УДК 004.056

***С.П. Серёдкин*[1]**

[1] *Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация*

ОБЗОР НОРМАТИВНО-ПРАВОВЫХ АКТОВ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Аннотация. На сегодняшний день в России пройден этап формирования единой государственной политики в области защиты информации, создана нормативно-правовая основа построения системы обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ).

Настоящая статья посвящена исследованию нормативно-правовой базы в вопросе обеспечения безопасности значимых объектов КИИ. Приведена хронология создания законодательной основы по защите информации начиная с ключевых систем информационной инфраструктуры (КСИИ) и до настоящего времени, обеспечения безопасности значимых объектов КИИ (ОБ ЗО КИИ).

Эволюция законодательной базы по приведённому вопросу отражает динамику возрастающих требований к защите информации на объектах КИИ с целью противодействия возрастающему количеству угроз информационной безопасности. Требования регуляторов в первую очередь направленны на создание эффективной системы противодействия кибератакам, повышению ответственности субъектов КИИ перед обществом и государством с целью защиты жизненно важных интересов общества от террористических угроз.

Представлена тематика вопросов по обзору нормативно-правовой базы в соответствие с пунктом 1 «Безопасность и противодействие терроризму» из перечня приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» (утверждён Указом Президента Российской Федерации от 7 июля 2011 г. №899). Показан текущий обзор законодательства РФ по реализации требований к защите информации и противодействию кибератакам в отношении объектов КИИ. С законодательной точки зрения проанализированы современные подходы к созданию системы безопасности значимых объектов как механизма защиты жизненно важных интересов общества от террористических угроз. Подчеркнута важная роль нормативно-правовой базы для обеспечения безопасности объектов КИИ как основных приоритетных направлений обеспечения национальной безопасности.

Ключевые слова: Критическая информационная инфраструктура (КИИ), значимые объекты КИИ (ЗО КИИ), угрозы информационной безопасности, Федеральная служба по техническому и экспортному контролю (ФСТЭК), Государственная система обнаружения, предупреждения кибератак (ГосСОПКА), Национальный координационный центр по компьютерным инцидентам (НКЦКИ), информационная безопасность (ИБ), автоматизированные системы управления (АСУ).

***S.P. Seryodkin*[1]**

[1]*Irkutsk State Transport University, Irkutsk, Russian Federation*

REVIEW OF REGULATORY AND LEGAL ACTS TO ENSURE THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Abstract. To date, Russia has passed the stage of forming a unified state policy in the field of information protection, a regulatory framework has been created for building a security system for significant objects of critical information infrastructure (CII).

This article is devoted to the study of the regulatory framework in the issue of ensuring the safety of significant CII facilities. The chronology of the creation of the legislative framework for the protection of information is given, starting with the key information infrastructure systems (CIIS) and up to the present time, ensuring the security of significant CII facilities (about the CII).

The evolution of the legislative framework on the above issue reflects the dynamics of increasing requirements for the protection of information at CII facilities with the aim of countering the increasing number of threats to information security. The requirements of regulators are primarily aimed at creating an effective system for countering cyber attacks, increasing the responsibility of the subjects of the CII to society and the state in order to protect the vital interests of society from terrorist threats.

The topic of issues on the review of the regulatory framework in accordance with paragraph 1 "Security and countering terrorism" from the list of priority areas for the development of science, technology and technology in the

Russian Federation and the list of critical technologies of the Russian Federation" (approved by Decree of the President of the Russian Federation dated July 7, 2011 No. 899) is presented. The current review of the legislation of the Russian Federation on the implementation of requirements for information protection and countering cyber-attacks against CII objects is shown. From the legislative point of view, modern approaches to the creation of a security system of significant objects as a mechanism for protecting vital interests of society from terrorist threats are analyzed. The important role of the regulatory and legal framework for ensuring the safety of CII facilities as the main priority areas of ensuring national security is emphasized.

Keywords: Critical Information Infrastructure (CII), significant objects of CII (ZO CII), threats to information security, Federal Service for Technical and Export Control (FSTEC), State System of Detection, Prevention of Cyber Attacks (GosSOPKA), National Coordination Center for Computer Incidents (NCCI), information security (IS), automated control systems (ACS).

Введение. Прошло уже несколько лет с даты вступления в действие ФЗ №187 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации». Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак [1].

Согласно закону № 187-ФЗ, к объектам критической информационной инфраструктуры относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры в одной из следующих сфер: здравоохранение, наука, транспорт, связь, энергетика, банки и иные организации финансового рынка, топливно-энергетический комплекс, атомная энергия, оборона, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленности.

С момента вступления закона в силу, нормативно поддержано на законодательном уровне путем внесения поправок в Уголовный Кодекс (УК РФ) [2] и Кодекс об административных правонарушениях [3], соответствующими Федеральными законами [4,5] и имеет достаточно обширную нормативно-методическую базу основных регуляторов в области информационной безопасности – ФСТЭК России и ФСБ России.

Принятая Указом Президента Российской Федерации от 02.07.2021 г. № 400 Стратегия национальной безопасности Российской Федерации, в которой, в пункте 51, в качестве одной из важных угроз безопасности указано стремление и отработка действий иностранных государств по выведению из строя объектов КИИ Российской Федерации. В пункте 57 (подпункт 3) дается директива по реализации противодействия такой угрозе в рамках государственной политики по обеспечению информационной безопасности России [6].

Государственные учреждения и предприятия, законодательно определенны как субъекты данного направления нормативного регулирования, проведен достаточно обширный перечень методологических и организационных мероприятий по его практической реализации.

Динамично проводятся научно-технические исследования по данной тематике как отечественных [7,8], так и зарубежных специалистов, по разработке, в частности, практических инструментов определения важнейших услуг информационной инфраструктуры, в том числе комплексных подходов, по оценке устойчивости критически важных элементов информационной инфраструктуры.

Практическая реализация требований ФЗ №187 по категорированию объектов КИИ и созданию системы безопасности значимых объектов КИИ сталкивается с определенными трудностями, поэтому необходим системный анализ нормативной базы с целью методологической помощи специалистам по защите информации.

Исследованию этих вопросов по нормативному обеспечению сферы безопасности КИИ и посвящена настоящая работа.

Предыстория законодательного регулирования безопасности КИИ. Предыстория появления законодательства о безопасности КИИ связана уже с феноменом все

возрастающего влияния современных информационно-коммуникационных технологий. Переход на рубеже XX–XXI века к глобальному постиндустриальному (именуемого иногда информационным) сообществу развитых стран зафиксировано впервые Окинавской Хартией. В то же время по мере развития информационных технологий актуализировались проблемы обеспечения их безопасности [9].

Адекватным отечественным ответом на новые вызовы стало утверждение в этот период информационной безопасности как одного из приоритетного направления в рамках Стратегии национальной безопасности и государственной политики по ее реализации.

В 2000 г. принимается первый вариант Доктрины информационной Безопасности, который по своей структуре и содержанию являлся директивой прямого действия. Так одним из важных положений Доктрины стал достаточно короткий обобщенный перечень угроз национальной безопасности в информационной сфере, не потерявшим актуальности и в настоящее время в силу фундаментальности предложенных формулировок.

В принятом 2016 г. вторым вариантом Доктрины, с учетом возрастающего уровня угроз информационной безопасности на информационную инфраструктуру опасных и особо опасных производств и государственного сектора определяется необходимость разработки федерального закона о безопасности КИИ. В новом варианте Доктрины информационной безопасности в пункте 8 (подпункт б) (Указ Президента Российской Федерации от 5 декабря 2016 г. № 646) данное направление обозначено как одно из приоритетных в аспекте национальных интересов в информационной сфере [14].

Доктрина стала мощным стимулом для развития научных исследований и формирования отечественной целостной системы обеспечения информационной безопасности, включая системную структуру нормативно–правового обеспечения информационной безопасности и распределение полномочий органов государственной власти.

В 2004 г. в ходе административной реформы Гостехкомиссия России, выполнявшая функции одного из регуляторов в сфере защиты информации с ограниченным доступом, была преобразована в Федеральную службу по техническому и экспортному контролю (ФСТЭК России) [10]. При этом наряду с традиционными полномочиями Гостехкомиссии служба также получила статус уполномоченного органа по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры (ОБИ КСИИ). Этот момент можно условно считать исходной точкой начального периода становления анализируемого нового направления госрегулирования, которое и на настоящий момент еще далеко от своего завершения.

Несмотря на отсутствие специального закона, продолжалась работа по развитию директивной базы анализируемого направления, особенно после 2011 г., отмеченного выше как условный срок завершения формирования законодательной базы основных элементов правового обеспечения информационной безопасности. Так, можно еще рассмотреть директивный документ [11], в котором в пункте 3 (подпункт в) появилось определение **критической информационной инфраструктуры** Российской Федерации как совокупности автоматизированных систем управления критически важными объектами и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования, которых может стать причиной наступления тяжких последствий.

Исходя из общепринятой иерархии, верхним уровнем любой нормативной базы госрегулирования является базовый специальный закон либо, Указ Президента Российской Федерации.

Современный этап нормативно-правового регулирования обеспечения безопасности объектов КИИ. В 2017 г. принимается Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской

Федерации». Закон определяет основные принципы обеспечения безопасности, полномочия госорганов, а также права, обязанности и ответственность субъектов КИИ. Предусмотрены категорирование объектов, ведение реестра значимых объектов, оценка состояния защищенности, госконтроль, создание специальных систем безопасности.

Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"»

Дополняет Уголовный кодекс статьей 274.1, которая предусматривает наказания за неправомерное воздействие на КИИ РФ. Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"».

В связи с введение в действие ФЗ №187 издан Указ Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю...», в котором ФСТЭК России наделён полномочиями в области обеспечения безопасности КИИ, в том числе функцией государственного контроля [15].

Указ Президента РФ от 02.03.2018 № 98 «О внесении изменения в перечень сведений, отнесенных к государственной тайне...» относит к гостайне информацию о мерах обеспечения безопасности КИИ и о состоянии ее защищенности от атак. ФСБ России и ФСТЭК России назначены государственными органами, наделенными полномочиями по распоряжению сведениями, отнесенными к государственной тайне.

Постановлением Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры РФ и их значений» определён порядок и сроки категорирования объектов КИИ.

Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» Определяет правила проведения плановых и внеплановых проверок в области обеспечения безопасности значимых объектов КИИ.

Постановление Правительства РФ от 8.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры» устанавливает приоритетность категорий сетей электросвязи, которые могут использовать субъекты КИИ для обеспечения функционирования значимых объектов. Так же вышеупомянутое постановление определяет обязанности оператора связи при подключении значимых объектов к сети связи общего пользования. Документ вступил в силу с 1 января 2020 года.

Для обеспечения нормативных требований для создания и функционирования системы защиты КИИ разрабатываются ведомственные акты:

1) приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» который определяет сведения о значимом объекте КИИ, необходимые для внесения в реестр. Решение о включении в реестр принимается в течение 30 дней со дня получения ФСТЭК России сведений от субъекта КИИ. Не реже чем один раз в месяц ФСТЭК России направляет сведения из реестра в ГосСОПКА;

2) приказ ФСТЭК России от 11.12.2017 № 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

Российской Федерации», определяет форму акта по итогам проверки значимого субъекта КИИ;

3) приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», устанавливает требования к силам обеспечения безопасности значимых объектов, программным и программно-аппаратным средствам, документам по безопасности значимых объектов, функционированию системы безопасности;

4) приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий», определяет набор сведений о результатах присвоения объекту КИИ категории значимости, который необходимо направить во ФСТЭК России. Сведения сгруппированы в девять разделов;

5) приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», устанавливает требования к обеспечению безопасности значимых объектов КИИ в ходе создания, эксплуатации и вывода их из эксплуатации, к организационным и техническим мерам защиты информации и определяет состав мер для каждой категории значимости объекта;

6) приказ ФСТЭК России от 26.04.2018 № 72 «О внесении изменений в Регламент Федеральной службы по техническому и экспортному контролю, утвержденный приказом ФСТЭК России от 12 мая 2005 г. № 167», относит обеспечение безопасности значимых объектов КИИ к нормативно-правовому регулированию вопросов ФСТЭК России. Слова «информации в ключевых системах» заменяет словом «критической»;

7) приказ ФСТЭК России от 09.08.2018 № 138 «О внесении изменений в Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах...», определяет список изменений в приказы № 31 и 239. Состав мер защиты информации и их базовые наборы по классу защищенности АСУ изложены в новой редакции.

Отдельно хотелось бы остановиться на целях и задачах ГосСОПКА — государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации. Цель системы — объединить усилия для предотвращения и противодействия кибератакам на критически важные информационные инфраструктуры. Для этого создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который организует сбор и обмен информацией об инцидентах между субъектами КИИ, координирует мероприятия по реагированию, предоставляет методические рекомендации по предупреждению компьютерных атак. Инициирование создания НКЦКИ определение его задач и прав изложено в приказе ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам». Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации...», устанавливает набор параметров инцидентов для передачи в НКЦКИ (не позднее 24 часов с момента их обнаружения) и способы передачи информации.

Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...», определяет способы передачи информации об инциденте другим субъектам КИИ и получения сведений субъектами КИИ об атаках. Обмен информацией с иностранными организациями осуществляет НКЦКИ. Приказ ФСБ России от

06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты...», обязывает субъекта КИИ согласовывать с НКЦКИ установку средств ГосСОПКА и уведомлять о приеме их в эксплуатацию. Определяет необходимые для согласования сведения. 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...», определяет состав плана реагирования на инциденты и принятия мер по ликвидации последствий, разрабатываемого субъектом КИИ. Обязует информировать НКЦКИ о результатах реагирования и ликвидации последствий не позднее 48 часов после завершения мероприятий.

Так же в этот период времени принимаются ведомственные акты:

1) «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 27.12.2016 (документ ограниченного доступа) Документ детализирует порядок создания ведомственных и корпоративных центров ГосСОПКА, их функции, а также технические и организационные меры защиты информации;

2) «Временный порядок включения корпоративных центров в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак...» (документ ограниченного доступа) Определяет состав документов и уровень квалификации специалистов группы реагирования, необходимые для подключения к ГосСОПКА. Информационно-аналитическое, организационное и материально-техническое обеспечение НКЦКИ осуществляется Центром защиты информации и специальной связи ФСБ России [12].

Нормативное регулирование и ответственность субъектов КИИ. Для реализации требований ФЗ № 187 от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» в отношении субъектов критической информационной инфраструктуры значительно претерпели изменения в Уголовном кодексе Российской Федерации, так же 26 мая 2021 года на официальном интернет-портале правовой информации был опубликован Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях». Вместе с штрафами установлен срок давности привлечения к административной ответственности за нарушения в области обеспечения безопасности КИИ РФ, который составляет 1 год (ч. 1 ст. 4.5). В случае признания правонарушения длящимся срок давности исчисляется с момента обнаружения правонарушения проверяющим.

В таблице №1 представлены типы нарушений и наказания за соответствующие правонарушения с учетом принятых в УК и КоАП изменений.

Таблица 1.

Типы нарушений и наказания за соответствующие правонарушения с учетом принятых в УК и КоАП изменений.

НПА	Статья	Тип нарушения	Наказание
Административная ответственность			
КоАП РФ	13.12.1 (ч.1)	Нарушение требований к созданию систем безопасности значимых объектов КИИ РФ и	• для должностных лиц – штраф от 10 000 до 50 000 рублей;

		обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов КИИ РФ, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ, если такие действия (бездействие) не содержат уголовно наказуемого деяния	• для юридических лиц – штраф от 50 000 до 100 000 рублей.
	13.12.1 (ч.2)	Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами РФ	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	13.12.1 (ч.3)	Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными организациями, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты	• для должностных лиц – штраф от 20 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
	19.7.15 (ч.1)	Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ РФ, сведений о результатах присвоения объекту КИИ РФ одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности КИИ РФ, либо об отсутствии необходимости присвоения ему одной из таких категорий	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 50 000 до 100 000 рублей.
	19.7.15 (ч.2)	Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ информации, предусмотренной законодательством в области обеспечения безопасности КИИ РФ, за исключением случаев, предусмотренных частью 2 статьи 13.12.1 КоАП	• для должностных лиц – штраф от 10 000 до 50 000 рублей; • для юридических лиц – штраф от 100 000 до 500 000 рублей.
Уголовная ответственность			
УК РФ	274.1 (ч.1)	Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной	• принудительные работы до 5 лет с ограничением свободы до 2 лет или без такового; • лишение свободы от 2 до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода, осужденного за период от 1 года до 3 лет.

		информации.	
	274.1 (ч.2)	Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на КИИ РФ, или иных вредоносных компьютерных программ, если он повлек причинение вреда КИИ РФ	• принудительные работы на срок до 5 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода, осужденного за период от 1 года до 3 лет и с ограничением свободы на срок до 2 лет или без такового; • лишение свободы на срок от 2 до 6 лет со штрафом в размере от 500 000 до 1 000 000 рублей или в размере заработной платы или иного дохода, осужденного за период от 1 до 3 лет;
	274.1 (ч.3)	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, или ИС, ИТС, АСУ, сетей электросвязи, относящихся к КИИ РФ, либо правил доступа к указанным информации, ИС, ИТС, АСУ, сетям электросвязи, если оно повлекло причинение вреда КИИ РФ.	• принудительные работы до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового; • лишение свободы на срок до 6 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.
	274.1 (ч.4)	Деяния, предусмотренные частями 1-3 статьи 274.1, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения.	лишение свободы на срок от 3 до 8 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.
	274.1 (ч.5)	Деяния, предусмотренные частями 1-4 статьи 274.1, если они повлекли тяжкие последствия.	лишение свободы на срок от 5 до 10 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 5 лет или без такового.

Выводы. Актуальность информации и выводы, приведенные в статье, очевидны. Действующая нормативно-правовая база по обеспечению безопасности объектов КИИ определяет механизм государственного регулирования и взаимодействия федеральных органов государственной власти в области защиты информации с субъектами, владельцами объектов КИИ. Законодательная база по обеспечению безопасности КИИ находится в постоянном развитии, в связи с изменяющимися вызовами и возрастающими угрозами информационной безопасности как внутренними, так и внешними.

Кроме того, приведенный в статье обзор нормативно – правовых актов показывает в настоящее время действующий механизм и системную структуру законодательной базы для создания и функционирования эффективной системы обеспечения безопасности объектов КИИ.

Есть надежда, что изложенная в статье информация может быть полезна аспирантам и преподавателям, ведущим научную и педагогическую деятельность в предметной области, а также даст возможность практического применения материала статьи специалистами по защите информации и владельцами объектов КИИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.Федеральный закон от 26 июня 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2.«Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ.

3. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ.

4. Федеральный закон от 26.05.2021 № 141-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

5. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 194-ФЗ.

6. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

7. Грачков И.А., Малюк А.А. Проблемы разработки доверенного программного обеспечения, применяемого на объектах критической информационной инфраструктуры (организационные и методические аспекты). Безопасность информационных технологий, [S.l.]. Т. 26, No. 1. С. 56–63, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.1.06.

8. Грачков И.А Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты. Безопасность информационных технологий, [S.l.]. Т. 25, No. 1. С. 90–98, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.09

9. Тарасов, Анатолий М. Окинавская хартия и конгрессы ООН: Вопросы противодействия киберпреступности. Безопасность информационных технологий, [S.l.]. Т. 26, No 4. С. 120–131, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.09.

10. Указ Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

11. «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». Утверждены Президентом Российской Федерации Д. Медведевым 3 февраля 2012 г., № 803.

12. http://www.consultant.ru/law/hotdocs/54965.html/ © КонсультантПлюс, 1992-2022

13. «Безопасность и противодействие терроризму» из перечня приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» (утверждён Указом Президента Российской Федерации от 7 июля 2011 г. №899)

14. «Доктрина информационной безопасности Российской Федерации». Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

15. Указ Президента РФ от 25.11.2017 N 569 "О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. N 1085"

REFERENCES

1. Federal Law No. 187-FZ of June 26, 2017 "On the Security of the Critical Information Infrastructure of the Russian Federation".

2. "Criminal Code of the Russian Federation" dated 13.06.1996 No. 63-FZ.

3. "Code of the Russian Federation on Administrative Offenses" dated 30.12.2001 No. 195-FZ.

4. Federal Law No. 141-FZ of 26.05.2021 "On Amendments to the Code of Administrative Offences of the Russian Federation".

5. Federal Law "On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Criminal Procedure Code of the Russian Federation in Connection with the Adoption of the Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" dated 26.07.2017 No. 194-FZ.

6. Decree of the President of the Russian Federation No. 400 dated July 2, 2021 "On the National Security Strategy of the Russian Federation".

7. Grachkov I.A., Malyuk A.A. Problems of trusted software development,

applied at critical information infrastructure facilities (organizational and methodological aspects). Information Technology Security, [S.L.]. Vol. 26, No. 1. pp. 56-63, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.1.06

8. Grachkov I.A. Information security of automated control systems: possible attack vectors and methods

of protection. Information Technology Security, [S.L.]. Vol. 25, No. 1. pp. 90-98, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.1.09

9. Tarasov, Anatoly M. Okinawa Charter and UN Congresses: Counteraction issues

cybercrime. Information Technology Security, [S.L.]. Vol. 26, No. 4. pp. 120-131, 2019.ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.09 .

10. Decree of the President of the Russian Federation No. 1085 dated 16.08.2004 "Issues of the Federal Service for Technical and Export Control".

11. "The main directions of the state policy in the field of ensuring the safety

of automated control systems for production and technological processes of critical infrastructure facilities of the Russian Federation". Approved by the President of the Russian Federation Dmitry Medvedev on February 3, 2012, No. 803.

12. http://www.consultant.ru/law/hotdocs/54965.html/ © ConsultantPlus, 1992-2022

13. "Security and countering terrorism" from the list of priority areas for the development of science, technology and technology in the Russian Federation and the list of critical technologies of the Russian Federation" (approved by Presidential Decree No. 899 of July 7, 2011)

14. "The Doctrine of Information Security of the Russian Federation". Approved by Decree of the President of the Russian Federation No. 646 of December 5, 2016.

15. Decree of the President of the Russian Federation of 25.11.2017 N 569 "On Amendments to the Regulations on the Federal Service for Technical and Export Control, approved by Decree of the President of the Russian Federation of August 16, 2004 N 1085"

Информация об авторе

Сергей Петрович Серёдкин – к. э. н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: sseryodkin2008@yandex.ru.

Author

Sergei Petrovich Seryodkin – Ph. D. in Economics, Associate Professor, the Subdepartment of Information systems and information security, Irkutsk State Transport University, Irkutsk, e-mail: sseryodkin2008@yandex.ru.

Для цитирования

Серёдкин С.П. Обзор нормативно-правовых актов по обеспечению безопасности критической информационной инфраструктуры // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2022. – №3(15). – С.47-57– DOI: 10.26731/2658-3704.2022.3(15).47-57 – Режим доступа: http://ismm-irgups.ru/toma/315-2022, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 15.10.2022)

For citations

Seryodkin S.P. Review of regulatory and legal acts to ensure the security of critical information infrastructure // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2022. No. 3(15). P. 47-57. DOI: 10.26731/2658-3704.2022.3(15).47-57 [Accessed 15/10/22]