Article

УДК: 341

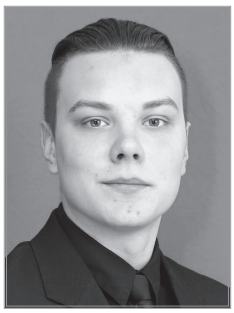
ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОГО КОМПЛЕКСА РОССИИ В КОНТЕКСТЕ РЕАЛИЗАЦИИ ЭНЕРГЕТИЧЕСКОЙ СТРАТЕГИИ ДО 2050 ГОДА

Сергей Лобанов*

Азиза Назарова**

Андрей Найденов***

DOI 10.24833/2073-8420-2025-2-75-26-34



Введение. *В статье рассматривается проблема кибербезопасности топливно-энергетического комплекса (ТЭК) России в условиях цифровой трансформации отрасли, обозначенной в Энергетической стратегии РФ до 2050 года. Обоснована актуальность темы в связи с ростом числа кибератак на критическую инфраструктуру и недостаточностью существующих нормативных механизмов.*

Материалы и методы. *Методологическую основу составляют сравнительно-правовой анализ, формально-юридический и системный подходы, с опорой на документы стратегического планирования РФ и международные нормативные акты (США, ЕС, КНР).*

Результаты исследования. *Выявлен пробел в российском законодательстве: отсутствие специального закона о кибербезопасности объектов ТЭК. Проанализированы положения действующих нормативных актов, установлено их фрагментарное и отрасле-нейтральное применение. Приведён анализ зарубежных моделей - NERC CIP (США), директивы NIS 2 (ЕС) и законодательства КНР.*

* **Лобанов Сергей Александрович**, доктор юридических наук, доцент, заведующий кафедрой правового регулирования ТЭК МГИМО МИД России, Москва, Россия
e-mail: lobanov-sa.lobanov@yandex.ru
ORCID ID: 0000-0001-9685-8172

** **Назарова Азиза Улугбековна**, кандидат юридических наук, старший преподаватель кафедры правового регулирования ТЭК МГИМО МИД России, Москва, Россия
e-mail: nazarazizaa@gmail.com
ORCID ID: 0000-0003-3136-1143

*** **Найденов Андрей Андреевич**, магистрант МГИМО МИД России, Москва, Россия
e-mail: a_naidenov21@mail.ru
ORCID ID: 0009-0001-8865-6834

Обсуждение и заключение. *Предложена концепция специального федерального закона о кибербезопасности объектов ТЭК, основанная на принципах превентивности, устойчивости, ответственности и отраслевой специфики. Сделан вывод о необходимости скорейшей законодательной регламентации в целях обеспечения энергетической безопасности России.*

Введение

Цифровая трансформация топливно-энергетического комплекса (ТЭК) приносит отрасли несомненные преимущества, повышая эффективность управления и мониторинга. Вместе с тем растущая зависимость энергетической инфраструктуры от информационных технологий порождает новые киберугрозы, способные нанести ущерб энергетической безопасности государства. Энергетическая стратегия Российской Федерации на период до 2050 года (утв. распоряжением Правительства РФ от 12 апреля 2025 г. № 908-р) прямо указывает на необходимость достижения "цифровой зрелости" процессов в энергетике при одновременном обеспечении управляемости и безопасности объектов критической информационной инфраструктуры (КИИ) в сферах энергетики[1].

Исследование

Цифровизация ТЭК и новые киберугрозы

Активное внедрение цифровых технологий в ТЭК сопровождается появлением новых угроз, на которые традиционные меры безопасности не всегда рассчитаны. Инфраструктура энергетики (электростанции, сети, нефтегазовые объекты, трубопроводы) становится мишенью не только физических диверсий, но и кибератак – злонамеренных воздействий через ИТ-системы управления. Отказ автоматизированных систем может привести к масштабным авариям, нарушению энергоснабжения регионов, экологическим катастрофам и экономическим потерям. Современные киберугрозы для энергетики включают: проникновение вредоносного ПО в системы промышленного управления (SCADA/АСУ ТП), ransomware-атаки (вымогательство с шифрованием данных), атаки на цепочки поставок ПО и оборудования, DDoS-атаки на сетевую инфраструктуру, а также целенаправленные действия, подкрепляемые ресурсами иностранных государств (так называемые APT-кампании).

Показателен кейс атаки на трубопроводную компанию **Colonial Pipeline** в США (май 2021 года). В результате заражения сетей компании вирусом-вымогателем DarkSide оператору пришлось превентивно отключить ключевые системы управления трубопроводом, что привело к полной остановке транспортировки топлива по крупнейшему магистральному трубопроводу США на пять дней. [2] Colonial Pipeline обеспечивает около 45% потребностей Восточного побережья США в топливе, поэтому кибератака вызвала локальный топливный кризис и вынудила власти ввести режим чрезвычайного положения. [3] Данный инцидент, крупнейший для нефтегазовой инфраструктуры США, продемонстрировал, что уязвимости информационных систем критических объектов ТЭК непосредственно угрожают экономике и безопасности общества. Другой пример – атаки на саудовские нефтехимические объекты с применением вредоноса Triton (2017) и т.д. – подтверждает глобальный характер проблемы.

В условиях цифровизации отечественного ТЭК подобные риски актуальны и для России. Доктрина энергетической безопасности РФ 2019 года относит к числу основных вызовов низкий уровень защищенности

[1] Распоряжение Правительства РФ от 12 апр. 2025 г. № 908-р // Офиц. интернет-портал правовой информации. 2025. 14 апр. № 0001202504140013. URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=0001202504140013 (дата обращения: 16.04.2025).

объектов ТЭК от актов незаконного вмешательства[2], к которым в современных реалиях следует отнести и компьютерные атаки. Ущерб от реализации киберугроз в энергетике потенциально выражается в нарушении надежного энергоснабжения потребителей, срыве экспортных контрактов, подрыве экономической стабильности и технологического суверенитета страны. Таким образом, защита критически важных объектов топливно-энергетического комплекса от кибератак выступает неотъемлемой частью понятия энергетической безопасности и требует адекватного правового обеспечения.

В рамках Энергетической стратегии РФ до 2050 года, утверждённой Распоряжением Правительства № 908-р от 12.04.2025, одним из ключевых направлений развития топливно-энергетического комплекса (ТЭК) названо внедрение цифровых технологий, включая искусственный интеллект, автоматизацию, а также развитие сквозных цифровых решений[3]. Стратегия предусматривает реализацию не менее 36 особо значимых проектов импортозамещения в цифровой сфере (2022–2023 гг.), а также этапную цифровую трансформацию с достижением технологического лидерства к 2050 году. Однако, при всей масштабности цифровизации, в стратегии отсутствует упоминание механизмов кибербезопасности, что подтверждает необходимость разработки специального федерального закона, устраняющего данный пробел.

Нормативно-правовая база РФ в сфере кибербезопасности объектов ТЭК

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646)[4] задаёт общую стратегическую рамку обеспечения национальной безопасности в информационной сфере. В ней подчёркивается приоритет защиты критически важных информационных инфраструктур (КИИ) и необходимость совершенствования законодательства для предотвращения компьютерных атак на объекты экономики. Однако сама по себе Доктрина носит доктринально-программный, а не нормативно-обязывающий характер и не содержит отраслевой детализации применительно к топливно-энергетическому комплексу.

Аналогичным статусом обладает Доктрина энергетической безопасности Российской Федерации (утв. Указом Президента РФ от 13 мая 2019 г. № 216)[5], выступающая ключевым документом стратегического планирования в сфере ТЭК. В ней энергетическая безопасность определяется как состояние защищённости экономики и населения от угроз в сфере энергетики, при котором обеспечивается удовлетворение внутреннего спроса и выполнение экспортных обязательств. В числе угроз зафиксированы технологические риски, включая отставание в разработке и внедрении современных средств защиты, а также недостаточная защищённость объектов ТЭК от незаконного вмешательства. Хотя кибератаки прямо не упомянуты, их правовая природа как разновидности информационно-коммуникационных угроз очевидна в современном контексте.

Отдельного внимания заслуживает Энергетическая стратегия Российской Федерации на период до 2050 года (утв. распоряжением Правительства РФ от 12 апреля 2025 г. № 908-р)[6], в которой цифровизация отрасли, внедрение ИИ и автоматизированных систем управления признаны одними из ключевых векторов развития ТЭК. Документ ориентирован на достижение технологического лидерства к 2050 году и подчёркивает приоритет формирования устойчивой, надёжной и управляемой энергосистемы.

---

[2] См. п. 20, д) Доктрины энергетической безопасности Российской Федерации, утв. Указом Президента РФ от 13 мая 2019 г. № 216. // Собрание законодательства Российской Федерации. 2019. № 20. Ст. 242.

[3] Энергетическая стратегия Российской Федерации на период до 2050 года : утв. распоряжением Правительства РФ от 12 апр. 2025 г. № 908-р. – М., 2025. – 107 с. – С. 12, 15, 61–62.

[4] Указ Президента РФ от 5 дек. 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074

[5] Указ Президента Российской Федерации от 13 мая 2019 г. № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 20. Ст. 2421

[6] Распоряжение Правительства Российской Федерации от 12 апр. 2025 г. № 908-р «Об утверждении Энергетической стратегии Российской Федерации на период до 2050 года» // Офиц. интернет-портал правовой информации. 2025. 14 апр. № 0001202504140013. URL: https://pravo.gov.ru/proxy/ips/?docbody=&nd=0001202504140013 (дата обращения: 16.04.2025)

Однако, несмотря на амбициозные цели цифровой трансформации, Стратегия не содержит нормативных механизмов обеспечения кибербезопасности энергетических объектов.

Таким образом, все три упомянутых документа: Доктрина информационной безопасности, Доктрина энергетической безопасности и Энергостратегия-2050 - формируют стратегическую нормативно-политическую основу, однако не обладают прямым регулирующим действием. Они обозначают векторы и цели государственной политики, создавая политико-правовые предпосылки для последующего нормативного закрепления соответствующих институтов в специализированных законах и подзаконных актах. Отсутствие такого закрепления на сегодняшний день и составляет один из ключевых вызовов правовому обеспечению кибербезопасности объектов ТЭК.

В настоящее время нормативно-правовая база кибербезопасности критически важных объектов в РФ включает ряд федеральных законов и подзаконных актов общего и отраслевого характера. Базовым является Федеральный закон от 26.07.2017 г. № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"[7]. Он впервые в российском праве ввел понятие критической информационной инфраструктуры и установил обязанности ее субъектов по обеспечению безопасности значимых объектов КИИ. К объектам КИИ, согласно закону, отнесены информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления в ряде жизненно важных сфер, включая энергетику (также топливно-энергетический комплекс прямо назван в Постановлении Правительства РФ от 08.02.2018 г. № 127 в перечне отраслей КИИ[8]). Закон № 187-ФЗ обязывает владельцев значимых объектов КИИ создавать системы обеспечения безопасности таких объектов и поддерживать их функционирование[9].

В целом, 187-ФЗ заложил фундамент правового режима кибербезопасности критической инфраструктуры. Однако он носит отраслево-нейтральный характер и устанавливает единые требования для всех сфер (энергетика, транспорт, связь, финансы и т.д.), не учитывая специфику отдельных отраслей. Кроме того, ряд положений закона требует дальнейшей детализации на уровне подзаконных актов (стандарты безопасности, порядок категорирования и взаимодействия, ответственность и т.п.), что в полной мере еще не реализовано. Эти моменты можно отнести к правовым пробелам текущей системы.

Отдельно следует рассмотреть Федеральный закон от 21.07.2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»[10]. Кибербезопасность напрямую в тексте не упоминается. Тем не менее закон предписывает принятие требований обеспечения безопасности объектов ТЭК и говорит об информационном и научно-техническом обеспечении безопасности ТЭК[11]. В период с 2011 г. в закон вносились изменения, однако акцент по-прежнему сделан на предотвращении физических угроз (охрана периметра, контрольно-пропускные режимы, категорирование по урону при терактах и авариях). Таким образом, специализированный "отраслевой" закон о безопасности объектов ТЭК пока не интегрирует аспекты кибербезопасности.

Другие нормативные акты также затрагивают вопросы информационной безопасности в энергетике косвенно. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[12] устанавливает об-

[7] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собр. законодательства РФ. 2017. № 31 (ч. I). Ст. 4736

[8] Постановление Правительства Российской Федерации от 8 февр. 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации. 2018. № 8. Ст. 1204

[9] См. ст. 10, п. 1 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[10] Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» // Собр. законодательства РФ. 2011. № 30 (ч. I). Ст. 4604

[11] Там же, см. ст. 3.

[12] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собр. законодательства РФ. 2006. № 31 (ч. I). Ст. 3448;

щие принципы защиты информации и обязанность обладателей информационных систем принимать меры по предотвращению несанкционированного доступа. Он создает правовую базу для защиты любых информационных систем, включая системы предприятий ТЭК, однако носит рамочный характер. Федеральный закон от 03.12.2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»[13] создал Государственную информационную систему ТЭК (ГИС ТЭК) – централизованный банк данных о производстве, потреблении и передаче энергоресурсов. Хотя основной акцент Закона – информационное обеспечение отрасли, косвенно он поднимает вопросы безопасности собираемых данных и доступа к ним. Очевидно, что успешное функционирование ГИС ТЭК требует защиты от несанкционированного вмешательства, но специальных норм об этом в законе нет.

Итак, анализ действующего законодательства РФ выявляет ***правовой пробел:*** отсутствует специальный правовой акт, посвященный именно кибербезопасности объектов ТЭК. Имеющаяся система регулирования фрагментирована: один закон (187-ФЗ) охватывает только значимые объекты КИИ и не учитывает отраслевую специфику; другой (256-ФЗ) охватывает объекты ТЭК, но лишь в контексте физической безопасности; остальные акты дают лишь общие положения. Это затрудняет формирование целостного режима защиты именно для критически важных энергетических объектов – не всех ИТ-систем подряд, а ключевых элементов энергетической инфраструктуры (генерирующие мощности, сети, нефте- и газопроводы, хранилища и т.п.), от стабильной работы которых зависит энергетическая безопасность. Кроме того, отсутствуют закрепленные на уровне закона специальные механизмы обеспечения кибербезопасности в отрасли – такие как обязательная сертификация используемых на объектах ТЭК средств информационной безопасности, регулярные аудиты киберзащищенности компаний ТЭК независимыми органами, отраслевые центры мониторинга киберинцидентов и обмена информацией и т. п. Данные элементы пока реализуются лишь точечно и на основе подзаконных актов (например, приказы ФСТЭК по аттестации систем или регламенты взаимодействия с ГосСОПКА), либо вовсе остаются на уровне рекомендаций. С учетом растущих угроз цифровой эпохи, такое положение представляется недостаточным.

Международный опыт кибербезопасности энергетической инфраструктуры

США одними из первых столкнулись с проблемой защиты энергосистем от киберугроз и разработали обязательные отраслевые требования. В электроэнергетике действуют стандарты NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection), являющиеся частью национальной системы стандартов надёжности энергосети.

NERC CIP представляет собой комплекс требований кибербезопасности, охватывающих все ключевые аспекты: идентификация и категоризация критически важных киберсистем, управление политикой безопасности и доступом, обучение и проверка надёжности персонала, защита электронных периметров и др. [5]

Ключевая особенность американского подхода — обязательность и системная проверка: стандарты CIP фактически приравнены к законодательству и регулярно проверяются аудиторами. [6] Эта модель стала реакцией на масштабные отключения электроэнергии и рост киберугроз после 2001 года. Также важна роль отраслевых организаций: NERC была создана самими энергетическими компаниями под государственным контролем, что облегчает внедрение требований и обмен данными об инцидентах.

В ЕС кибербезопасность критической инфраструктуры регулируется директивой NIS 2 (Network and Information Security Directive 2) – обновлённой версией первой директивы 2016 года. Новый правовой акт (2022/2555 от 14 декабря 2022 г.) охватывает 18 критически важных секторов, включая энергетику (электроэнергия, нефть, газ, теплоснабжение)[14].

Государства ЕС обязаны разработать национальные стратегии, определить

[13] Федеральный закон от 3 дек. 2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» // Собр. законодательства РФ. 2011. № 49 (ч. V). Ст. 7060.

[14] NIS2 Directive [Электронный ресурс] // European Commission – Digital Strategy. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (дата обращения: 16.04.2025).

уполномоченные органы и наладить сотрудничество на общеевропейском уровне (обмен информацией, совместные группы реагирования). Компании, относящиеся к основным или важным операторам критической инфраструктуры, обязаны внедрять политики информационной безопасности, осуществлять контроль доступа, использовать криптографию и физическую защиту, регулярно проводить оценку уязвимостей, обеспечивать резервирование и планирование непрерывности, в течение 24 часов уведомлять национальные органы о значимых инцидентах и подавать финальный отчёт и др.

КНР выстроила жёсткую систему киберрегулирования, охватывающую в том числе энергетику. Базовый Закон о кибербезопасности (принят в 2016 г., вступил в силу 1 июня 2017 г.) устанавливает требования к защите сетей и информации, с особым вниманием к критически важной информационной инфраструктуре (КВИИ): энергетика, транспорт, финансы, госуправление и др.

Ключевые положения Закона касаются локализации данных – обязательное хранение внутри страны, вывоз — только с разрешения регулятора; контроля закупок – продукты и услуги в сфере информационной безопасности подлежат сертификации государством; и обязательных аудитов – не реже одного раза в год с передачей отчётов в надзорные органы [1. С. 153].

Модель дополняется принятыми в 2021 году Положением «О защите безопасности ключевой информационной инфраструктуры» и Законом «О безопасности данных», которые конкретизируют требования к операторам. Таким образом, Китай выстраивает централизованную вертикаль кибербезопасности, где государство координирует, проверяет и наказывает[15]. С одной стороны, это обеспечивает высокий уровень защиты, с другой – увеличивает издержки и ограничивает доступ к иностранным технологиям.

На фоне рассмотренного международного опыта становится очевидно, что Россия пока не имеет аналогичного целостного нормативного акта, посвященного кибербезопасности именно в сфере энергетики. Наличие правовых пробелов создает риски несогласованности действий и недостаточного уровня защиты. Можно выделить несколько ключевых аргументов в пользу разработки и принятия специального федерального закона о кибербезопасности объектов ТЭК.

Энергетика как стратегическая отрасль требует особого правового режима защиты. Объекты ТЭК — электростанции, сети, месторождения, трубопроводы - критически важны для экономики и жизнеобеспечения. Кибератаки на них способны вызвать серьёзные последствия для национальной безопасности. Поэтому необходима отраслевая спецификация норм, выходящая за рамки общего регулирования безопасности КИИ.

Современные угрозы размывают границы между физической и цифровой безопасностью. Закон № 256-ФЗ ориентирован на защиту от физических посягательств, но не охватывает ИТ-системы. Между тем кибератака может привести к реальному техногенному ущербу. Требуется единый подход к безопасности энергетических объектов как целостных технологических систем.

Энергостратегия-2050 и Доктрина энергетической безопасности фиксируют цели цифровизации и необходимость защиты КИИ. Однако их реализация невозможна без конкретных правовых механизмов. Специальный закон призван превратить стратегические установки в обязательные правовые нормы.

Такой закон станет основой для разработки подзаконных актов и технических стандартов. Он зафиксирует принципы регулирования, компетенции органов власти и обязанности субъектов, обеспечив нормативную базу для отраслевых требований к киберзащите.

Принятие закона повысит ответственность энергетических компаний и сформирует корпоративную культуру информационной безопасности. В нём могут быть предусмотрены обязательные системы ИБ, требования к квалификации персонала, механизмы аудита и санкции за нарушения.

Закон также обеспечит выполнение международных обязательств России в сфере кибербезопасности критической инфраструктуры и облегчит международное

[15] Закон КНР о безопасности данных (Data Security Law, 2021) [Электронный ресурс] // CNLegal.ru. URL: https://cnlegal.ru/china_economic_law/china_data_security_law_2021/ (дата обращения: 16.04.2025); Положение о безопасности критической информационной инфраструктуры КНР (2021) [Электронный ресурс] // CNLegal.ru. URL: https://cnlegal.ru/china_economic_law/critical_information_infrastructure_security_2021/ (дата обращения: 16.04.2025).

сотрудничество, в том числе в рамках совместных учений и обмена информацией об инцидентах.

Учитывая эти аргументы, разработка проекта федерального закона о кибербезопасности объектов ТЭК представляется своевременной и необходимой. Ниже предлагаются возможные принципы, механизмы и формы, которые целесообразно включить в такой закон, с опорой на выявленные лучшие практики.

Целью предлагаемого закона является формирование целостной правовой модели защиты критически важной энергетической инфраструктуры от кибератак в условиях цифровой трансформации отрасли. Такая модель должна обеспечивать устойчивость и безопасность функционирования топливно-энергетического комплекса, опираясь на стратегические ориентиры, закреплённые в Энергетической стратегии до 2050 года.

К основополагающим принципам предлагаемой правовой конструкции относятся превентивный подход, при котором безопасность закладывается на этапе проектирования цифровых систем, а также дифференциация мер защиты в зависимости от уровня критичности объектов. Немаловажную роль играют комплексность (объединение технических и организационных механизмов), персональная ответственность операторов, развитие государственно-частного партнёрства в сфере информационной безопасности, а также закрепление возможности преследования организаторов кибератак вне зависимости от их юрисдикции.

Проект закона должен охватывать объекты ТЭК, отнесённые к критической информационной инфраструктуре и особо значимым объектам отрасли, включая государственные информационные системы. Предполагается, что координацию в сфере кибербезопасности будет осуществлять Минэнерго России во взаимодействии с ФСТЭК, ФСБ и, при необходимости, Минцифры. В обязанности операторов объектов ТЭК предлагается включить внедрение сертифицированных систем защиты информации, категорирование ИТ-систем по уровню значимости, проведение независимых аудитов, разработку внутренней нормативной базы и организацию отраслевого мониторинга инцидентов. Органы регулирования должны получить право проведения проверок, выдачи предписаний и приостановки эксплуатации критически уязвимых систем, а также разрабатывать и актуализировать технические стандарты защиты.

Важным элементом нормативной конструкции являются меры юридической ответственности и стимулирования: для недобросовестных операторов – штрафные санкции, для соблюдающих требования – государственная поддержка и поощрение. Отдельный блок нового закона должен быть посвящён международному сотрудничеству в сфере противодействия киберугрозам, обмену информацией и участию в международных расследованиях. Такая правовая модель позволит устранить пробелы действующего законодательства и обеспечить необходимый уровень киберзащиты в стратегически важной отрасли.

Заключение

Цифровизация ТЭК, будучи одним из приоритетов Энергетической стратегии РФ до 2050 года, требует синхронного развития правовых механизмов защиты отрасли от киберугроз. Проведенный анализ показал, что несмотря на наличие в России базового законодательства о безопасности информации и критической инфраструктуры, в его применении к энергетическому сектору имеются пробелы. Международный опыт - от строгих стандартов NERC CIP в США до комплексного законодательства Китая и нормативов ЕС - демонстрирует необходимость специальных мер для обеспечения киберустойчивости энергетики. Российская правовая система энергетического права в силу объективных факторов пока отстает в этом вопросе, однако обладает потенциалом для быстрого развития, опираясь на уже заданные стратегические ориентиры и наработки других стран. Разработка и внедрение специального федерального закона о кибербезопасности объектов топливно-энергетического комплекса позволит устранить нормативные лакуны и создать условия для надежной защиты критически важной энергетической инфраструктуры. Предложенная в статье правовая модель предусматривает установление четких обязанностей для субъектов ТЭК, введение механизмов сертификации цифровых решений, обязательных аудитов информационной безопасности, мониторинга инцидентов и гибкой системы подзаконного регулирования. Данная модель отвечает требованиям времени и основана на сочетании лучших зарубежных практик с учетом российских реалий. Ее реализация обеспечит необходимый уровень защищенности отечественного ТЭК от киберпреступников, повысит устойчивость экономики и энергетическую

безопасность государства. Кроме того, это станет вкладом России в формирование международных стандартов кибербезопасности энергетики и укрепит авторитет страны как технологически суверенного и ответственного участника глобального энергетического сотрудничества.

Литература:

1. Балакин Д.А., Аликберова А.Р. Особенности Закона о кибербезопасности Китайской Народной Республики 2017 г. и международная реакция на его принятие // Modern Oriental Studies. 2023. № 2.
2. DarkChronicles: последствия атаки на Colonial Pipeline [Электронный ресурс] // Kaspersky ICS CERT. 2021. 21 мая. URL: https://ics-cert.kaspersky.ru.
3. Эксперт оценил влияние атаки на Colonial Pipeline на сферу киберпреступности [Электронный ресурс] // Известия. 2021. 24 мая. URL: https://iz.ru.
4. Positive Technologies: сегодня кибербезопасность ТЭК должна быть результативной // Neftegaz.RU. 2024. № 4 (148). URL: https://magazine.neftegaz.ru.
5. Что такое соответствие стандарту NERC CIP? // Continuum GRC. URL: https://continuumgrc.com.
6. Vijayshankar S., Chang C.-Y., Utkarsh K., Wald D., Ding F., Balamurugan S., King J., Macwan R. Assessing the Impact of Cybersecurity Attacks on Energy Systems // Applied Energy. 2023. Vol. 345. DOI: 10.1016/j.apenergy.2023.121297.
7. Dong S., Cao J., Flynn D., Fan Z. Cybersecurity in Smart Local Energy Systems: Requirements, Challenges, and Standards // Energy Informatics. 2022. Vol. 5. Article 9. DOI: 10.1186/s42162-022-00195-7.
8. Zografopoulos I., Ospina J., Liu X., Konstantinou C. Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies // Computers & Security. 2021. Vol. 105. DOI: 10.1016/j.cose.2021.102221.
9. Mashima D., Chen Y., Roomi M.M., Lakshminarayana S., Chen D. Cybersecurity for Modern Smart Grid Against Emerging Threats // Electric Power Systems Research. 2024. Vol. 229. DOI: 10.1016/j.epsr.2023.109964.

LEGAL SUPPORT FOR CYBERSECURITY IN THE RUSSIAN FUEL AND ENERGY SECTOR IN THE CONTEXT OF THE ENERGY STRATEGY UNTIL 2050

Introduction. *The article addresses the issue of cybersecurity in Russia's fuel and energy sector (FES) in the context of digital transformation, as outlined in the Russian Energy Strategy until 2050. The relevance of the topic is substantiated by the growing number of cyberattacks targeting critical infrastructure and the inadequacy of existing legal instruments.*

Materials and methods. *The research methodology includes comparative legal analysis, formal legal methods, and systemic approaches, drawing upon Russian strategic planning documents and international legal frameworks (USA, EU, China).*

Results of the study. *The study identifies a legislative gap in the absence of a dedicated federal law on cybersecurity in the FES. The analysis of existing Russian laws shows that current regulations are fragmented and sector-neutral. Foreign models – NERC CIP (USA), NIS 2 Directive (EU), and Chinese cybersecurity legislation – are examined in detail.*

Discussion and conclusion. *The authors propose a conceptual framework for a federal law on cybersecurity in the FES, based on the principles of prevention, resilience, accountability, and sectoral specificity. The need for prompt legislative action is emphasized as a strategic priority for Russia's energy security.*

Sergey A. Lobanov,
Doctor of Sciences (Law),
Associate Professor, Head of the Department of Legal Regulation of the Fuel and Energy Industry, MGIMO University,
Moscow, Russia

Aziza U. Nazarova,
Candidate of Sciences (Law), Senior Lecturer, the Department of Legal Regulation of the Fuel and Energy Industry, MGIMO University,
Moscow, Russia

Andrey A. Naydenov,
Master's student, MGIMO University,
Moscow, Russia

Ключевые слова:
кибербезопасность, энергетическая стратегия, топливно-энергетический комплекс, критическая инфраструктура, цифровизация, правовое регулирование, энергетическая безопасность, стандарты безопасности, стратегическое планирование.

Keywords:
cybersecurity, energy strategy, fuel and energy sector, critical infrastructure, digitalization, legal regulation, energy security, security standards, strategic planning.

References:

1. Balakin, D.A., Alikberova, A.R., 2023. Osobennosti zakona o kiberbezopasnosti Kitajskoy Narodnoy Respubliki 2017 g. i mezhdunarodnaya reaktsiya na ego prinyatie [Features of the Cybersecurity Law of the People's Republic of China (2017) and the international reaction to its adoption]. *Modern Oriental Studies.* № 2.
2. Kaspersky ICS CERT, 2021. DarkChronicles: posledstviya ataki na Colonial Pipeline [DarkChronicles: consequences of the attack on Colonial Pipeline]. 21 May. URL: https://ics-cert.kaspersky.ru.
3. Ekspert otsenil vliyanie ataki na Colonial Pipeline na sferu kiberprestupnosti [Expert assessed the impact of the Colonial Pipeline attack on the cybercrime sphere]. *Izvestiya [News].* 2021. 24 May. URL: https://iz.ru.
4. Positive Technologies: segodnya kiberbezopasnost' TEK dolzhna byt' rezul'tativnoy [Today, cybersecurity in the fuel and energy sector must be effective]. *Neftegaz.RU.* 2024.No. 4 (148). URL: https://magazine.neftegaz.ru.
5. Chto takoe sootvetstvie standartu NERC CIP? [What is NERC CIP compliance?]. *Continuum GRC.* 2022. URL: https://continuumgrc.com.
6. Vijayshankar, S., Chang, C.-Y., Utkarsh, K., Wald, D., Ding, F., Balamurugan, S., King, J., Macwan, R., 2023. Assessing the impact of cybersecurity attacks on energy systems. *Applied Energy.* Vol. 345. DOI: 10.1016/j.apenergy.2023.121297.
7. Dong, S., Cao, J., Flynn, D., Fan, Z., 2022. Cybersecurity in smart local energy systems: requirements, challenges, and standards. *Energy Informatics.* Vol. 5. Article 9. DOI: 10.1186/s42162-022-00195-7.
8. Zografopoulos, I., Ospina, J., Liu, X., Konstantinou, C., 2021. Cyber-physical energy systems security: threat modeling, risk assessment, resources, metrics, and case studies. *Computers & Security.* Vol. 105. DOI: 10.1016/j.cose.2021.102221.
9. Mashima, D., Chen, Y., Roomi, M.M., Lakshminarayana, S., Chen, D., 2024. Cybersecurity for modern smart grid against emerging threats. *Electric Power Systems Research.* Vol. 229. DOI: 10.1016/j.epsr.2023.109964.