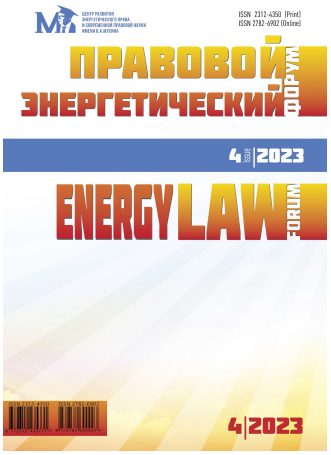

Правовой энергетический форум 2013-2024

ISSN 2079-8784

URL - http://ras.jes.su

Выпуск № 4 Том . 2023

Правовые проблемы обеспечения информационной (кибер-) безопасности энергетического сектора в условиях цифровизации

Вашечкина Анастасия Валерьевна
Специалист 2-й категории отдела экономической безопасности службы корпоративной защиты ООО "Газпром трансгаз Югорск", ООО "Газпром трансгаз Югорск"
Российская Федерация, Югорск

Аннотация

Цель данной работы — исследование проблем правового обеспечения информационной (кибер-) безопасности в энергетическом секторе, что позволяет сделать попытку выявления ключевых направлений дальнейшего развития правового регулирования, в том числе на законодательном уровне. Модернизация такого правого института, как информационная безопасность, является необходимой и приоритетной, особенно принимая во внимание внешнеполитические условия. Надлежащее соблюдение и охрана объектов информационной безопасности — основа государственной, экономической и социальной стабильности. В статье делается вывод о необходимости построения системы надлежащей сертификации программных продуктов, используемых в сфере ТЭК, создания государственно-частных посреднических институтов, регулирующих вопросы информационной безопасности в сфере ТЭК, современной нормативно-правовой базы в сфере регулирования информационной безопасности энергетических объектов, обращается внимание на категорирование объектов критической информационной инфраструктуры.

Ключевые слова: энергетическая безопасность, энергетическое право, энергетический правопорядок, кибербезопасность

Дата публикации: 24.01.2024

Ссылка для цитирования:

Вашечкина А. В. Правовые проблемы обеспечения информационной (кибер-) безопасности энергетического сектора в условиях цифровизации // Правовой энергетический форум – 2023. – Выпуск № 4 С. 90-97 [Электронный ресурс]. URL: https://mlcjournal.ru/S231243500029322-2-1 (дата обращения: 03.07.2024). DOI: 10.61525/S231243500029322-2

1 Энергетический сектор неустанно занимал лидирующие позиции в вопросах внедрения новых технологий, способствовавших повышению эффективности производственного процесса и производительности труда.

2 В настоящее время возникла необходимость внедрения и распространения цифровых начал, создания интеллектуальных компьютерных сетей, сопровождающих весь цикл производства.

3 Например, добыча нефти или газа все больше связана с удаленными месторождениями, находящимися в «экстремальных климатических условиях», или с «труднодобываемыми» месторождениями, что неизбежно ведет к цифровизации технологий, например, путем использования умных технологий добычи нефти, газа, таких как: Smart Field, i-field, Field of the future.

4 Кроме того, перед предприятиями сферы энергетики стоит задача по обеспечению энергосбережения, что также расширяет необходимость цифровизации, например, путем применения систем диспетчеризации энергопотребления.

5 В сфере транспортировки нефти и газа используется, как правило, дистанционное управление процессами производства. Компьютерная атака на такую систему способна привести к блокировке или остановке всего цикла производства.

6 Случаи атак на организации сферы ТЭК фиксируются по всему миру: 2012 – атака на национальную нефтяную компанию в Саудовской Аравии, в 2021 году произошла резонансная компьютерная атака, вынудившая остановить американский нефтяной трубопровод на пять дней. В 2022 году в результате кибер-атаки был остановлен центр европейской торговли нефтью Амстердам - Роттердам - Антверпен.

7 В настоящее время приходит понимание необходимости создания эффективных институтов, способных ответить на вызовы информационной (кибернетической) безопасности. Для создания таких институтов представляется необходимым обеспечить логичную, емкую правовую базу, не перегруженную большим количеством разнородных нормативных актов, а также не обремененную бюрократизацией процессов – т.е. систематизированную.

8 Рассматривая заявленную тему необходимо обратить внимание на такие документы стратегического планирования как:

9 «Национальная стратегия развития искусственного интеллекта на период до 2030 года» [1];

10 «Стратегия национальной безопасности» [2], которая затрагивает такие аспекты, как необходимость цифровизации промышленности, в том числе и труда работников, с обязательным приоритетом развития информационной безопасности, которая в том числе должна быть обеспечена российскими разработками технологий;

11 «Энергетическая стратегия Российской Федерации от 09.06.2020 №1523р», где указано на необходимость «рывка», который в том числе включает: «цифровую

трансформацию и интеллектуализацию отраслей топливно-энергетического комплекса» [3]; Кроме того, в Энергетической стратегии Российской Федерации указывается на необходимость увеличения организаций, деятельность которых направлена на разработку и внедрение технологических инноваций.

12 «Доктрина энергетической безопасности» [4], принятая в 2019 году, которая среди прочих рисков в области энергетической безопасности указывает на недостаточность реагирования российскими организациями ТЭК на вызовы мировой экономики в сфере технологического прогресса, распространение прорывных технологий, в том числе цифровых и интеллектуальных.

13 Среди угроз для энергетического сектора перечислены, в том числе компьютерные атаки на информационную инфраструктуру.

14 Все вышеперечисленные документы стратегического планирования указывают на необходимость совершенствования нормативно-правовой базы для возможностей: внедрения и функционирования высокотехнологичных продуктов в организациях энергетического комплекса, привлечения частного сектора в целях разработки и внедрения в деятельность организаций инновационных систем, соответствующих систем безопасности.

15 Широкое распространение цифровизации, необходимость которой обусловлена мировыми экономическими тенденциями требует от субъектов, которых затрагивают названные процессы, соблюдения высоких стандартов конфиденциальности, безопасности, этических норм и правил.

16 Кроме того, перед законодателем стоит выявленная проблема обеспечения единых стандартов функционирования цифровых продуктов, в том числе для потребителей энергии; виртуальных платформ; облачных сервисов; внутренней инфраструктуры организаций энергетического сектора.

17 Стоит отметить, что в Российской Федерации в текстах федеральных законов надлежаще не раскрыто понятие «информационная безопасность», а определение понятия «кибербезопасность» отсутствует.

18 Так, например, основополагающий закон в области защиты информации: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее - ФЗ № 149) [5] не раскрывает содержание понятия «информационная безопасность».

19 Что касается термина «кибербезопасность», его применение в нормативных документах ограничено. Так, например в недействующем в настоящее время Приказе Министерства финансов России от 06.06.2019 № 85н «О Порядке формирования и применения кодов бюджетной классификации Российской Федерации, их структуре и принципах назначения» [6], содержался термин «киберпространство».

20 В научной среде нет единства относительно применения к тому или иному предмету, таких терминов, как «информационная безопасность», «кибербезопасность».

21 Изучением разграничений рассматриваемых понятий занимались в том числе: А.А. Антипов, Е.М. Гришанова, М.М. Безкоровайный, А.Л. Татузрв, Е.С. Митряев, Н.Л. Каллимулин, О.А. Пучков.

22 В международной среде термин «информационная безопасность» и «кибербезопасность» имеют различное смысловое наполнение.

23 Обратимся к международным стандартам:

24 Стандарт ISO 27001 [7], регулирующий вопросы информационной безопасности, определяет «информационную безопасность» - как свойство информации, основанное на конфиденциальности, целостности и доступности.

25 Стандарт NIST800-53 [8], так же предлагает определять «информационную безопасность», как свойство информации, а «кибербезопасность» Стандарт определяется именно как обеспечение безопасности компьютеров, электронных систем связи, электронных коммуникаций, в том числе и содержащуюся в этих системах информацию.

26 В Китайской народной республике термин «кибербезопасность» и «защита данных» (в КНР термин «информация» раскрывается через понятие «данные») также имеют различное правовое и лингвистическое толкование. Так в КНР принят как Закон о кибербезопасности [9], вступивший в силу в 2017 году, так и Закон о безопасности данных Китайской Народной Республики [10].

27 В Индии действует Закон об информационных технологиях [11], который содержит раскрытие именно понятия «кибербезопасность».

28 Нормативные акты Европейского союза также разделяют кибернетическую безопасность и защиту данных.

29 По мнению автора, для построения логичной правовой системы необходимо разработать прежде всего унифицированный понятийный аппарат.

30 В рамках данной работы будут использованы: термин «информационная безопасность», а также термин «кибербезопасность» - при обращении к зарубежному регулированию.

31 Одним из основополагающих нормативных актов, регулирующих отношения в сфере защиты информации, является ФЗ № 149.

32 В научной середе вызывает определенные вопросы обеспечения правового режима конфиденциальности информации. Определенные трудности создает соотнесение правового режима конфиденциальности информации и различных правовых институтов в сфере «тайн», а также информации ограниченного доступа. Как указывает Г.Г. Камалова: «Ученые и специалисты, как правило, не разделяют признаки правового режима конфиденциальности и признаки охраняемых сведений – объекта режима, что, полагаем, не совсем правильно» [12, с. 100].

33 Существует правовая проблема в определении правового наполнения таких понятий, как личная тайна, семейная тайна, персональные данные. Правовые положения законодательства не определяют, кто именно определяет характер вышеперечисленных сведений.

34 Кроме того, определенную дискуссию вызывает наличие в ФЗ № 149 исключительно понятия «обладатель информации», под которым понимается, как субъект, создавший информацию, так и субъект, которому предоставлено право

пользования информацией. Субъект, создавший информацию, имеет исключительные права на информацию, в отличие от субъекта - пользователя информации.

35 Рассмотрев некоторую правовую проблематику, относительно защиты информации, как сведений и данных, обратим внимание на информационную безопасность производства - организаций сферы ТЭК.

36 Оценить значение критически важной инфраструктуры для каждого государства представляется сложной или скорее невозможной задачей, поскольку может способствовать выводу из строя основных «двигателей»: экономики, обороноспособности государства, влиять на жизнь простых граждан, а в некоторых случаях способны повлиять и на жизнедеятельность государств-партнеров.

37 Каждая организация энергетического сектора должна быть киберустойчивой, что означает, в том числе, сократить время простоя вследствие информационной атаки, а также ограничить распространение атаки на информационную систему предприятия, путем сужения области атаки.

38 Предлагается рассмотреть опыт зарубежных законодательств, а также провести некоторое сравнение с отечественными нормативными актами, регулирующими вопросы информационной защиты в энергетическом секторе.

39 В настоящее время Канадскими законодателями рассматривается законопроект под названием «Bill 26-C» [13], где особое внимание уделено правовому регулированию кибербезопасности критически важной инфраструктуры, путем выявления и управления рисками в сфере критической инфраструктуры, связанной с поставками ресурсов, выявление всех без исключения инцидентов, сведение к минимум возможных последствий инцидентов.

40 Согласно законопроекту, критическая киберсистема – при воздействии на конфиденциальность, целостность и доступность которой, нарушается непрерывность, безопасность жизненно необходимой службы или системы.

41 В законопроекте указано, что после того, как исполнительным органом власти назначается оператор критической киберсистемы (субъект – предприятие) оператору необходимо подготовить и внедрить в свой производственный цикл «программу кибербезопасности».

42 Программа кибербезопасности включает обязанности оператора в рамках обеспечения кибербезопасности: выявление рисков, недопущение разрыва цепочек поставок, ведение учета всех инцидентов, соблюдение нормативных документов.

43 Также программа должна содержать конкретные разумные действия, меры, которые будут внедрены для обеспечения безопасности.

44 После утверждения программы оператором критической киберсистемы, оператор обязан уведомить регулирующий орган о создании программы, а также предоставить последнему доступ к программе.

45 Программа кибербезопасности регулярно должна пересматриваться (проверяться оператором), для увеличения ее эффективности с учетом анализа возможных новых угроз. Для пересмотра программы может быть установлена выбранная дата самим оператором, но такой пересмотр должен происходить не реже одного раза в год, такой датой может быть дата утверждения программы.

46 Интерес представляет пункт законопроекта, где говорится, о том, что оператор обязан уведомлять регулирующий орган не только о корпоративных изменениях, происходящих в организации, но о таких изменениях как, использование иных программных продуктов или услуг, чем описано в программе.

47 Оператор непрерывно должен работать над выявлением и координацией возможных рисков, незамедлительно применять меры для снижения выявленных рисков.

48 Законопроект также предусматривает обязательное уведомление Учреждения безопасности об инциденте кибербезопасности – событие, которое может тем или иным образом повлиять на непрерывность поставок, услуг, которые являются жизненно необходимыми, либо событие, которое нарушает конфиденциальность. Внутренний механизм действия по такому уведомлению в обязательном порядке должен содержаться в правилах безопасности организации.

49 Следует отметить, что в Российской Федерации аналогично действует порядок уведомлений о компьютерных инцидентах, регулирующийся Приказом ФСБ России от 19 июня 2019 г. № 282 [14], который распространяется только на значимые объекты критической информационной инфраструктуры.

50 В рассматриваемом законопроекте отражен порядок инспектирования организаций – операторов критических киберсистем, а также прямо указано, на то, что лицо, которое осуществляет функции, обязанности по исполнению будущего закона и при этом действующее добросовестно, не несет ответственности за совершенные действия или бездействия, в рамках своих функций и полномочий.

51 Основное достоинство законопроекта заключается в удобстве его применения, которое достигнуто путем регулирования всей цепочки по обеспечению кибербезопасности оператора, в том числе и включения в законопроект положений о порядке проведения надзорных мероприятий.

52 В Российской Федерации информационная безопасность критической информационной инфраструктуры регулируется Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее - ФЗ № 187) [15].

53 Законопроект о защите критически важных киберсистем Канады и ФЗ № 187, имеют определенные схожие направления.

54 Рассматривая ФЗ «О безопасности критической информационной инфраструктуры» и приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (далее - Требования ФСТЭК № 239), следует обратить внимание на следующее: Требования ФСТЭК № 239 распространяются только на значимые объекты информационной инфраструктуры (пункт 2 Требований ФСТЭК № 239), к значимым государственным информационным системам данные Требования применяются с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 года № 17 [16].

55 Проблема категорирования объектов критической инфраструктуры вызывает широкую дискуссию в научной правовой среде. Остановимся только на одном положении – о выделении такого понятия, как значимый объекта критической инфраструктуры, при этом можно предположить, что существуют и «не значимые» объекты. Отдельным вопросом является: как объект критической информационной инфраструктуры может быть «не значимым»? Учитывая то, что воздействие на один объект критической инфраструктуры может повлиять на другой объект критической инфраструктуры, нужно ли учитывать «значимость»? Возможно, необходимо преобразовать систему категорирования объектов критический информационной инфраструктуры, не основываясь исключительно на возможных последствиях и ущербе от атаки на такие объекты.

56 В положениях Требований ФСТЭК России № 239 (пункты 28, 29) не содержится запрета на использование несертифицированного программного обеспечения, такого запрета нет и в ФЗ № 187.

57 Не содержит требований об обязательной сертификации средств информационной безопасности сферы энергетики «Положение по аттестации объектов информатизации по требованиям безопасности информации» (пункт 1.5.) [17], Федеральный закон от 27.12.2002 № 184-ФЗ «О техническом регулировании» [18].

58 В контексте рассмотрения данного вопроса необходимо обратить внимание на Приказ Минэнерго России от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования» [19]. Данный документ регулирует использование СУМиД в электроэнергетике и предусматривает применение только сертифицированных средств защиты информации для таких систем, в соответствии с ФЗ № 184-ФЗ.

59 Необходимо учитывать, что вышеназванный акт применимым только при регулировании правоотношений в сфере электроэнергетики.

60 Иллюстрацией необходимости использования как отечественных технологий, так и сертифицированных программных продуктов организациями ТЭК является резонансная история, связанная со швейцарским производителем шифровального оборудования Crypto AG, широкую известность которого обеспечила в том числе, публикация «Вашингтон пост» [20]. В ходе расследования было выяснено, что данная фирма действовала со времен Второй мировой войны. Закупку оборудования у Crypto AG производили организации из 120 стран мира, в том числе Иран, Латинская Америка, Пакистан, Индия. Важным фактом в разрезе информационной безопасности является то, что Crypto AG по соответствующей корпоративной схеме принадлежало ЦРУ и западногерманской разведке, как следствие разведывательные ведомства двух стран осуществляли перехват и прочтение засекреченных сообщений организаций 120 государств, как частного, так и государственного сектора.

61 Таким образом, недостаточность правового регулирования по вопросу использования определенных программных продуктов, обеспечивающих безопасность объектов ТЭК, и непосредственно программных продуктов, используемых в повседневной работе организаций сферы ТЭК может привести к негативным

последствиям. Существует необходимость разработки в Российской Федерации единой системы сертификации в области информационной безопасности в сфере ТЭК, путем создания единого нормативного акта, который будет регламентировать весь цикл правового регулирования данных правоотношений.

62 За рубежом поддерживаются требования о необходимости сертификации в сфере информационной безопасности, например, в Европейском Союзе был принят Регламент 2019/881 [21] [21], который установил правовые основы для создания единой системы сертификации продуктов, процессов и услуг – соответствующих определенному уровню кибербезопасности.

63 Риски в области защиты критической инфраструктуры вынуждают страны к принятию неоднозначных нормативных актов, так, например: «В июне 2019 Сенатом США принят Закон о безопасности энергетической инфраструктуры. Законопроект предлагал вернуться к использованию архаичных систем, отказаться от автоматизации и цифровизации процессов энергосистемы [22].

64 Кроме того, в сфере защиты критической инфраструктуры необходимо создание сбалансированных частно-государственных учреждений, которые не являлись бы надзорными органами в сфере информационной безопасности, как ФСБ, ФСТЭК.

65 Например, в США создан центр по оценке рисков и угроз для инфраструктуры, обеспечивающей национальную безопасность – DHS (HITRAC) [23], куда входят как специалисты в области разведки, так и специалисты в области промышленного комплекса. Центр непосредственно взаимодействует с частным сектором, чтобы его работа по выявлению, анализу угроз, исследованию последствий атак, разработки сценариев инцидентов и реагирования на них, разработки программных решений имели практическую ценность и были применимы.

66 Так же, в 2018 году, в США, Законом о кибербезопасности и безопасности инфраструктуры было создано одноименное Агентство (CISA), основные функции которого заключаются в следующем: оказании технической поддержки в области кибербезопасности предприятиям, которые подвергнуты кибер- рискам, выявление предприятий сферы кибернетического риска, проведении оценки рисков, способствовании информационному обмену по координации угроз, разработки рекомендаций по восстановлению после компьютерных инцидентов.

67 Правовой интерес вызывает относительно недавний документ Европейского Союза от 08.10.2022 «Цифровизация энергетической системы. План действий ЕС» [24]. План по цифровизации включает привлечение частных инвестиций в цифровые технологии, обеспечение интеллектуальными счетчиками потребителей, подключение 5G, 6G технологий, создание единой европейской базы энергетических данных, путем облачных хранилищ.

68 В Плане прямо указывается, на то, что безопасность поставок энергии, защита данных потребителя, конфиденциальность и кибербезопасность не должны быть оставлены на усмотрение инвесторов и рынка. Одной из мер, предлагающих обеспечить снижение киберугроз, является децентрализация производства и потребления энергии. Так же, отдельное внимание уделено рискам кибербезопасности и необходимости дальнейшего развития данного института.

69 Рассмотрев, как российскую законодательную модель информационной защиты в сфере ТЭК, так и примеры зарубежного законодательства, принимая во внимание проведенный анализ, можно прийти к следующим выводам.

70 В Российской Федерации необходимо сформировать единую законодательную базу, соответствующую современным тенденциям в целях обеспечения информационной безопасности топливно-энергетического комплекса.

71 Представляется целесообразным использование подхода, основанного на расчете рисков и соответственно соотношения объема необходимой информационной защиты.

72 Необходимы меры поддержки для стимулирования разработок и внедрения отечественных, как частных, так и государственных технологий в системы ТЭК. Кроме того, внедрение технологий, в том числе и для коммунальной инфраструктуры, способствующих более совершенному обмену информацией о возможных угрозах.

73 Представляется целесообразным на законодательном уровне закрепить требование о непрерывном взаимном обмене между частным сектором и государственными институтами, обеспечивающими координацию с взаимосвязанными организациями критической инфраструктуры, повышение осведомленности в сфере информационной безопасности, путем создания частно-государственных институтов. Необходимо правовое регулирование, способствующего развитию российских институтов стандартизации и внедрению единых стандартов безопасности для сферы ТЭК.

74 Кроме того, представляется необходимым сформировать единую правовую базу по сертификации продуктов автоматизации, цифровизации в сфере критической инфраструктуры, в том числе энергетическом секторе.

75 Изучение зарубежного законодательство показало, достаточно высокий уровень разработанности проблем защиты информации, производственных систем, но автор уверен, что в Российской Федерации присутствуют все возможности для проведения реформ, в области правовых норм, регулирующих институт информационной безопасность энергетического сектора.

Примечания:

1. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // URL: >>>> (дата обращения 01.05.2023).

2. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // URL: >>>> (дата обращения 01.05.2023).

3. Энергетическая стратегия Российской Федерации (утверждена Распоряжением Правительства РФ от 09.06.2020 № 1523-р) // URL: >>>> (дата обращения 01.05.2023)

4. Указ Президента РФ от 13.05.2019 № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» // URL: >>>> (дата обращения 01.05.2023).

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // URL: >>>> (дата обращения 02.05.2023).

6. Приказ Минфина России от 06.06.2019 № 85н (ред. от 21.03.2022) «О Порядке формирования и применения кодов бюджетной классификации Российской Федерации, их структуре и принципах назначения» // [сайт].- URL: >>>> (дата обращения 02.05.2023).

7. ГОСТ Р ИСО/МЭК 27001-2006. // URL: >>>> (дата обращения 02.05.2023).

8. NIST Special Publication 800-53. // URL: >>>> (дата обращения 02.05.2023).

9. China Cybersecurity Law. 2017. // URL: >>>> (дата обращения 02.05.2023).

10. Data Security Law of the People's Republic of China. 2021. // URL: >>>> (дата обращения 02.05.2023).

11. The information technology Act 2000. // URL: >>>> (дата обращения 02.05.2023).

12. Г.Г. Кагамалова. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества. Дис. Доктора юридических наук. 2019. С. 100.

13. BILL C-26. Critical Cyber Systems Protection Act. 2022. // URL: >>>> (дата обращения 03.05.2023).

14. Приказ ФСБ России от 19.06.2019 № 282 (ред. от 07.07.2022) «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации». // URL: >>>> (дата обращения 03.05.2023).

15. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. // URL: >>>> (дата обращения 03.05.2023).

16. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». // URL: >>>> (дата обращения 04.05.2023).

17. Положение по аттестации объектов информатизации по требованиям безопасности информации (утверждено Гостехкомиссией РФ 25.11.1994). // URL: >>>> (дата обращения 03.05.2023).

18. Федеральный закон от 27.12.2002 № 184-ФЗ (ред. от 02.07.2021) «О техническом регулировании» (с изм. и доп., вступ. в силу с 23.12.2021). // URL: >>>> (дата обращения 05.05.2023).

19. Приказ Минэнерго России от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования». // URL: >>>> (дата обращения 05.05.2023).

20. The intelligence coup of the century. // URL: >>>> (дата обращения 05.05.2023).

21. Regulation (EU) 2019/881 of the European Parliament and of the Council.2019. //URL: >>>> (дата обращения 10.05.2023)

22. Молчанов Н.А., Матевосова Е.К. Энергетическая безопасность в эпоху дигитализации. Вестник университета имени О.Е. Кутафина (МГЮА). С.92. // URL: >>>> (дата обращения от 05.50.2023).

23. Белоус А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. Москва Вологда «Инфра-Инженерия». 2020. С. 241-244. [Электронный ресурс]. URL: >>>> (дата обращения 08.05.2023).

24. Digitalising the energy system - EU action plan. Strasbourg, 18.10.2022 COM (2022) 552 final // URL: >>>> (дата обращения 09.05.2023).

Библиография:

1. Указ Президента РФ от 10.10.2019 № 490 “О развитии искусственного интеллекта в Российской Федерации”. URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 01.05.2023).

2. Указ Президента РФ от 02.07.2021 № 400 “О Стратегии национальной безопасности Российской Федерации”. URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 01.05.2023).

3. Энергетическая стратегия Российской Федерации, утверждена распоряжением Правительства РФ от 09.06.2020 № 1523-р. URL: http://www.consultant.ru/document/cons_doc_LAW_354840/ (дата обращения: 01.05.2023).

4. Указ Президента РФ от 13.05.2019 № 216 “Об утверждении Доктрины энергетической безопасности Российской Федерации”. URL: http://www.consultant.ru/document/cons_doc_LAW_324378/ (дата обращения: 01.05.2023).

5. Федеральный закон от 27.07.2006 № 149-ФЗ “Об информации, информационных технологиях и о защите информации”. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 02.05.2023).

6. Приказ Минфина России от 06.06.2019 № 85н “О Порядке формирования и применения кодов бюджетной классификации Российской Федерации, их структуре и принципах назначения” (ред. от 21.03.2022). URL: http://www.consultant.ru/document/cons_doc_LAW_327296/ (дата обращения: 02.05.2023).

7. ГОСТ Р ИСО/МЭК 27001-2006. URL: https://docs.cntd.ru/document/1200058325 (дата обращения: 02.05.2023).

8. NIST Special Publication 800-53. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата обращения: 02.05.2023).

9. China Cybersecurity Law. 2017. URL: https://d-russia.ru/wp-content/uploads/2017/04/China-Cybersecurity-Law.pdf (дата обращения: 02.05.2023).

10. Data Security Law of the People's Republic of China. 2021. URL: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (дата обращения: 02.05.2023).

11. The information technology Act 2000. URL: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (дата обращения: 02.05.2023).

12. Кагамалова Г.Г. Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: дис. … д-ра юрид. наук. М., 2019. С. 100.

13. BILL C-26. Critical Cyber Systems Protection Act. 2022. URL: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-26/first-reading (дата обращения: 03.05.2023).

14. Приказ ФСБ России от 19.06.2019 № 282 “Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации” (ред. от 07.07.2022). URL: http://www.consultant.ru/document/cons_doc_LAW_329210/ (дата обращения: 03.05.2023).

15. Федеральный закон от 26.07.2017 № 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 03.05.2023).

16. Приказ ФСТЭК России от 11.02.2013 № 17 “Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах” (ред. от 28.05.2019). URL: http://www.consultant.ru/document/cons_doc_LAW_147084/ (дата обращения: 04.05.2023).

17. Положение по аттестации объектов информатизации по требованиям безопасности информации, утверждено Гостехкомиссией РФ 25.11.1994. URL: http://www.consultant.ru/document/cons_doc_LAW_111428/ (дата обращения: 03.05.2023).

18. Федеральный закон от 27.12.2002 № 184-ФЗ “О техническом регулировании” (ред. от 02.07.2021, с изм. и доп., вступ. в силу с 23.12.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_111428/ (дата обращения: 05.05.2023).

19. Приказ Минэнерго России от 06.11.2018 № 1015 “Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования”. URL: http://www.consultant.ru/document/cons_doc_LAW_318489/ (дата обращения: 05.05.2023).

20. The intelligence coup of the century. URL: https://www.washingtonpost.com/graphics/2020/world/nationalsecurity/cia-crypto-encryption-machines-espionage/ (дата обращения 05.05.2023).

21. Regulation (EU) 2019/881 of the European Parliament and of the Council. 2019. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (дата обращения: 10.05.2023).

22. Молчанов Н.А., Матевосова Е.К. Энергетическая безопасность в эпоху дигитализации // Вестник университета имени О.Е. Кутафина (МГЮА). 2020. № 3. С. 92. URL: https://elibrary.ru/download/elibrary_42832238_13279092.pdf (дата обращения: 05.50.2023).

23. Белоус А.И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. М.; Вологда: Инфра-Инженерия, 2020. С. 241–244. URL: https://znanium.com/read?id=361650 (дата обращения: 08.05.2023).

24. Digitalising the energy system — EU action plan. Strasbourg, 18.10.2022 COM (2022). 552 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0552&qid=1666369684560 (дата обращения: 09.05.2023).

Legal Problems of the Assurance of Information (Cyber) Security of the Energy Sector in the Conditions of Digitalization

Anastasiia V. Vashechkina
Category 2 Specialist of the Economic Security Unit of the Corporate Protection Service of Gazprom Transgaz Yugorsk, LLC, Gazprom Transgaz Yugorsk, LLC
Russian Federation, Yugorsk

Abstract

The purpose of this paper is the study of problems of the legal support of information (cyber) security in the energy sector to enable making an attempt at the identification of key areas of further development of the legal regulation, inter alia, on the legislative level. Modernization of such legal institution as information security is a necessity and a priority especially considering the geopolitical conditions. Due maintenance and protection of information security facilities is the basis for the state, economic and social stability. The article concludes that there is a need to develop a system of proper certification of software products used in the fuel and energy complex, create public-private intermediary institutions to regulate issues of information security in the fuel and energy complex, pays attention to the classification of critical information infrastructure facilities and the development of an up-to-date regulatory framework in the sphere of regulation of information security of energy facilities.

Keywords: energy security, energy law, energy law and order, cyber security

Publication date: 24.01.2024

Citation link:

Vashechkina A. Legal Problems of the Assurance of Information (Cyber) Security of the Energy Sector in the Conditions of Digitalization // Energy law forum – 2023. – Issue 4 C. 90-97 [Electronic resource]. URL: https://mlcjournal.ru/S231243500029322-2-1 (circulation date: 03.07.2024). DOI: 10.61525/S231243500029322-2
