Михнев Илья Павлович
заслуженный работник науки и образования,
канд. техн. наук, доцент
Михнева Светлана Владимировна
канд. юрид. наук, доцент РАН, доцент
Волгоградский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Волгоград, Волгоградская область

DOI 10.31483/r-32617

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ: ПОЛНОМОЧИЯ ФЕДЕРАЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РФ

Аннотация*: в статье рассматриваются компетенции и полномочия органов государственной власти РФ в рамках их правового статуса в сфере обеспечения безопасности критической информационной инфраструктуры. В ряде федеральных органов исполнительной власти изменились некоторые функции и полномочия в сфере информационной безопасности. В частности, Федеральная Служба Безопасности на основании Указа Президента РФ уполномочена на создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Однако не все права и обязанности являются закрепленными, ряд полномочий вызывает двойственность правового положения некоторых федеральных органов государственной власти. Четкость и однозначность закрепления прав и обязанностей государственных органов, уполномоченных в сфере информационной безопасности, являются гарантиями эффективного обеспечения безопасности значимых объектов информационной инфраструктуры.*

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

***Ключевые слова**: информационная безопасность, компьютерные инциденты, орган государственной власти, полномочия федерального органа, компьютерные атаки, критическая информационная инфраструктура.*

Информационная безопасность сегодня наиболее актуальная составляющая всей системы национальной безопасности, так как экономическая, экологическая, пожарная, продовольственная и иные виды безопасности напрямую связаны с информационными системами, автоматизированным управлением объектами инфраструктуры. В Российской Федерации тема критической информационной инфраструктуры развивается на протяжении последних 10 лет, однако в системной совокупности норм и положений нашла свое законченное оформление только в Федеральном законе №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Во многом это обусловлено ситуацией на международной арене, где обострение отношений между государствами зачастую сопровождается информационными конфликтами, приводящими к так называемой информационной войне [1].

Современные события в ряде стран, связанные с нарушением и сбоями в работе компьютерных операционных систем в важных социально-экономических и политических сферах, в частности, в Иране, Северной Корее, Венесуэле, Уругвае обусловили наибольшую актуальность разработки комплекса мер защиты информации, информационных систем, а также выделили для государственного аппарата на первый план задачу уточнения объектов критической информационной инфраструктуры и обеспечения их безопасности широким рядом органов государственной власти федерального уровня [2]. В связи с этим законодатель четко систематизировал и обозначил основные сферы общественной жизнедеятельности нашей страны, объекты критической информационной инфраструктуры которых нуждаются в защите и обеспечении информационной безопасности. В частности, это сфера здравоохранения, науки, транспорта, финансового сектора, ракетно-космическая промышленность, атомная энергетика и другие. В связи с этим, была проделана тщательная работа законодателем по разработке категориального аппарата, поясняющего и

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

уясняющего новые вводимые термины, впервые на федеральном уровне четко определено понятие термина – критическая информационная инфраструктура, выделены ее субъекты, значимые объекты и способы их защиты [3].

Основной вопрос, который встал на повестку дня перед государственными структурами при обеспечении безопасности критической информационной инфраструктуры, это определение перечня органов государственной власти и установление их полномочий в рассматриваемой сфере. Прежде всего, следует указать на исполнительную и правоохранительную составляющие государственного аппарата. Так, Президент РФ, Правительство РФ, Федеральная служба безопасности (ФСБ) России, Федеральная служба по техническому и экспортному контролю (ФСТЭК) – являются основными субъектами, уполномоченными обеспечивать безопасность критической информационной инфраструктуры в России. Федеральный закон №187-ФЗ закрепил в функциях ФСБ – создание и функционирование государственной системы обнаружения, предотвращения и ликвидации компьютерных атак и образование Национального координационного центра по компьютерным инцидентам. Основное назначение и важная цель данного центра состоит в организации и осуществлении обмена информацией о компьютерных инцидентах между субъектами информационной безопасности, а также между субъектами и уполномоченными органами иностранных государств, международными организациями, в координировании мероприятий по реагированию на компьютерные инциденты и непосредственное участие в таких мероприятиях [4].

Важность анализа полномочий органов власти обусловлена разработкой механизма эффективной защиты информации, информационных систем и автоматизированных систем управления в приоритетных и значимых сферах здравоохранения, науки, транспорта, атомной энергетики. Сегодня говорить о надлежащем уровне обеспеченности безопасности современным потребностям государства, общества и возможным угрозам в информационной сфере еще рано. В связи с чем, четкость в установлении функций государственных органов по обеспечению безопасности критической информационной инфраструктуры,

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

определении их полномочий и механизма реализации являются необходимыми составляющими комплекса мероприятий по осуществлению государственной политики обеспечения информационной безопасности в России. С введением новых положений в области защиты информации в результате принятия нового Федерального закона «О безопасности критической информационной инфраструктуры в РФ» можно выявить эффективность введенных норм, а также указать на проблемные стороны и пробелы правового регулирования соответствующих общественных отношений. Элементы информационного права России как развивающейся самостоятельной публичной отрасли требуют соответствующего юридического сопровождения. А потому нуждаются в научном осмыслении с учетом действующего законодательства и практики его применения для правильности определения ряда понятий, выявления юридического положения участвующих субъектов, их полномочий, прав, обязанностей и ответственности [5].

Полномочия федеральных органов исполнительной власти РФ в сфере обеспечения безопасности критической информационной инфраструктуры являются необходимым элементом их деятельности. От четкости их установления зависит и степень защиты значимых объектов критической информационной инфраструктуры. Поэтому важность анализа закрепления и определения полномочий федеральных органов обусловлена выявлением степени правовой урегулированности сферы информационной безопасности и ее соответствия реальным потребностям и правовым, финансовым возможностям субъектов критической информационной инфраструктуры [6].

Учитывая важность сферы безопасности критической информационной инфраструктуры, основные функции по обеспечению ее безопасности отводятся федеральной власти, прежде всего, Президенту РФ, Правительству РФ, ФСБ России и ФСТЭК России. В целях оптимального распределения и определения функций, полномочий, прав и обязанностей данных органов, исключения их дублирования законодатель закрепляет понятие критической информационной инфраструктуры, хотя правоприменительное использование этой категории на

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

практике отмечалось и ранее [7]. Согласно закону, под критической информационной инфраструктурой подразумеваются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, используемые для организации их взаимодействия. Ключевым условием отнесения системы к КИИ является ее использование государственным органом или учреждением в 12 обозначенных сферах, в частности: здравоохранения, науки, транспорта, финансовом секторе, ракетно-космической промышленности и других [8].

Полномочия можно определить как определенные законом возможности правового действия органа власти, а также задачи и функции, направленные на выполнение компетенции органов. Прежде всего, ряд полномочий по обеспечению критической информационной инфраструктуры РФ закон закрепляет за Президентом РФ, который вырабатывает основу государственной политики в этой сфере, а также определяет два федеральных органа исполнительный власти: уполномоченный в области обеспечения безопасности критической информационной инфраструктуры и орган, обеспечивающий функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, порядок создания и задачи этой системы [9].

Правительство РФ, обеспечивая безопасность критической информационной инфраструктуры, осуществляет категорирование, контроль и интегрирование электросвязи. В связи с этим, в полномочия его входит: налаживание единой сети электросвязи России для функционирования объектов информационной инфраструктуры; установление данных факторов и критериев значимости объектов критической информационной инфраструктуры с их значениями, а также порядок и сроки осуществления их категорирования; определение порядка и процедуры осуществления госконтроля в области безопасности информационной инфраструктуры.

В полномочия ФСТЭК входит обеспечение безопасности критической информационной инфраструктуры, а ФСБ отвечает за функционирование госу-

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)

дарственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА). Согласно закону ФСТЭК несет ответственность за ведение реестра объектов КИИ, проверку правильности их категорирования, разработку требований по безопасности для каждой категории объектов, осуществление государственного контроля. ФСБ несет ответственность за оценку состояния защищенности, порядок реагирования на компьютерные инциденты, порядок ликвидации последствий компьютерных атак, порядок обмена информацией об инцидентах, разработку требований к ГосСОПКА.

Проблематика обеспечения информационной безопасности сегодня активно развивается, но утверждать о соответствии уровня ее обеспеченности требованиям современных реалий государственной и общественной жизни еще рано. Для качественной реализации положений Федерального закона 2017 года о безопасности критической информационной инфраструктуры требуется комплекс мероприятий нормативно-правового и финансово-экономического характера, поскольку выдвигаемые государством требования по установления усовершенствованных систем обеспечения безопасности повлекут для субъектов – обладателей объектов инфраструктуры значительные расходы по внедрению систем защиты инфраструктуры, а также мероприятия по повышению квалификации сотрудников.

Список литературы

1. Михнев И.П. Правовое регулирование деятельности в сфере информационной безопасности в Российской Федерации: достижения, проблемы и перспективы развития / И.П. Михнев [и др.] // Вестник Алтайской академии экономики и права. – 2018. – №6. – С. 227–233.

2. Иванова Ю.О. Функции субъектов по защите критической информационной инфраструктуры в РФ / Ю.О. Иванова, А.Н. Крылов // Муниципальная служба: правовые вопросы. – 2018. – №4. – С. 33–35.

3. Михнев И.П. Полномочия федеральных органов государственной власти Российской Федерации в области обеспечения безопасности критической ин-

Содержимое доступно по лицензии Creative Commons Attribution 4.0 license (CC-BY 4.0)

формационной инфраструктуры / И.П. Михнев // Вестник Алтайской академии экономики и права. – 2019. – №1–2. – С. 202–208.

4. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. №187-ФЗ // Российская газета. – 2017. – №7333 (167), 31 июля.

5. Михнев И.П. Защита конфиденциальной информации от несанкционированного доступа при проектировании автоматизированных систем радионуклидной спектрометрии на базе сцинтилляционного гамма-спектрометра / И.П. Михнев, Н.А. Сальникова, И.П. Мединцева // Научное обозрение: монография / гл. ред. Э.Н. Рябинина. – Чебоксары, 2018. – С. 48–58.

6. Бачолин Н.Л. Информационное право. Основы практической информатики. – М.: Юринформцентр, 2012.

7. Михнев И.П. Защита информации от несанкционированного доступа при анализе радиационных характеристик помещений спектрометрическим методом / И.П. Михнев, Н.А. Сальникова, А.Г. Кравец // Известия Волгоградского государственного технического университета. – 2018. – №8 (218). – С. 105–109.

8. Кленина В.И. Информационные технологии в профессиональной деятельности юриста / В.И. Кленина // Ученые записки. – 2010. – №7. – С. 99–102.

9. Михнева С.В. Правовое положение главы исполнительно-распорядительного органа местного самоуправления в Российской Федерации / С.В. Михнева, И.П. Михнев, Е.С. Митячкина // Вестник Алтайской академии экономики и права. – 2019. – №1. – С. 191–197.

Content is licensed under the Creative Commons Attribution 4.0 license (CC-BY 4.0)