Устинов Иван Максимович
студент
Белицкий Кирилл Андреевич
студент
Текучева Светлана Николаевна
канд. техн. наук, доцент
ФГБОУ ВО «Донской государственный
технический университет»
г. Ростов-на-Дону, Ростовская область

НЕОДНОЗНАЧНОСТЬ ЗАКОНОДАТЕЛЬСТВА О КИБЕРБЕЗОПАСНОСТИ: МЕЖДУНАРОДНЫЙ И НАЦИОНАЛЬНЫЙ АСПЕКТЫ

***Аннотация**: статья посвящена анализу неоднозначности законодательства о кибербезопасности, рассматривая как международные, так и национальные аспекты. Освещается проблематика отсутствия унифицированных международных стандартов и соглашений, что ведёт к разнородности национальных подходов и создаёт сложности в международном сотрудничестве. Представлены конкретные примеры из различных юрисдикций и предложены пути решения проблемы, включая разработку международных стандартов и адаптивного национального законодательства. Акцентируется важность образования и повышения осведомлённости в области кибербезопасности для укрепления защиты на всех уровнях.*

***Ключевые слова**: кибербезопасность, международное законодательство, национальное законодательство, международное сотрудничество, защита данных, юридическая неопределённость, образование в области кибербезопасности, адаптивное законодательство, международные стандарты, гармонизация законов.*

В эпоху цифровизации кибербезопасность становится одним из центральных элементов национальной и международной безопасности. Однако, несмотря

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

на нарастающее осознание её важности, законодательство в этой области часто остаётся неоднозначным и противоречивым, что затрудняет его эффективное применение и сотрудничество на разных уровнях [2].

Международный аспект.

На международной арене основной проблемой является отсутствие универсального соглашения или договора, регулирующего вопросы кибербезопасности. Различные страны имеют свои подходы и стандарты, что создаёт сложности в согласовании общих правил. Например, Европейский союз принял Общий регламент по защите данных (GDPR), который стал эталоном в области защиты персональных данных, но такие меры не всегда приемлемы или применимы в других регионах.

Существуют и международные организации, такие как Международная организация стандартизации (ISO), которые разрабатывают стандарты, например, ISO/IEC 27001, охватывающие аспекты информационной безопасности. Однако принятие и интеграция этих стандартов в национальное законодательство происходят неравномерно.

Национальный аспект.

На национальном уровне каждая страна сталкивается со своими уникальными вызовами в регулировании кибербезопасности. Во многих странах законодательство развивается реактивно, часто в ответ на киберинциденты, что приводит к созданию списка из правил и стандартов, которые могут быть несогласованными или устаревшими к моменту их принятия [1].

Примером может служить законодательство США, где различные штаты могут иметь собственные законы о кибербезопасности, отличающиеся от федеральных норм. Это создаёт дополнительные сложности для компаний, которые должны соблюдать разные требования в разных юрисдикциях.

Проблемы и вызовы.

Одной из главных проблем неоднозначности законодательства является сложность обеспечения соблюдения законов. Когда законы расплывчаты или их интерпретация оставляет место для множества трактовок, организации и частные

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

лица могут столкнуться с трудностями в их понимании и применении. Это, в свою очередь, может вести к снижению общей защищённости данных и систем.

Кроме того, международное сотрудничество осложняется из-за отсутствия единой международной платформы для обмена информацией и опытом в области кибербезопасности. Различия в законодательстве могут препятствовать совместным операциям по предотвращению кибератак или быстрому реагированию на них.

Пути решения.

Для улучшения ситуации можно предложить несколько подходов. Во-первых, разработка международных стандартов и соглашений по ключевым аспектам кибербезопасности могла бы содействовать гармонизации национальных законов и упростить международное сотрудничество. Это требует активного участия и компромиссов со стороны всех государств.

Во-вторых, на национальном уровне страны могли бы пересмотреть свои подходы к законодательству, делая акцент на прозрачности, предсказуемости и гибкости. Принятие адаптивного законодательства, способного быстро реагировать на новые угрозы и технологии, улучшило бы общую защищённость и снизило бы юридическую неопределённость.

Также важным аспектом является образование и повышение осведомлённости как важные инструменты в борьбе с киберпреступностью. Обучение граждан и создание культуры безопасности способствуют более ответственному отношению к защите данных на всех уровнях общества.

Неоднозначность законодательства в области кибербезопасности ставит под угрозу как национальную, так и международную безопасность [3]. Эффективное решение этой проблемы требует совместных усилий на международном уровне, а также глубокой переработки национальных подходов к законодательству. Только через сотрудничество, инновации в законотворчестве и образование можно достичь стабильности и безопасности в цифровом мире.

Список литературы

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

1. Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом: монография / В.М. Елин; под ред. А.П. Баранова. – М.: Изд-во Моск. ин-та гос. управления и права, 2016. – С. 178–179. – EDN XRCLFL

2. Зиновьева Е.С. Международная информационная безопасность: монография / Е.С. Зиновьева; Моск. гос. ин-т междунар. отношений (ун-т) МИД России, каф. мировых политических процессов. – М.: МГИМО-Университет, 2013. – С. 267–268. – EDN SMVKMV

3. Зубова Л.В. Схема модели принятия управленческих решений на основе оценки рискоустойчивости хозяйствующих субъектов / Л.В. Зубова // Известия СПбГЭУ. – 2018. – №3. – С. 68.

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)