

**Ссылка для цитирования этой статьи:**

Ганиева Л.Р., Никифоров А.Ю. Механизмы правового регулирования и обеспечения информационной безопасности объектов топливно-энергетического комплекса Российской Федерации в условиях цифровизации // Human Progress. 2025. Том 11, Вып. 1. С. 33. URL: [http://progress-human.com/images/2025/Tom11\\_1/Ganieva.pdf](http://progress-human.com/images/2025/Tom11_1/Ganieva.pdf) DOI 10.46320/2073-4506-2025-1a-33.

## **МЕХАНИЗМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ**

**Ганиева Лиана Ринатовна**

магистрант кафедры «Социальные и политические коммуникации»,  
Уфимский государственный нефтяной технический университет  
г. Уфа, Российская Федерация

**Никифоров Александр Юрьевич**

кандидат политических наук,  
доцент кафедры «Социальные и политические коммуникации»,  
Уфимский государственный нефтяной технический университет  
г. Уфа, Российская Федерация

**Аннотация.** В условиях цифровизации объектов топливно-энергетического комплекса (ТЭК) РФ резко возросла уязвимость их информационных систем к киберугрозам, включая атаки на SCADA-комплексы, утечки данных через IoT-устройства и нарушения целостности критических процессов. Объект исследования — объекты ТЭК Российской Федерации. Предмет исследования — механизмы правового регулирования и обеспечения информационной безопасности. Цель исследования — повышение уровня информационной защиты объектов ТЭК через совершенствование существующих механизмов. Несмотря на наличие законодательной базы (ФЗ-187, ФЗ-152, ISO/IEC 27001), механизмы регулирования не учитывают специфику отрасли, что подтверждается анализом методологий оценки рисков (OCTAVE, NIST SP 800-30) и пробелами в реализации мер защиты. Исследование выявляет зависимость эффективности кибербезопасности от внешних факторов (санкции, технологические ограничения) и недостаток кадрового потенциала. Предложены меры по ужесточению контроля за соблюдением нормативных актов, внедрению отраслевых стандартов, обучению сотрудников и стимулированию инноваций.

**Ключевые слова:** цифровизация, информационная безопасность, правовое регулирование, топливно-энергетический комплекс, риски кибербезопасности, законодательные меры, защита данных.

## **Введение**

Цифровизация топливно-энергетического комплекса Российской Федерации становится ключевым фактором модернизации отрасли. Однако, с внедрением передовых технологий, таких как интернет вещей (IoT), искусственный интеллект и блокчейн, возрастает риск кибератак на объекты ТЭК. Эти системы являются стратегически важными для экономики страны, и их дестабилизация может привести к значительным последствиям. В связи с этим актуальность темы правового регулирования и обеспечения информационной безопасности становится особенно высокой. Настоящая статья направлена на анализ существующих механизмов защиты и предложений по их совершенствованию.

## **Методология исследования**

Методология исследования включает в себя несколько этапов, каждый из которых позволяет глубже понять текущую ситуацию и предложить пути её улучшения. Первым этапом является анализ нормативно-правовой базы, которая регулирует вопросы информационной безопасности в ТЭК. Это включает изучение Федеральных законов, постановлений правительства и других нормативных актов, которые затрагивают данную область. Например, Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] и Федеральный закон № 152-ФЗ «О персональных данных» [2].

На втором этапе проводится оценка текущего состояния информационной безопасности на объектах ТЭК. Эти методы позволяют получить объективную информацию о том, какие меры безопасности уже внедрены, какие из них оказались наиболее эффективными, а какие требуют доработки.

На третьем этапе исследования выполняется комплексная оценка потенциальных опасностей и угроз. Для этих целей используются специализированные аналитические инструменты, включая риск-ориентированные матрицы и системно-динамические подходы. Такие методологии позволяют не только идентифицировать слабые места в существующих системах, но и разработать целенаправленные стратегии минимизации выявленных негативных факторов. Применение комбинированных оценочных моделей обеспечивает

многогранный анализ угроз, что значительно повышает эффективность принимаемых решений в области риск-менеджмента.

Четвёртым этапом является разработка рекомендаций и предложений по совершенствованию существующих механизмов правового регулирования и обеспечения информационной безопасности. На этом этапе используются методы экспертных оценок, а также моделирование различных сценариев развития событий. Это позволяет создать комплексный план действий, который будет максимально эффективным в условиях цифровизации.

### **Обзор литературы и нормативных актов**

В течение последних лет в Российской Федерации принят ряд законодательных актов, направленных на обеспечение информационной безопасности в различных сферах. Основными документами, регулирующими вопросы кибербезопасности в ТЭК, являются:

1. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1]. Указанный закон, вступивший в силу в 2017 году, является одним из ключевых документов, регулирующих вопросы защиты критической информационной инфраструктуры, к которой относятся объекты ТЭК. Закон устанавливает основные требования к защите информации, используемой в процессах управления и контроля технологическими системами. Особое внимание уделяется:

- идентификации объектов критической информационной инфраструктуры;
- оценке рисков кибератак и технических сбоев;
- внедрению мер защиты, включая физические, организационные и технические средства.

Кроме того, закон обязывает организации проводить регулярные аудиты и проверки состояния информационной безопасности, а также своевременно устранять выявленные уязвимости. Это создает правовые основы для защиты объектов ТЭК от киберугроз и предписывает разработку специальных стандартов безопасности, которые должны быть соблюдены всеми участниками данной отрасли.

2. Федеральный закон № 152-ФЗ «О персональных данных»[2]. Принятый в 2006 году, этот закон регулирует вопросы обработки и защиты персональных данных, в том числе на объектах ТЭК. В рамках данного закона операторы обязаны:

- обеспечивать конфиденциальность данных сотрудников и потребителей услуг;
- внедрять меры защиты информации, включая использование средств шифрования и ограничение доступа к данным;

- осуществлять регулярный аудит систем хранения и обработки персональных данных.

Для ТЭК это особенно важно, так как многие организации собирают и обрабатывают большие объемы данных о клиентах, партнерах и сотрудниках, что требует дополнительного внимания к защите данной информации.

3. Правила обработки персональных данных при использовании информационных систем личных данных[3]. Эти правила, утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года, детализируют требования к защите персональных данных, установленные Федеральным законом № 152-ФЗ. Они обязывают организации:

- внедрять организационные и технические меры защиты данных;
- проводить обучение персонала по вопросам информационной безопасности;
- использовать сертифицированные системы защиты информации.

На объектах ТЭК данные требования имеют особое значение, поскольку утечка персональных данных может привести не только к финансовым потерям, но и к дестабилизации работы всей системы.

Также стоит отметить разработанные Минэнерго РФ рекомендации и методические указания по обеспечению кибербезопасности в ТЭК [4], направленные на обеспечение кибербезопасности в ТЭК. Эти документы включают:

- стандарты оценки уязвимостей и минимизации рисков;
- методики проведения аудитов информационной безопасности;
- рекомендации по внедрению современных технологий защиты данных.

Например, в рекомендациях Минэнерго РФ предлагается использовать единые протоколы взаимодействия между различными элементами цифровых систем, что позволит минимизировать риски кибератак. Также рекомендуется внедрять системы мониторинга и анализа событий безопасности (SIEM), которые позволяют в реальном времени отслеживать подозрительную активность и оперативно реагировать на угрозы.

Анализ нормативной базы выявляет существенные пробелы в регулировании объектов топливно-энергетического комплекса (ТЭК). Действующие стандарты, в частности в сфере защиты данных, зачастую разрабатываются без учета специфики энергетических систем. Это приводит к ситуации, когда общепринятые требования оказываются неприменимыми к инфраструктуре ТЭК из-за ее уникальной архитектуры, повышенных рисков киберугроз и критических требований к бесперебойности функционирования.

Таким образом, обзор литературы, нормативных актов показывает, что существующая правовая база требует дальнейшего совершенствования для обеспечения эффективной защиты объектов ТЭК в условиях цифровизации [7], [8].

## **Анализ текущего состояния правового регулирования**

Несмотря на наличие вышеупомянутых документов, существует ряд проблем, связанных с их применением в реальных условиях. Одним из основных вызовов является недостаточное осознание важности кибербезопасности со стороны руководства энергокомпаний. Это влечёт за собой, что многие предприятия не уделяют должного внимания внедрению необходимых мер защиты. Другая проблема заключается в нехватке квалифицированных специалистов, способных адекватно оценивать и минимизировать риски.

Существующие методы защиты информации в этом секторе имеют свои плюсы и минусы.

Достоинства:

- Комплексный подход: В ТЭК используется системный и комплексный подход к защите информации, который учитывает все актуальные и вероятные угрозы и уязвимости. Это позволяет создать многоуровневую защиту, охватывающую как технические, так и организационные меры.

- Соблюдение законодательства: Методы защиты информации в ТЭК соответствуют требованиям российского законодательства, таким как ФЗ «О коммерческой тайне», Постановления Правительства РФ о сертификации средств защиты информации и Приказы ФСБ о шифровальных средствах. Это обеспечивает соблюдение правовых норм и стандартов.

- Защита критических информационных процессов: В каждой подотрасли ТЭК выделены критические информационные процессы, которые требуют особой защиты. Это позволяет сосредоточить усилия на наиболее уязвимых участках и минимизировать риски.

Недостатки:

- Высокая сложность реализации: Комплексный подход требует значительных ресурсов и высокой квалификации специалистов. Это может быть сложно и дорого для предприятий, особенно в условиях ограниченного бюджета.

- Зависимость от внешних факторов: Несмотря на наличие законодательной базы, эффективность мер защиты может зависеть от внешних факторов, таких как изменения в законодательстве или международные санкции, что может осложнить их реализацию.

- Риски кибератак: Несмотря на все меры, риски компьютерных атак остаются высокими. Кибератаки могут привести к приостановке работы, сбоям и авариям на промышленных объектах, что может иметь серьезные последствия для всего комплекса.

Таким образом, методы информационной защиты в ТЭК РФ обеспечивают высокий уровень безопасности, но требуют доработок и значительных усилий и ресурсов для их реализации, а также остаются уязвимыми к внешним угрозам.

## **Анализ рисков и угроз в информационной безопасности**

### **1. Особенности ТЭК в контексте информационной безопасности**

Топливо-энергетический комплекс включает в себя множество подотраслей:

- Добыча и переработка нефти и газа.
- Производство электроэнергии.
- Транспортировка энергоресурсов (трубопроводы, электросети).
- Хранение и распределение энергоресурсов.

Эти процессы характеризуются высокой степенью автоматизации и интеграции с информационными системами, что делает их уязвимыми для кибератак. Основные угрозы включают:

- Кибератаки на системы управления технологическими процессами (SCADA, ICS).
- Атаки на системы мониторинга и диагностики.
- Утечка конфиденциальной информации.
- Нарушение целостности данных.
- Физические атаки на инфраструктуру, усиленные киберкомпонентами.

### **2. Модели оценки рисков в информационной безопасности**

Для анализа рисков в топливо-энергетическом комплексе (ТЭК) применяются различные методики, позволяющие оценивать угрозы как количественно, так и качественно. Основные подходы включают:

а) Методология OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Разработанная CERT, эта методика самооценки рисков фокусируется на трёх ключевых элементах:

- Выявление критически важных активов.
- Анализ угроз и уязвимостей.
- Разработка мер по минимизации рисков.

В контексте ТЭК, OCTAVE может использоваться для выявления слабых мест в системах управления трубопроводами или энергетическими объектами.

б) Стандарт NIST SP 800-30

Этот подход, созданный Национальным институтом стандартов и технологий США, включает пять этапов:

1. Подготовка к оценке рисков.
2. Идентификация угроз и уязвимостей.
3. Оценка последствий и вероятности реализации угроз.

4. Расчёт уровня риска.

5. Формирование рекомендаций по снижению рисков.

Методология широко применяется в международной практике и адаптируется для нужд ТЭК.

в) Стандарт ISO/IEC 27005

Международный стандарт управления рисками в области информационной безопасности (ИБ) предполагает:

- Картографирование активов, угроз и уязвимостей.
- Оценку последствий и вероятности инцидентов.
- Выбор стратегий управления рисками (нейтрализация, передача, принятие).

Данный подход универсален и подходит для внедрения систем менеджмента ИБ в ТЭК.

### 3. Матрица рисков

Матрица рисков — инструмент визуализации и классификации угроз на основе их вероятности и тяжести последствий. В ТЭК она позволяет ранжировать риски и определять приоритеты для оперативного реагирования.

Пример матрицы рисков:

Последствия \ Вероятность	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Катастрофические	Низкий	Средний	Высокий	Критический	Критический
Серьезные	Низкий	Средний	Средний	Высокий	Критический
Умеренные	Низкий	Низкий	Средний	Средний	Высокий
Незначительные	Низкий	Низкий	Низкий	Средний	Средний

### **Предложения по совершенствованию механизмов правового регулирования**

Для повышения уровня информационной безопасности объектов ТЭК предлагается следующий комплекс мероприятий:

#### 1. Ужесточение контроля за соблюдением нормативных актов

Необходимо создать единую систему мониторинга и контроля за выполнением требований кибербезопасности. Эта система должна включать регулярные проверки предприятий и обязательные аудиты для выявления слабых мест в системах защиты.

#### 2. Обучение и сертификация сотрудников

Введение обязательных курсов по кибербезопасности для всех сотрудников, работающих с информационными системами ТЭК. Кроме того, необходимо внедрить систему сертификации специалистов, которая будет подтверждать их профессиональную компетентность в данной области.

### 3. Разработка новых стандартов и методик

Необходимо разработать и внедрить новые стандарты, учитывающие специфику работы объектов ТЭК. Например, можно создать единый протокол для взаимодействия между различными элементами цифровых систем, который будет минимизировать риски кибератак.

### 4. Стимулирование внедрения современных технологий

Государство должно активно стимулировать внедрение инновационных решений в области кибербезопасности. Это может быть сделано через предоставление налоговых льгот или грантов на разработку и внедрение новых технологий.

## Заключение

Цифровизация топливно-энергетического комплекса России открывает новые возможности для повышения эффективности и устойчивости энергосистем. Однако, для успешного функционирования этих систем в условиях возрастающей киберугрозы требуется усиленное внимание к вопросам правового регулирования и информационной безопасности. В статье были рассмотрены существующие проблемы и предложены пути их решения. Внедрение предложенных мер позволит повысить уровень защиты объектов ТЭК и обеспечить надежное функционирование энергосистем в будущем.

## Список литературы

1. Федеральный закон Российской Федерации № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 (с изменениями на 01.03.2022).
2. Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных» от 27.07.2006 (с изменениями на 01.03.2022).
3. Постановление Правительства Российской Федерации № 1119 от 01.11.2012 «Об утверждении правил обработки персональных данных при использовании информационных систем персональных данных» (с изменениями на 27.03.2021).
4. Министерство энергетики Российской Федерации. Рекомендации по обеспечению кибербезопасности в топливно-энергетическом комплексе. Москва: Минэнерго России, 2020.
5. Software Engineering Institute. Методология OCTAVE Allegro: улучшение процесса оценки рисков информационной безопасности / Software Engineering Institute. — Питтсбург: Университет Карнеги-Меллона, 2007. [Электронный ресурс]. Режим доступа: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8296>.

6. Национальный институт стандартов и технологий (NIST). Руководство по проведению оценки рисков (NIST Special Publication 800-30) / Национальный институт стандартов и технологий (NIST). — 2020. <https://doi.org/10.6028/NIST.SP.800-30r1>.
7. Кретьова, А. Ю. Оценка несистематических рисков и ущерба в нефтегазовом комплексе / А. Ю. Кретьова // Дискуссия. 2024. № 6 (127). С. 97-102. DOI 10.46320/2077-7639-2024-6-127-97-102. – EDN AIEVRP.
8. Скрыбин А.В. Правовое регулирование отношений в сфере добычи нефти и газа: выявление проблемных аспектов / А.В. Скрыбин // Евразийский юридический журнал. 2024. № 6 (193). С. 296-298. EDN CXIHNN.

## **MECHANISMS OF LEGAL REGULATION AND ENSURING INFORMATION SECURITY OF FUEL AND ENERGY FACILITIES OF THE RUSSIAN FEDERATION IN THE CONTEXT OF DIGITALISATION**

**Ganieva Liana Rinatovna**

Master's student of the Department of "Social and Political Communications",  
Ufa State Petroleum Technological University,  
Ufa, Russian Federation

**Nikiforov Aleksandr Yurievich**

Candidate of Political Sciences, Associate Professor at the Department of "Social and Political Communications",  
Ufa State Petroleum Technological University  
Ufa, Russian Federation

**Abstract.** In the context of digitalization of the Russian fuel and energy complex (FEC), the vulnerability of its information systems to cyber threats has sharply increased, including attacks on SCADA systems, data leaks through IoT devices, and integrity breaches of critical processes. The research object is the facilities of the Russian Federation's fuel and energy complex. The research subject is the mechanisms of legal regulation and information security. The study aims to enhance the level of information protection for FEC facilities by improving existing mechanisms. Despite the existing legislative framework (Federal Law No. 187-FZ, Federal Law No. 152-FZ, ISO/IEC 27001), regulatory mechanisms fail to account for industry-specific challenges, as evidenced by an analysis of risk assessment methodologies (OCTAVE, NIST SP 800-30) and gaps in the implementation of protective measures. The study reveals that the effectiveness of cybersecurity depends on external factors (sanctions, technological constraints) and a shortage of qualified personnel. Proposed measures include stricter oversight of regulatory compliance, adoption of industry standards, employee training, and incentives for innovation.

**Keywords:** digitalisation, information security, legal regulation, fuel and energy complex, cybersecurity risks, legislative measures, data protection.

### **References**

1. Federal Law of the Russian Federation No. 187-FZ 'On the Security of the Critical Information Infrastructure of the Russian Federation' dated 26.07.2017 (as amended on 01.03.2022).

2. Federal Law of the Russian Federation No. 152-FZ ‘On Personal Data’ dated 27.07.2006 (as amended on 01.03.2022).
3. Resolution of the Government of the Russian Federation No. 1119 dated 01.11.2012 ‘On Approval of the Rules of Personal Data Processing when Using Information Systems of Personal Data’ (as amended on 27.03.2021).
4. Ministry of Energy of the Russian Federation. Recommendations on ensuring cyber security in the fuel and energy complex. Moscow: Ministry of Energy of Russia, 2020.
5. Software Engineering Institute. OCTAVE Allegro Methodology: Improving the Information Security Risk Assessment Process / Software Engineering Institute. — Pittsburgh: Carnegie Mellon University, 2007. [Electronic resource]. Access mode: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8296>.
6. National Institute of Standards and Technology (NIST). Guide for Conducting Risk Assessments (NIST Special Publication 800-30) / National Institute of Standards and Technology (NIST). 2020. <https://doi.org/10.6028/NIST.SP.800-30r1>.
7. Kretova A.Y. Assessment of unsystematic risks and damage in the oil and gas complex / A. Y. Kretova // Discussion. 2024. № 6 (127). Pp. 97-102. DOI 10.46320/2077-7639-2024-6-127-97-102. – EDN AIEVRP.
8. Scriabin A.V. Legal regulation of relations in the field of oil and gas production: identification of problematic aspects / A.V. Scriabin // Eurasian Law Journal. 2024. № 6 (193). Pp. 296-298. EDN CXIHNN.