Реферат на тему ‘Законодательный уровень информационной безопасности’

Основы информационной безопасности

Закиров Нурислам Дамирович

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

1. Изучении законодательства РФ в области информационной безопасности;
2. Определении ключевых нормативных актов и их содержания;
3. Анализ механизмов защиты информации;
4. Рассмотрении проблем и перспектив развития законодательства в данной сфере.

2 Введение

Информационная безопасность (ИБ) представляет собой комплекс мер, направленных на защиту информации и информационных систем от несанкционированного доступа, уничтожения, модификации, блокирования или копирования. В условиях стремительного роста цифровых технологий и увеличения объемов данных вопросы информационной безопасности приобретают особую актуальность.

Законодательное регулирование играет ключевую роль в обеспечении защиты информации, устанавливая правила, обязанности и ответственность субъектов в данной сфере. В Российской Федерации сформирована обширная нормативная база, включающая Конституцию РФ, федеральные законы, подзаконные акты, приказы ведомств, а также международные стандарты

3 Основные понятия

Для понимания законодательного регулирования в области ИБ важно рассмотреть ключевые термины:

1. Информационная безопасность – защита информации и её носителей от угроз;
2. Конфиденциальность – ограничение доступа к информации;
3. Целостность – защита данных от модификации;
4. Доступность – обеспечение своевременного доступа к информации;
5. Персональные данные – информация, позволяющая идентифицировать личность.

4 Основные законы РФ в сфере ИБ

Законодательная база в России включает Конституцию, федеральные законы и подзаконные акты.

4.1 Конституция РФ

Конституция РФ закрепляет следующие положения:
Статья 23 – право граждан на защиту частной жизни;

1. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.
2. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.

Статья 24 – запрет на сбор и распространение информации без согласия;

1. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.
2. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

4.2 Федеральные законы

149-ФЗ («Об информации» – регулирует доступ, обработку и защиту данных). Регулирует оборот информации в России, разделяя её на общедоступную и ограниченного доступа (государственная, коммерческая тайна). Закон устанавливает правила обработки данных, требования к информационным системам и меры противодействия распространению запрещённого контента (например, экстремистских материалов). Также определяет порядок блокировки сайтов и ответственность операторов связи.

152-ФЗ («О персональных данных» – устанавливает требования к защите ПДн). Обязывает операторов ПДн получать согласие граждан на обработку их данных и обеспечивать защиту от утечек. Закон требует уведомлять Роскомнадзор о работе с ПДн, хранить информацию на серверах в РФ (локализация) и применять меры защиты в зависимости от категории данных. За нарушения предусмотрены штрафы до 6 млн руб.

187-ФЗ («О КИИ» – определяет меры защиты критической инфраструктуры). Направлен на защиту объектов, чей выход из строя угрожает безопасности страны (энергетика, транспорт, банки). Закон обязывает организации выявлять и защищать критически важные системы, проводить аудиты безопасности и использовать сертифицированные средства защиты. Контроль осуществляют ФСТЭК и ФСБ, а за нарушения грозят крупные штрафы и уголовная ответственность.

5 Примеры нарушений и угроз информационной безопасности.

Рассмотрим несколько реальных примеров киберинцидентов в России:

1. Утечка данных клиентов Сбербанка (2019 год) – более 60 млн записей оказалось в открытом доступе.
2. Взлом серверов российских министерств (2022 год) – утечка служебных документов.
3. Атака на систему голосования «Госуслуги» (2023 год) – DDoS-атака привела к временному сбою.

6 Органы регулирования информационной безопасности

6.1 ФСТЭК (Федеральная служба по техническому и экспортному контролю)

Основные функции:

-Утверждает требования к защите информации (например, Приказ № 239 о защите ГИС) -Проводит сертификацию средств защиты информации (СЗИ) -Контролирует безопасность критической информационной инфраструктуры (КИИ) -Разрабатывает методики противодействия кибератакам

Пример: ФСТЭК проверяет банки и энергетические компании на соответствие требованиям 187-ФЗ, выдает предписания об устранении уязвимостей.

6.2 ФСБ (Федеральная служба безопасности)

Основные функции:

-Лицензирует деятельность по криптографической защите данных (Приказ № 66) -Борется с кибершпионажем и компьютерными атаками на госструктуры -Контролирует использование шифровальных средств -Расследует преступления в сфере ИБ (ст. 272–274 УК РФ)

Пример: ФСБ выявляет хакерские группы, атакующие российские госучре-

ждения, и блокирует их деятельность.

6.3 Роскомнадзор (Федеральная служба по надзору в сфере связи, ИТ и массовых коммуникаций)

Основные функции:

-Контролирует соблюдение 152-ФЗ (персональные данные) -Ведет реестр нарушителей закона о ПДн -Блокирует незаконный контент в интернете (по 149-ФЗ) -Налагает штрафы за утечки данных (до 6 млн руб. для юрлиц)

Пример: Роскомнадзор оштрафовал соцсеть за хранение данных россиян на зарубежных серверах.

6.4 Минцифры (Министерство цифрового развития, связи и массовых коммуникаций)

Основные функции:

-Разрабатывает стратегии развития ИБ (например, “Стратегия кибербезопасности РФ до 2030 года”) -Координирует цифровизацию госуслуг с учетом требований безопасности -Участвует в создании законопроектов (например, о регулировании ИИ) -Внедряет новые технологии защиты (квантовая криптография, биометрия)

Пример: Минцифры инициировало закон о защите данных в системах с искусственным интеллектом.

7 Проблемы и перспективы развития законодательства в сфере ИБ

7.1 Стремительное развитие технологий (ИИ, квантовые вычисления)

Проблемы:

-Отставание нормативной базы: Законы не успевают адаптироваться к новым угрозам (например, deepfake-мошенничество или атаки с использованием ИИ). -Неопределенность регулирования: Отсутствие четких норм для квантовой криптографии, нейросетей и IoT-устройств. -Пример: ChatGPT и аналогичные ИИ-сервисы могут генерировать вредоносный код, но меры противодействия в 149-ФЗ не прописаны.

Пути решения:

-Создание “регуляторных песочниц” для тестирования новых технологий (пилотные проекты Минцифры). -Гибкие поправки в законы (как в случае с криптовалютами).

7.2 Недостаточная осведомленность бизнеса о требованиях безопасности

Проблемы:

-Малый и средний бизнес часто игнорирует 152-ФЗ, считая его избыточным. -Путаница в стандартах: Компании не различают требования ФСТЭК (Приказ № 239) и ФСБ (Приказ № 378). Пример: Утечка данных в сети клиник (2023 г.) из-за отсутствия шифрования, хотя это прямое нарушение ст. 19 152-ФЗ.

Пути решения:

-Обязательные обучающие программы для ИТ-специалистов (инициатива Роскомнадзора). -Упрощение нормативов для малого бизнеса (например, базовый чек-лист от Минцифры).

7.3 Трудности в привлечении к ответственности киберпреступников

Проблемы:

-Анонимность в DarkNet: 80% атак проводятся через TOR или VPN (данные ФСБ). -Международный характер преступлений: Хакеры атакуют из-за рубежа, а экстрадиция почти невозможна. Пример: Группировка LockBit, действующая из неизвестной юрисдикции, годами избегает правосудия.

Пути решения:

-Развитие международного сотрудничества (вступление в конвенции, обмен данными с INTERPOL). -Технические меры: блокировка криптовалютных транзакций для вымогателей (опыт ЦБ РФ).

8 Заключение

Законодательство РФ в сфере информационной безопасности развивается в ответ на растущие вызовы цифрового мира. Основные тенденции включают усиление защиты персональных данных, контроль за критической инфраструктурой и гармонизацию с международными стандартами. Однако, для повышения эффективности необходимо постоянно совершенствовать нормативную базу, повышать уровень киберграмотности населения и бизнеса, а также усиливать международное сотрудничество.

9 Выводы

Изучили законодательные акты РФ в сфере информационной безопасности, определили механизмы защиты информации, рассмотрели актуальные угрозы и способы их минимизации, а также оценили перспективы развития законодательства в данной сфере.

Список источников

1. Конституция РФ – http://www.consultant.ru/document/cons_doc_LAW_28399/
2. Федеральный закон №149-ФЗ – http://www.consultant.ru/document/cons_doc_LAW_61798/
3. Федеральный закон №152-ФЗ – http://www.consultant.ru/document/cons_doc_LAW_61801/
4. Официальный сайт ФСТЭК – https://fstec.ru/
5. Официальный сайт Роскомнадзора – https://rkn.gov.ru/