УДК 004.056

**КИБЕРБЕЗОПАСНОСТЬ И ПРАВО: КАК ЗАКОНЫ РЕГУЛИРУЮТ ЗАЩИТУ ВЕБ-ПРИЛОЖЕНИЙ ОТ КИБЕРАТАК И УТЕЧЕК ДАННЫХ**

**ПРАВОВОЕ РЕГУЛИРОВАНИЕ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ ОТ КИБЕРАТАК И УТЕЧЕК ДАННЫХ**

**Худалов Эльбрус Ибрагимович,** студент 3курса специальности 09.03.03 Прикладная информатика в экономике Факультета информационных технологий и электронной техники Северо-Кавказского горно-металлургического института (государственного технологического университета), г. Владикавказ, Российская Федерация

Научный руководитель: **Чеджемов Сергей Русланович**, профессор кафедры органов власти и публичного права Северо-Кавказского горно-металлургического института (ГТУ), кандидат исторических наук, доктор педагогических наук, профессор теории и истории государства и права.

**Аннотация.** ВСтатье рассматриваются вопросы правового регулирования кибербезопасности в Российской Федерации, акцентируется внимание на законодательстве, регулирующим защиту веб-приложений от кибератак и утечек данных, в частности анализируются основные нормативные акты, такие как Федеральный закон № 152-ФЗ "О персональных данных" и Указ Президента РФ № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". В качестве вывода предлагается особое внимание уделять проблемам, связанным с соблюдением требований законодательства в виде популяризации требований законодательства на этот счет, а также предложены рекомендации по улучшению правовой базы для повышения уровня защищенности веб-приложений общего пользования.

**Ключевые слова**: Кибербезопасность, защита данных, кибератаки, законодательство Российской Федерации, правовое регулирование, веб-приложения, утечки данных.

**CYBERSECURITY AND LAW: HOW LAWS REGULATE THE PROTECTION OF WEB APPLICATIONS FROM CYBER ATTACKS AND DATA LEAKS**

Elbrus Ibrahimovich Khudalov, 3rd year student, 09.03.03 Applied Informatics in Economics, Faculty of Information Technology and Electronic Engineering, North Caucasus Mining and Metallurgical Institute (State Technological University), Vladikavkaz, Russian Federation

Scientific supervisor: Sergey RuslanovichChedzhemov, Professor of the Department of Government and Public Law at the North Caucasus Mining and Metallurgical Institute (GTU), Candidate of Historical Sciences, Doctor of Pedagogical Sciences, Professor of Theory and History of State and Law.

**Annotation**. The article examines the issues of legal regulation of cybersecurity in the Russian Federation, focusing on legislation aimed at protecting web applications from cyber attacks and data leaks. The interaction of cybersecurity and law is investigated, and the main regulatory acts such as Federal Law No. 152-FZ "On Personal Data" and Presidential Decree No. 646 "On Approval of the Information Security Doctrine of the Russian Federation" are analyzed. Special attention is paid to problems related to compliance with legal requirements, and recommendations are also proposed to improve the legal framework for improving the security of web applications. Keywords: Cybersecurity, data protection, cyber-attacks, legislation, legal regulation, web applications, data leaks.

**Keywords**: Cybersecurity, data protection, cyber attacks, legislation, legal regulation, web applications, data leaks.

**Введение**

Цифровая эпоха принесла с собой не только новые возможности, но и значительные риски. Кибератаки и утечки данных стали одной из главных угроз современности, затрагивающих как государственные структуры, так и частные компании. В условиях глобализации экономики и информационной среды возрастает необходимость разработки эффективных правовых механизмов для защиты веб-приложений от киберпреступников. Настоящая статья посвящена исследованию вопросов правового регулирования кибербезопасности, анализу существующих законодательных актов и выявлению пробелов в правовом поле, требующих внимания и доработки.

**Основные понятия и термины**

Прежде чем перейти к рассмотрению российского законодательства, уточним основные термины, используемые в рамках темы:

Кибербезопасность — это совокупность мероприятий и технологий, направленных на защиту информационных систем, сетей и данных от несанкционированного доступа, модификации или разрушения.

Утечка данных — это случайное или преднамеренное разглашение конфиденциальной информации, приводящее к потенциальному ущербу для владельцев данных.

Правовое регулирование — это система юридических норм, предписывающих поведение участников общественных отношений в сфере кибербезопасности и устанавливающих ответственность за нарушение установленных правил.

**Законодательство в области кибербезопасности в России**

Российское законодательство в области кибербезопасности включает несколько ключевых актов, которые регулируют защиту персональных данных и информацию в целом.

**Федеральный закон "О персональных данных"**

Федеральный закон Федеральный закон № 152-ФЗ "О персональных данных", принятый в 2006 году, является основным нормативным актом, регулирующим обработку и защиту персональной информации в России. Закон устанавливает требования к сбору, хранению и обработке персональных данных, включая необходимость получения согласия субъектов на обработку их данных. Организации обязаны обеспечивать безопасность данных и принимать меры по предотвращению утечек [1]

**Закон "О безопасности критической информационной инфраструктуры"**

Федеральный закон № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", принятый в 2017 году, определяет основные принципы защиты критически важной информации, включая меры по предотвращению кибератак на объекты критической инфраструктуры. Закон обязывает организации, работающие с критической информацией, разрабатывать и внедрять системы защиты и реагирования на инциденты [2].

**Законодательство о борьбе с киберпреступностью**

В России также действуют нормы уголовного законодательства, направленные на борьбу с киберпреступностью. Уголовный кодекс РФ содержит статьи, касающиеся несанкционированного доступа к компьютерной информации (статья 272), создания и распространения вредоносных программ (статья 273) и других преступлений в сфере информационных технологий [3].

**Обязанности организаций по обеспечению кибербезопасности**

Законы обязывают организации принимать меры для защиты своих веб-приложений от кибератак. К таким мерам относятся: Оценка рисков,регулярная оценка уязвимостей системы позволяет выявить слабые места и принять меры по их устранению. Также обучение сотрудников так какобучение сотрудников основам кибербезопасности становится необходимым для снижения риска атак через человеческий фактор. Но немало важным является шифрование данных, потому чтоиспользование шифрования для защиты конфиденциальной информации снижает риск утечек. По мимо всего необходим мониторинг и реагирование на инциденты, организации должны иметь планы по реагированию на инциденты и мониторингу систем для быстрого выявления угроз [7]**.**

**Ответственность за нарушение норм кибербезопасности**

Соблюдение норм кибербезопасности в России является обязательным для всех организаций, работающих с персональными данными и информацией. За несоблюдение этих норм предусмотрены различные меры ответственности, которые могут быть как административными, так и уголовными.

Федеральный закон "О персональных данных" (152-ФЗ) устанавливает административную ответственность за нарушение требований к обработке персональных данных. В частности, это может включать:

• **Штрафы**: за нарушение норм закона на юридических лиц могут накладываться штрафы, которые варьируются в зависимости от характера нарушения. Например, за отсутствие согласия субъекта на обработку данных или за неисполнение требований по обеспечению безопасности персональных данных размер штрафа может достигать нескольких миллионов рублей.

• **Предписания**: кроме штрафов, уполномоченные органы, такие как Роскомнадзор, могут выдавать предписания об устранении нарушений. Организациям может быть дан срок для исправления ситуации, и несоблюдение этого предписания также может повлечь за собой дополнительные штрафы [6].

Уголовный кодекс Российской Федерации также содержит нормы, касающиеся киберпреступлений. Основные статьи, которые могут быть применены в случае нарушений кибербезопасности:

**Статья 272** — Несанкционированный доступ к компьютерной информации: Эта статья предусматривает уголовную ответственность за несанкционированный доступ к компьютерным системам и базам данных. Наказание может варьироваться от штрафа до лишения свободы на срок до 5 лет в зависимости от обстоятельств дела [3].

**Статья 273** — Создание и распространение вредоносных программ: Эта статья касается создания и распространения программ, предназначенных для несанкционированного доступа к компьютерной информации или для причинения вреда информационным системам. Наказание может включать лишение свободы на срок до 7 лет [4].

**Статья 274** — Нарушение правил эксплуатации средств обработки информации: Эта статья охватывает случаи, когда действия сотрудников или организаций приводят к утечке данных или другим инцидентам в области кибербезопасности [5].

**Заключение**

Кибербезопасность и право в России — это взаимосвязанные области, которые требуют постоянного внимания со стороны как государственных органов, так и частного сектора. Эффективное законодательство может значительно повысить уровень защиты веб-приложений и данных пользователей, а также обеспечить ответственность организаций за соблюдение норм безопасности. В условиях постоянно меняющегося цифрового ландшафта важно не только следовать существующим законам, но и активно участвовать в их разработке и совершенствовании.

Список используемых источников и литературы

1. № 152-ФЗ "О персональных данных"

<https://www.consultant.ru/document/cons_doc_LAW_61801/>

Дата обращения 20.04.2025.

1. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

<https://www.consultant.ru/document/cons_doc_LAW_220885/>. Дата обращения 12.04. 2025.УК РФ

1. Статья 272. Неправомерный доступ к компьютерной информации

<https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/> Дата обращения 20.04.2025.

1. УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ

<https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/> Дата обращения 20.04.2025.

1. УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей <https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/> Дата обращения 20.04.2025
2. Статья 19.6.1 КоАП РФ. <https://www.consultant.ru/document/cons_doc_LAW_34661/073e7610ef13acfc057ac554e6bc9a5df165e55a/> Дата обращения 20.04.2025
3. Матяш Екатерина Дмитриевна, Никонов Вячеслав Викторович, Иванова Ирина Алексеевна «Обеспечение безопасности Web-сайтов» // Текст научной статьи по специальности «Компьютерные и информационные науки», 2016. C.161-168.
4. Полухтин И.М. ПРАВОВОЕ РЕГУЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ // Вестник науки №6 (63) том 4. С. 618 - 622. 2023 г. ISSN 2712-8849 /