел киберпреступлений (Cyber Crime Dimension) Центрального управления криминиальной полиции в целях расследования киберпреступлений. В случаях, когда киберпреступность направлена против государства, Отдел киберпреступлений делегирует следственные задачи Совету государственной безопасности. В настоящее время правовая и институциональная база Грузии обеспечивает прочную основу для реализации политики эффективной кибербезопасности.

Основным документом в области информационной безопасности в Республике Казахстан является Закон Республики Казахстан «Об информатизации». Согласно принятому закону, защита информационных объектов – это реализация комплекса правовых, организационных и технических мер, направленных на обеспечение безопасности информационных объектов, предотвращение неправомерного, несанкционированного доступа к ним.

В соответствии с Законом «Об информатизации» уполномоченным органом в области информационной безопасности является Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Закон также определяет полномочия регулятора по информационной безопасности, Оперативного центра информационной безопасности, Службы реагирования на инциденты информационной безопасности, Национального центра координации информационной безопасности, Центра систем информационной безопасности, Государственной технической службы и Национального института по информационной безопасности. В Уголовный кодекс Республики Казахстан включен перечень противоправных действий в области связи и информатизации.

В результате принятия данного закона утверждена Концепция кибербезопасности («Киберщит Казахстана»), определяющая основные направления государственной политики в области защиты электронных информационных ресурсов и систем, а также телекоммуникационных сетей, обеспечивающие безопасное использование информационных и коммуникационных технологий.

В Украине 9 мая 2017 года был принят Закон «Об основных принципах обеспечения кибербезопасности Украины», который определяет правовые и организационные основы обеспечения защиты национальных интересов Украины в киберпространстве, основные цели, направления и принципы государственной политики в сфере кибербезопасности, полномочия государственных органов, предприятий, учреждений, организаций и граждан в этой сфере, основные принципы координации их деятельности по обеспечению кибербезопасности.

Деятельность в сфере кибербезопасности координирует президент Украины, через возглавляемый им Совет национальной безопасности и обороны (СНБО) страны. Рабочим органом СНБО является Национальный координационный центр кибербезопасности, который осуществляет координацию и контроль за деятельностью субъектов сектора безопасности и обороны.

В данном законе отражены вопросы киберзащиты коммуникационных систем всех форм собственности, в которых обрабатываются национальные информационные ресурсы, а также используемых в интересах органов государственной власти и местного самоуправления, правоохранительных органов и воинских формирований, в сферах электронного управления, электронных государственных услуг, электронной коммерции, электронного документооборота, включая объекты критической информационной инфраструктуры.

Вместе с этим, согласно вышеуказанному закону, органы государственного управления получили новые функции. В частности, Нацбанк определяет порядок, требования и меры по обеспечению киберзащиты и информационной безопасности в банковской системе, а также для субъектов перевода денежных средств.

Кроме того, ранее утверждённая Указом Президента Украины Стратегия национальной безопасности, от 28 мая 2015 года детализирует основные направления государственной политики национальной безопасности в вопросах информационной безопасности.

Базовым документом по информационной безопасности в Российской Федерации является утвержденная президентом страны Доктрина информационной безопасности Российской Федерации, которая представляет собой свод официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности в Российской Федерации. Под доктриной понимается информационная безопасность Российской Федерации, защита национальных интересов России в области информации, определяемая сбалансированным комплексом интересов личности, общества и государства.

Так, правовой режим информации в России определяется Федеральным законом «Об информации, информационных технологиях и защите информации». Закон предусматривает разделение информации на общедоступную информацию в зависимости от категории доступа к ней, а также информацию, ограниченную федеральным законом (информация с ограниченным доступом).

В соответствии с настоящим Законом под защитой информации понимается

принятие правовых, организационных и технических мер, направленных на:

- защиту информации от уничтожения, изменения, блокировки, копирования, представления, распространения, несанкционированного доступа и других подобных противоправных действий;

- соблюдение конфиденциальности информации с ограниченным доступом;

- регламентацию условий использования права на информацию.

Государственное регулирование отношений в области информационной безопасности осуществляется посредством установления требований по защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

В соответствии с законодательством Российской Федерации владельцы информации и операторы информационных систем обязаны обеспечить:

-предотвращение несанкционированного доступа к информации и (или) ее передачу лицам, не имеющим права на получение информации;

- своевременное выявление случаев несанкционированного доступа к информации;

- предотвращение возможности негативных последствий нарушения порядка доступа к информации;

- предотвращение воздействий на работу технических средств обработки информации;

- возможность немедленно восстановить данные, которые были изменены или удалены из-за несанкционированного доступа;

- постоянный мониторинг уровня информационной безопасности. И, соответственно, несут ответственность в случае неисполнения своих обязанностей.

Компетентным органом в области технической защиты информации (кроме криптографической защиты) является Федеральная служба по техническому и экспортному контролю России (ФСТЭК). Его задача – обеспечение информационной безопасности в ключевых системах инфор-мационной инфраструктуры (без исполь-зования криптографических методов) и противодействие иностранным службам технической разведки на территории Российской Федерации.

Закон Китайской Народной Республики «О кибербезопасности был принят 7 ноября 2016 года (вступил в силу в 2017 году). Закон КНР о кибербезопасности уделяет особое внимание сбору, хранению и использованию личных данных и информации граждан Китая, связанных с национальной безопасностью.

Применение настоящего Закона распространяется на всех операторов и предприятия, имеющие важные объекты информатизации, а также на любые системы, состоящие из компьютеров и соответствующего оборудования, которые фактически занимаются сбором, хранением, передачей и обработкой информации. Регламент также требует тестирования и сертификации оборудования операторами сетей и запрещает экспорт экономической, технологической или научной информации, которая угрожает национальной безопасности или общественным интересам.

В данном законе особое внимание уделяется защите общественных служб связи и информации, энергетики, транспорта, ирригации, финансов, обороны, электронного правительства и другим важным секторам, а также безопасности важной информационной инфраструктуры, которая может представлять серьезную угрозу национальной безопасности и общественным интересам.

В частности, были усилены требования к профессиональной подготовке персонала, работающего на важных объектах информационной инфраструктуры, и запрещено хранение данных за пределами Китая. Согласно закону, закупка сетевых продуктов и услуг для важных объектов информационной инфраструктуры должна осуществляться под контролем компетентных государственных органов. Кроме того, в соответствии с законом, на критически важных объектах КНР предусмотрена необходимость проведения ежегодной оценки рисков безопасности и предоставление отчетов о результатах этой деятельности.

В случае обнаружения нарушений, по закону налагается штраф от 10 000 до 1 млн юаней (от 1400$ до 140925$) - в зависимости

от степени тяжести киберпреступления, а все незаконные доходы конфискуются. Согласно статье 75 указанного закона, должностные лица КНР имеют право замораживать активы иностранных учреждений, организаций и частных лиц, если они подозреваются в организации и проведении атак, вторжений и вмешательства в критически важную информационную инфраструктуру Китая.

Закон также предусматривает реализацию мер по повышению грамотности населения в области кибербезопасности с участием государственных органов и СМИ всех уровней.

Следует отметить, что иностранные специалисты, критикующие чрезмерную строгость некоторых требований законодательства КНР в области кибербезопасности (в частности, запрет на сокрытие пользователей Интернета), отмечают, что китайская модель кибербезопасности разработана детально. Так, с 1 июня 2020 г. вступили в силу «Меры кибербезопасности», разработанные Управлением по кибербезопасности Китая в сотрудничестве с 11 специализированными агентствами. Меры определяют обязательство по обеспечению кибербезопасности китайских и зарубежных сетевых продуктов, которые предоставляют услуги для стратегических секторов, таких как связь, радио и телевидение, энергетика, финансы, транспорт, железные дороги и гражданская авиация в соответствии с законом о кибербезопасности.

Согласно новым правилам, операторы информационной инфраструктуры, приобретающие сетевые продукты и услуги, должны пройти проверку на кибербезопасность. Документ также понуждает операторов оценивать потенциальные киберугрозы, связанные с закупаемыми продуктами и услугами. При выявлении потенциальных угроз, таких как незаконный контроль и повреждение базовой информационной инфраструктуры, утечка, потеря и фальсификация ключевых данных, операторы должны связаться с компетентными органами для дальнейшего расследования.

Сингапур активно разрабатывает методы защиты данных от кибербезопасности и киберпреступности. Как говорится в Отчете о стратегии кибербезопасности Сингапура: «Правительство рассматривает свои усилия в этих областях как часть своего плана по защите страны от киберугроз и укреплению репутации Сингапура как ведущего центра информационных систем». В Азиатско-Тихоокеанском регионе Сингапур – безусловный лидер в области кибербезопасности.

Национальный правовой механизм кибербезопасности Сингапура имеет самую долгую историю по сравнению с другими государствами-членами АСЕАН (Ассоциация государств Юго-Восточной Азии). Уровень социально-экономического развития этого государства зависит от его реального статуса как регионального и международного торгово-экономического центра. Сингапур реализует модель государственно-частного партнерства в области кибербезопасности, в которой государству отводится роль политически ориентированного субъекта, мнение представителей частного сектора играет решающую роль в определении механизма регулирования кибербезопасности, при этом представители частного сектора сами включены в институциональный механизм кибербезопасности. На сегодняшний день законодательному органу удалось найти баланс в обеспечении общественных интересов и защите прав и свобод граждан, что очень важно для поддержания и повышения инвестиционной привлекательности государства.

Основные правила кибербезопасности Сингапура включают, но не ограничиваются:

- Законом «О защите личных данных» 2012 г. (PDPA), всеобъемлющая правовая база, разработанная для обеспечения защиты личных данных;

- Законом «О защите личных данных» 2012 г. (PDPA), всеобъемлющая правовая база, разработанная для обеспечения защиты личных данных;

- Законом «О борьбе с киберпреступностью и другими киберугрозами»;

- Законом «О кибербезопасности и неправомерном использовании компьютеров»;

- Законом «О кибербезопасности» 2018 года, который направлен на защиту критически важной информационной инфраструктуры Сингапура и создание всеобъемлющей национальной системы кибербезопасности.

Необходимо отметить, что Сингапурское агентство кибербезопасности (CSA) было создано в качестве регулятора системы кибербезопасности для защиты страны от угроз и разработки национальных киберстратегий.

Помимо разработки и внедрения новой политики кибербезопасности, Агентство стимулирует развитие сферы кибербезопасности в стране. При этом Сингапур стал штаб-квартирой одного из подразделений Интерпола по борьбе с киберпреступностью, при которой действует новый операционный центр FireEye, разрабатывающий оптимальные решения для оперативного реагирования на угрозы безопасности.

В 2002 году Соединенные Штаты Америки приняли Закон «Об управлении информационной безопасностью», который регулирует: защиту от несанкционированного доступа, использования, раскрытия, распространения, изменения или уничтожения информации и информационных систем; защиту целостности информации от несанкционированного изменения или уничтожения; обеспечение конфиденциальности личной и имущественной информации; обеспечение надлежащего (безопасного) доступа к информации.

Между тем, Закон США «Об информационной безопасности» 1987 года по-прежнему играет важную роль. Он обеспечивает базовые и минимально необходимые меры для обеспечения информационной безопасности в федеральных компьютерных системах, без ограничения объема всех возможных действий. В соответствии с этим законом все государственные учреждения разрабатывают планы информационной безопасности для устранения рисков и предотвращения потенциального ущерба от потери данных, несанкционированного доступа или изменения федеральных систем.

Закон “Об обмене информацией о кибербезопасности” (CISA) – это федеральный закон США, который предусматривает «улучшение кибербезопасности в Соединенных Штатах для других целей посредством широкого обмена информацией об угрозах кибербезопасности». Закон принятый 27 октября 2015 года позволяет правительству США обмениваться информацией об Интернет трафике между технологическими и производственными компаниями.

Тем не менее, важность CISA неоднократно подвергалось сомнению его противниками, поскольку передача ответственности от частного бизнеса государству увеличивает уязвимость личных данных, а также распространение личной информации между ответственными государственными учреждениями, включая Агентство национальной безопасности и местную полицию.

Этот документ также обеспечивает дополнительную защиту для компаний, которые добровольно решили поделиться информацией о киберугрозах с государственными органами, которая может быть использована для незаконного распространения личной информации.

Документ определяет порядок взаимодействия государственных органов и частных компаний в сфере информационной безопасности. Закон направлен на защиту представителей бизнеса от воз-можных судебных исков со стороны пользователей, если информация о киберугрозах, предоставленная компетентным государственным органам, содержит личную информацию.

При этом ключевые решения по управлению рисками доверены владельцам и операторам информационной инфраструктуры. Государственные учреждения предоставляют этим лицам информацию об угрозах, стандартах управления рисками, передовых методах и возможных решениях.

В нашей стране вопросы ответственности за совершение преступлений с использованием информационных технологий предусмотрены Уголовным кодексом (ст.ст. 103, 1031, 1881, 2441, 278, Глава XXI преступления в сфере информационных технологий, ст. ст. 2781-2787), Кодексом об административной ответственности (ст.ст. 155, 1551, 191). В марте 2020 года для Республики Узбекистан вступило в силу Соглашение «О сотрудничестве государств-участников содружества независимых государств в борьбе с преступлениями в сфере информационных технологий» (подписанное в Душанбе 28 сентября 2018 года). Вместе с тем, в национальном законодательстве существует необходимость дальнейшего

совершенствования вопросов ответственности за преступления, совершаемые с использованием информационных технологий.

Основные направления профилактики киберпреступности

Во-первых, в борьбе с киберпреступлениями большую роль играет профилактика и обучение. Условно говоря, в каждой школе должен быть хотя бы один учитель, который может внятно рассказать, показать и объяснить детям, что такое киберриски, как вести себя в сети Интернет, что такое этика киберпространства, как обезопасить себя в Интернете.

Второе направление – это работа с кадрами правоохранительных органов. Это необходимость создания и внедрения специализированных учебных программ, по обучению специалистов в области обеспечения кибербезопасности.

И третье направление противодействия и профилактики киберпреступности – это расширение полномочий больших интернет-сервисов, провайдеров услуг, социальных платформ в своевременном выявлении и предупреждении подозрительных фактов и активностей в сети Интернет. Предоставление им больших прав и возложение обязанности по блокированию вредоносного содержания тех интернет-ресурсов, которые занимаются преступной деятельностью, привлекают своих жертв через Интернет, стимулирование к разработке и внедрению новых инновационных технологий по раннему предупреждению киберопасностей.

Кроме того, по мнению видного ученого, доктора юридических наук Расулева А.К. в Узбекистане следует создать специальную лабораторию при Центре информационной безопасности и содействия в обеспечении общественного порядка для проведения испытательных и исследовательских работ, а также тестирования средств защиты в области информационной безопасности. Данная лаборатория будет осуществлять функции своеобразного «полигона» по испытанию новейших средств защиты от компьютерных вирусов, вредоносных программ, взломов и т.д. К примеру, в России, Беларуси, Венгрии и ряде государств существуют аналогичные компании по обеспечению информационной безопасности, деятельность которых направлена на защиту информации ограниченного доступа в органах государственной власти, государственных учреждениях и предприятиях, организациях банковской системы и коммерческом секторе[3].

Вместе с тем необходимым условием успешной борьбы с киберпреступностью представляется дальнейшее развитие международного сотрудничества в сфере обеспечения информационной безопасности.

В целом на сегодняшний день можно считать, что в нашей стране сформирована прочная правовая база для осуществления государственной политики в сфере кибербезопасности. Вместе с тем следует продолжать совершенствование законодательства в сфере обеспечения кибербезопасности в целях дальнейшего улучшения государственного регулирования кибербезопасности, системы правового, организационного, научно-технического и нормативно-методического обеспечения, а также обеспечения целостности информационных систем и ресурсов.

[3] *Противодействие преступлениям в сфере информационных технологий и безопасности в Республике Узбекистан на современном этапе. Журнал юридических исследований, том 4, № 4, 2019 // https://naukaru.ru/ru/nauka/author/76067/view*

Использованные источники

1. Закон Республики Узбекистан “О кибербезопасности” (2022 г.) https://lex.uz/ru/docs/5960609
2. Постановление Президента Республики Узбекистан №ПП-167 “О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан” (31 мая 2023 г.) https://lex.uz/ru/docs/6479197
3. Закон Грузии “Об информационной безопасности” https://matsne.gov.ge/en/document/view/1679424?impose=translateRu&publication=4.
4. Закон Республики Казахстан “Об информатизации” https://adilet.zan.kz/rus/docs/Z1500000418
5. Закон Украины “Об основных принципах обеспечения кибербезопасности Украины” (2017 г.) https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Доктрина информационной безопасности Российской Федерации http://www.kremlin.ru/acts/bank/41460
7. Федеральный закон Российской Федерации “Об информации, информационных технологиях и защите информации” http://www.consultant.ru/document/cons_doc_LAW_61798/
8. Закон Китайской Народной Республики “О кибербезопасности” (2016 г.) https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin.
9. Закон Сингапура “О защите личных данных” (2012 г.) https://sso.agc.gov.sg/Act/PDPA2012
10. Закон Сингапура “О кибербезопасности” (2018 г.) https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312
11. Закон США “Об управлении информационной безопасностью” (2002 г.) https://www.congress.gov/bill/107th-congress/house-bill/3844
12. Закон США “Об информационной безопасности” (1987 г.) https://www.congress.gov/bill/100th-congress/house-bill/145
13. Закон США “Об обмене информацией о кибербезопасности” (CISA) (2015 г.) https://www.congress.gov/bill/114th-congress/senate-bill/754
14. Уголовный кодекс Республики Узбекистан https://lex.uz/docs/111457
15. Кодекс Республики Узбекистан об административной ответственности https://lex.uz/docs/97661
16. Соглашение “О сотрудничестве государств-участников содружества независимых государств в борьбе с преступлениями в сфере информационных технологий” (2018 г.) https://www.cisatc.org/1289/9115/135/9126/9128/9034
17. Отчет о киберугрозах за 2023 год. https://www.statista.com/study/134738/cyber-threat-report-2023/
18. Расулев А. К. Противодействие преступлениям в сфере информационных технологий и безопасности в Республике Узбекистан на современном этапе. Журнал юридических исследований, том 4, № 4, 2019. https://naukaru.ru/ru/nauka/article/34199/view