

Дата поступления рукописи в редакцию: 18.11.2025 г.
Дата принятия рукописи к печати: 03.12.2025

DOI: 10.24412/3034-4395-2025-4-68-73

СПИРИДОНОВ Вячеслав Валентинович,
*студент ФГАОУ ВО «Санкт-Петербургский политехнический
университет Петра Великого»
г. Санкт-Петербург, Россия
e-mail: info@law-books.ru*

ПРАВОВЫЕ ВЫЗОВЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ЭЛЕКТРОЭНЕРГЕТИКИ: «УМНЫЕ» СЕТИ, КИБЕРБЕЗОПАСНОСТЬ И ДАННЫЕ

Аннотация. В статье анализируются ключевые правовые вызовы, возникающие в процессе цифровой трансформации электроэнергетики России. Рассматриваются вопросы правового регулирования «умных» сетей (Smart Grid), обеспечения кибербезопасности критической информационной инфраструктуры и обращения с данными, генерируемыми интеллектуальными системами учета. Выявляются пробелы и коллизии в действующем законодательстве, предлагаются направления для его совершенствования.

Ключевые слова: цифровая трансформация, электроэнергетика, «умные» сети, кибербезопасность, критическая информационная инфраструктура, большие данные, интеллектуальные системы учета, правовое регулирование.

SPIRIDONOV Vyacheslav Valentinovich,
*student of the Federal State Autonomous
Educational Institution of Higher Education
«Peter the Great St. Petersburg Polytechnic University»
St. Petersburg, Russia*

LEGAL CHALLENGES OF THE DIGITAL TRANSFORMATION OF THE ELECTRIC POWER INDUSTRY: SMART GRIDS, CYBERSECURITY, AND DATA

Annotation. The article analyzes the key legal challenges arising from the digital transformation of the Russian electric power industry. The issues of legal regulation of Smart Grids, ensuring the cybersecurity of critical information infrastructure, and the handling of data generated by intelligent metering systems are considered. Gaps and conflicts in the current legislation are identified, and directions for its improvement are proposed.

Key words: digital transformation, electric power industry, smart grids, cybersecurity, critical information infrastructure, big data, intelligent metering systems, legal regulation.

Цифровая трансформация электроэнергетики фундаментально меняет ее архитектуру, трансформируя традиционную централизованную систему в распределенную, интерактивную и интеллектуальную среду, известную как «умная» сеть (Smart Grid). В российской правовой системе отсутствует прямое законодательное определение понятия «умная» сеть.

Однако его сущность раскрывается через цели и задачи, закреплённые в стратегических документах, и опосредованно – через регулирование интеллектуальных систем учета.

Ключевым документом, задающим вектор развития, является Распоряжение Правительства РФ от 09.06.2020 № 1523-р «Об утверждении Концепции развития интеллектуальной

энергетической системы Российской Федерации» [1]. Концепция определяет интеллектуальную энергетическую систему (ИЭС) как комплекс технологических, управленческих и информационных решений, обеспечивающих эффективное функционирование электроэнергетики за счет автоматизированного управления и двустороннего обмена информацией между всеми ее участниками. По мнению А.В. Лагутиной, отсутствие легальной дефиниции «умных» сетей создает правовую неопределенность при применении к ним существующих норм, предназначенных для традиционной энергетики [2].

Функционально ядро «умной» сети составляют интеллектуальные системы учета, правовые основы внедрения которых установлены Федеральным законом от 27.12.2018 № 522-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с развитием систем учета электрической энергии (мощности)» [3]. Данный закон возложил на гарантирующих поставщиков и сетевые организации обязанность по оснащению точек поставки интеллектуальными приборами учета (ИПУ). С точки зрения С.М. Зыкова, Закон № 522-ФЗ стал катализатором цифровизации, но породил и новые вызовы, в частности, в области защиты прав потребителей и определения ответственности за работоспособность и данные ИПУ [4].

Важным аспектом является вопрос ответственности на данные и технологическую инфраструктуру. Интеллектуальный прибор учета, как правило, устанавливается на стороне потребителя, но принадлежит и обслуживается сетевой организацией или гарантирующим поставщиком. Это порождает сложную правовую конструкцию. Гражданский кодекс РФ (часть первая) от 30.11.1994 № 51-ФЗ [5] не содержит специальных норм, регулирующих отношения, возникающие в связи с установкой оборудования одной стороной на объекте другой стороны для целей исполнения договора. На практике это регулируется договорами энергоснабжения и оказания услуг по передаче электроэнергии. Однако, как справедливо отмечает Е.И. Афанасьева, в этих договорах зачастую не прописаны детальные условия об использовании данных, получаемых с ИПУ, что создает риски для обеих сторон [6].

Таким образом, первым правовым вызовом является формирование целостного понятийного аппарата и адекватного правового режима для «умных» сетей, который бы учитывал их распределенный, интерактивный и технологически сложный характер, выходящий за рамки классического энергетического законодательства.

«Умные» сети, будучи киберфизическими системами, уязвимы для компьютерных атак, последствия которых могут быть сопоставимы с физическими диверсиями. Электроэнергетика в Российской Федерации отнесена к сфере критической информационной инфраструктуры (КИИ) в соответствии с Указом Президента РФ от 17.03.2021 № 140 «Об утверждении Перечня объектов критической информационной инфраструктуры Российской Федерации» [7]. Следовательно, ее правовой режим в области безопасности определяется Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [8].

Закон № 187-ФЗ возлагает на субъектов КИИ (к которым относятся сетевые и генерирующие компании) ряд обязательств, включая:

- Категорирование объектов КИИ.
- Проведение оценки рисков и прогнозирование угроз.
- Установление особых требований к средствам защиты информации.
- Обеспечение непрерывности функционирования путем создания систем безопасности и инцидент-менеджмента.
- Предоставление в Федеральную службу по техническому и экспортному контролю (ФСТЭК России) информацию об инцидентах.

По мнению В.А. Минаева, несмотря на комплексный характер Закона № 187-ФЗ, его практическая реализация в электроэнергетике сталкивается с трудностями, связанными с высокой стоимостью внедрения средств защиты, нехваткой квалифицированных кадров и постоянной эволюцией киберугроз [9]. Особую сложность представляет интеграция устаревших промышленных систем (АСУ ТП), которые не были рассчитаны на современные киберугрозы, в новую парадигму безопасности.

Коллизия возникает на стыке законодательства о КИИ и энергетического законодательства. Например, Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике» [10] обязывает субъекты отрасли обеспечивать надежность и безопасность энергосистемы. Однако он не детализирует кибернетические аспекты этой безопасности. В результате, как указывает К.Р. Петросян, требования к физической и кибернетической безопасности могут разрабатываться и контролироваться разными ведомствами (Ростехнадзор, ФСТЭК, ФСБ), что создает риск возникновения противоречивых предписаний [11].

Еще одним вызовом является вопрос ответственности за кибератаки. В случае успешной атаки на объект КИИ, приведшей к веерным отключениям, сложно определить виновное лицо в рамках действующего административного и уголовного права. Кодекс РФ об административных правонарушениях и Уголовный кодекс РФ содержат составы правонарушений, связанных с неправомерным доступом к компьютерной информации (ст. 13.12 КоАП РФ [12], ст. 272 УК РФ [13]), но они не в полной мере учитывают специфику последствий для объектов жизнеобеспечения.

Следовательно, вторым ключевым вызовом является необходимость дальнейшей гармонизации законодательства о КИИ с отраслевым энергетическим законодательством, развития механизмов публично-частного партнерства в области кибербезопасности и совершенствования мер ответственности за кибератаки на объекты энергетики.

Цифровая трансформация порождает огромные массивы данных (Big Data), которые становятся новым стратегическим активом. В контексте «умных» сетей можно выделить несколько типов данных:

1. Данные интеллектуального учета (потребление, генерация, профили нагрузки).
2. Телеметрические данные с оборудования сетей (трансформаторов, выключателей).
3. Данные о состоянии рынка и режимах работы энергосистемы.

Правовой режим этих данных формируется под воздействием нескольких отраслей законодательства.

Во-первых, законодательство о персональных данных. Данные о потреблении электро-

энергии, особенно с высокой детализацией (например, с интервалом в 30 минут или менее), позволяют де-анонимизировать потребителя и получить о нем информацию: режим дня, использование специфических электроприборов, факт присутствия или отсутствия в жилище. Таким образом, они являются персональными данными в смысле Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [14]. Субъекты КИИ, обрабатывающие такие данные, обязаны соблюдать все требования Закона: получать согласие субъекта, обеспечивать конфиденциальность и безопасность, уведомлять Роскомнадзор и т.д. А.Б. Наумов и С.В. Куракин отмечают, что получение действительного информированного согласия на обработку данных с ИПУ является нетривиальной задачей, так как потребитель зачастую не осознает объем собираемой о нем информации [15].

Во-вторых, законодательство о коммерческой тайне. Для сетевых и сбытовых компаний данные об объемах перетока и потребления, а также о режимах работы сети могут составлять коммерческую тайну (Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [16]). Однако здесь возникает конфликт интересов. С одной стороны, компания заинтересована в защите этих данных. С другой стороны, в условиях «умной» сети для обеспечения эффективного функционирования системы эти данные должны в определенном объеме и формате предоставляться системному оператору, участникам оптового и розничного рынков. Правовые рамки такого обмена на сегодняшний день определены недостаточно четко.

В-третьих, вопросы права собственности на данные. Гражданское законодательство РФ не знает понятия «право собственности на данные». Данные рассматриваются как объект гражданских прав – информация (ст. 128 ГК РФ). Создаваемые интеллектуальными приборами учета данные являются производными от процесса потребления услуги. Кто является их «создателем» и правообладателем? Потребитель, чье поведение генерирует данные? Сетевая компания, чье оборудование их фиксирует и передает? Гарантирующий поставщик, который обязан их собирать в силу закона? Доктринальных и судебных от-

ветов на эти вопросы пока нет. По мнению Д.В. Петрова, разрешить этот тупик могло бы введение конструкции «производных данных» и закрепление в законе презумпции, что данные, созданные в процессе исполнения публично-правовой обязанности (как в случае с ИПУ), являются общедоступными, за исключением той части, что относится к персональным данным [17].

В-четвертых, регулирование обмена данными. Для реализации потенциала «умных» сетей необходим свободный, но регламентированный обмен данными между всеми участниками: генерацией, сетевыми компаниями, системным оператором, поставщиками и потребителями. В настоящее время такой обмен регламентирован фрагментарно – отдельными правилами оптового и розничных рынков, утверждаемыми Правительством РФ. Требуется создание комплексной нормативной базы, определяющей форматы, протоколы, сроки и условия доступа к различным типам данных в электроэнергетике, по аналогии с европейской директивой о внутреннем рынке электроэнергии (Directive (EU) 2019/944).

Таким образом, третий правовой вызов заключается в формировании сбалансированного правового режима данных, который, с одной стороны, защищал бы права потребителей (включая право на неприкосновенность частной жизни), а с другой – обеспечивал бы свободный поток информации, необходимый для эффективного и надежного функционирования цифровой энергосистемы.

Для преодоления обозначенных правовых вызовов целесообразно рассмотреть следующие меры:

1. Разработка и принятие специального федерального закона (или масштабная поправка в ФЗ «Об электроэнергетике»), который бы укрепил понятийный аппарат «умных» сетей, принципы их функционирования, права и обязанности всех участников, включая потребителей-просьюмеров.

2. Углубление гармонизации законодательства о КИИ и энергетического законодательства. Возможно, создание единого подзаконного акта (например, постановления Правительства РФ), который бы устанавливал комплексные требования к безопасности для объектов электроэнергетики, объединяющие кибернетические и физические аспекты.

3. Создание детализированного правового режима для данных ИПУ. Необходимо четко разграничить персональные и неперсональные данные, установить исчерпывающий перечень целей, для которых данные могут использоваться без дополнительного согласия потребителя (биллинг, управление режимами сети), и ввести упрощенные процедуры получения согласия для иных целей (сервисы энергосбережения).

4. Стимулирование разработки и внедрения стандартов и протоколов для обеспечения интероперабельности (совместимости) устройств и систем от разных производителей, что является основой для создания конкурентной экосистемы «умной» энергетики.

5. Развитие саморегулирования. Следует поощрять создание отраслевых стандартов и кодексов поведения, регулирующих обмен данными и обеспечение кибербезопасности, что позволит гибко реагировать на быстрое технологическое развитие.

Список литературы:

- [1] Распоряжение Правительства РФ от 09.06.2020 № 1523-р «Об утверждении Концепции развития интеллектуальной энергетической системы Российской Федерации» // *Собрание законодательства РФ*. – 2020. – № 24. – Ст. 3940.
- [2] Лагутина А. В. Правовые проблемы внедрения технологий «умных сетей» (Smart Grid) в электроэнергетике России / А. В. Лагутина // *Энергетическое право*. – 2021. – № 2. – С. 44–49.
- [3] Федеральный закон от 27.12.2018 № 522-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с развитием систем учета электрической энергии (мощности)» // *Собрание законодательства РФ*. – 2018. – № 53 (часть I). – Ст. 8456.
- [4] Зыков С. М. Правовые аспекты внедрения интеллектуальных систем учета электроэнергии: вызовы и перспективы / С. М. Зыков // *Журнал российского права*. – 2020. – № 5. – С.

[5] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

[6] Афанасьева Е. И. Договорные отношения в сфере интеллектуального учета электроэнергии: проблемы и решения / Е. И. Афанасьева // Хозяйство и право. – 2022. – № 4. – С. 110–118.

[7] Указ Президента РФ от 17.03.2021 № 140 «Об утверждении Перечня объектов критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2021. – № 12. – Ст. 1975.

[8] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. – 2017. – № 31 (часть I). – Ст. 4736.

[9] Минаев В. А. Кибербезопасность объектов критической информационной инфраструктуры топливно-энергетического комплекса: правовые аспекты / В. А. Минаев // Право и безопасность. – 2022. – № 3. – С. 75–82.

[10] Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике» // Собрание законодательства РФ. – 2003. – № 13. – Ст. 1177.

[11] Петросян К. Р. Правовое обеспечение кибербезопасности в электроэнергетике: коллизии и пробелы законодательства / К. Р. Петросян // Вестник университета имени О.Е. Куцафина (МГЮА). – 2021. – № 10. – С. 20–28.

[12] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 1.

[13] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.

[14] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3451.

[15] Наумов А. Б. Персональные данные в интеллектуальных системах учета электроэнергии: проблемы правовой квалификации и защиты / А. Б. Наумов, С. В. Куракин // Информационное право. – 2020. – № 4. – С. 88–94.

[16] Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // Собрание законодательства РФ. – 2004. – № 32. – Ст. 3283.

[17] Петров Д. В. Big Data в энергетике: поиск правового режима / Д. В. Петров // Закон. – 2023. – № 1. – С. 130–140.

Spisok literatury:

[1] Rasporiazhenie Pravitel'stva RF ot 09.06.2020 № 1523-r «Ob utverzhdenii Kontseptsii razvitiia intellektual'noi energeticheskoi sistemy Rossiiskoi Federatsii» // Sobranie zakonodatel'stva RF. – 2020. – № 24. – St. 3940.

[2] Lagutina A. V. Pravovye problemy vnedreniia tekhnologii «umnykh setei» (Smart Grid) v elektroenergetike Rossii / A. V. Lagutina // Energeticheskoe pravo. – 2021. – № 2. – S. 44–49.

[3] Federal'nyi zakon ot 27.12.2018 № 522-FZ «O vnosenii izmenenii v ot del'nye zakonodatel'nye akty Rossiiskoi Federatsii v sviazi s razvitiem sistem ucheta elektricheskoi energii (moshchnosti)» // Sobranie zakonodatel'stva RF. – 2018. – № 53 (chast' I). – St. 8456.

[4] Zykov S. M. Pravovye aspekty vnedreniia intellektual'nykh sistem ucheta elektroenergii: vyzovy i perspektivy / S. M. Zykov // Zhurnal rossiiskogo prava. – 2020. – № 5. – S. 112–125.

[5] Grazhdanskii kodeks Rossiiskoi Federatsii (chast' pervaiia) ot 30.11.1994 № 51-FZ // Sobranie zakonodatel'stva RF. – 1994. – № 32. – St. 3301.

[6] Afanas'eva E. I. Dogovornye otnosheniia v sfere intellektual'nogo ucheta elektroenergii: problemy i resheniia / E. I. Afanas'eva // Khoziaistvo i pravo. – 2022. – № 4. – S. 110–118.

[7] Ukaz Prezidenta RF ot 17.03.2021 № 140 «Ob utverzhdenii Perechnia ob»ektov kriticheskoi

информационной инфраструктуры Российской Федерации» // *Собрание законодательства РФ*. – 2021. – № 12. – Ст. 1975.

[8] *Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»* // *Собрание законодательства РФ*. – 2017. – № 31 (часть I). – Ст. 4736.

[9] *Минаев В. А. Киберабезопасность объектов критической информационной инфраструктуры топливно-энергетического комплекса: правовые аспекты* / В. А. Минаев // *Право и безопасность*. – 2022. – № 3. – С. 75–82.

[10] *Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике»* // *Собрание законодательства РФ*. – 2003. – № 13. – Ст. 1177.

[11] *Петросян К. Р. Правовое обеспечение кибербезопасности в электроэнергетике: коллизии и проблемы законодательства* / К. Р. Петросян // *Вестник университета имени О.Е. Кутафина (МГЮА)*. – 2021. – № 10. – С. 20–28.

[12] *Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ* // *Собрание законодательства РФ*. – 2002. – № 1 (часть I). – Ст. 1.

[13] *Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ* // *Собрание законодательства РФ*. – 1996. – № 25. – Ст. 2954.

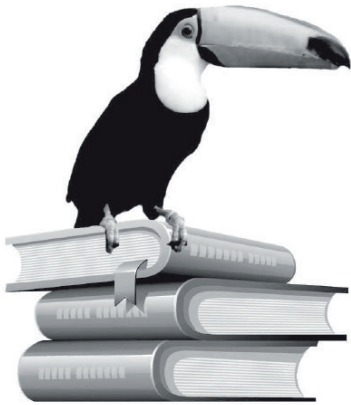
[14] *Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»* // *Собрание законодательства РФ*. – 2006. – № 31 (часть I). – Ст. 3451.

[15] *Наумов А. В. Персональные данные в интеллектуальных системах учета электроэнергии: проблемы правовой квалификации и защиты* / А. В. Наумов, С. В. Курakin // *Информационное право*. – 2020. – № 4. – С. 88–94.

[16] *Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»* // *Собрание законодательства РФ*. – 2004. – № 32. – Ст. 3283.

[17] *Петров Д. В. Big Data в энергетике: поиск правового режима* / Д. В. Петров // *Закон*. – 2023. – № 1. – С. 130–140.





ЮРКОМПАНИ

www.law-books.ru

Юридическое издательство
«ЮРКОМПАНИ»

Издание учебников,
учебных и методических
пособий, монографий,
научных статей.

Профессионально.

В максимально
короткие сроки.

Размещаем
в РИНЦ, Е-Library.