УДК 004.73
DOI 10.21685/2587-7704-2018-4-1-7

Open Access | RESEARCH ARTICLE

Обзор нормативно-правовых актов в области обеспечения безопасности критической информационной инфраструктуры

Д. В. Чернов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. П. Иванов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В статье рассмотрен Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», постановление Правительства РФ от 08.02.2018 № 127 и Приказ ФСТЭК России от 25.12.2017 № 239.

Ключевые слова: критическая информационная инфраструктура, субъект критической информационной инфраструктуры, объект критической информационной инфраструктуры, безопасность критической инфраструктуры.

A review of regulatory legal acts in the field of critical information infrastructure security

D. V. Chernov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. P. Ivanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article considers the Federal Law No. 187-FL “On Security of Critical Russian Federation Information Infrastructure” of 26.07.2017, the Resolution of the Government of the Russian Federation of 08.02.2018 No. 127, and the Order of the FSTEC Russia of 25.12.2017 No. 239.

Keywords: critical information infrastructure, subject of critical information infrastructure, object of critical information infrastructure, safety of critical infrastructure.

Вступивший в силу 1 января 2018 г. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [1] вводит понятие критической информационной инфраструктуры, заменяя им понятие ключевой системы информационной инфраструктуры.

Целью настоящего закона является обеспечение функционирования объектов критической информационной инфраструктуры при проведении в их отношении компьютерных атак.

Закон устанавливает понятия субъектов критической информационной инфраструктуры, объектов и значимых объектов критической информационной инфраструктуры.

В качестве объектов критической информационной инфраструктуры выступают:

– информационные системы;

– информационно-телекоммуникационные сети;

– автоматизированные системы управления субъектов критической информационной инфраструктуры.

При этом объекты критической информационной инфраструктуры должны функционировать в сферах:

– банковской сфере и иных сферах финансового рынка;
– науки;
– здравоохранения;
– транспорта;
– связи;
– энергетики;
– топливно-энергетического комплекса;
– оборонной;
– ракетно-космической;
– горнодобывающей, металлургической и химической промышленности;
– атомной энергии.

В качестве субъектов критической информационной инфраструктуры выступают:

– государственные органы,
– государственные учреждения;
– российские юридические лица и (или) индивидуальные предприниматели.

Объекты критической информационной инфраструктуры должны принадлежать субъектам на законном основании.

В рамках реализации требований настоящего закона созданы Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, Национальный координационный центр по компьютерным инцидентам и реестр значимых объектов критической информационной инфраструктуры.

В соответствии со ст. 7 настоящего закона объекты критической информационной инфраструктуры подлежат категорированию.

Категорирование проводится непосредственно субъектом критической информационной инфраструктуры в соответствии с Постановлением Правительства РФ от 08.02.2018 № 127 [2]. Для этих целей субъектом создается комиссия.

На первом этапе категорирования составляется перечень критических процессов, т.е. процессов, нарушение или прекращение которых может привести к негативным последствиям. К ним относятся:

– социальные последствия;
– политические последствия;
– экономические последствия;
– экологические последствия;
– последствия для обеспечения обороны страны, безопасности государства и правопорядка.

На втором этапе определяется перечень объектов критической информационной инфраструктуры, подлежащих категорированию. В него входят объекты, которые обрабатывают информацию, необходимую для обеспечения критических процессов и (или) осуществляют управление, контроль или мониторинг критических процессов. Данный перечень утверждается руководителем субъекта критической информационной инфраструктуры и направляется ФСТЭК в течение пяти дней с момента утверждения.

Категорирование объектов критической информационной инфраструктуры проводится в срок, не превышающий одного года со дня утверждения перечня объектов.

Категорирование проводится на основе масштаба возможных последствий в случае возникновения компьютерных инцидентов, с учетом анализа угроз безопасности и уязвимостей объекта и анализа возможных действий нарушителя.

Результатом категорирования является присвоение одной из трех категорий объекту критической информационной инфраструктуры или отсутствие необходимости присвоения, а также оформление соответствующего акта. Результаты категорирования направляются ФСТЭК в течение десяти дней с момента подписания акта. Объекты, которым была присвоена категория, являются значимыми объектами критической инфраструктуры.

Стоит отметить тот факт, что ни Постановление Правительства, ни Федеральный закон не устанавливают срока начала проведения категорирования либо срока, к которому это категорирование необходимо провести. Устанавливается лишь срок между определением перечня объектов, подлежащих категорированию, и самим категорированием.

Категория значимости объекта может быть изменена:

– по мотивированному решению ФСТЭК по результату проверки в рамках государственного контроля;

– в случае изменения значимого объекта, в результате которого он перестает соответствовать критериям значимости, по которым был категорирован;

– в случае ликвидации, реорганизации субъекта или изменения его организационно-правовой формы, в результате он перестает являться субъектом критической информационной инфраструктуры.

В соответствии со ст. 10 настоящего закона субъект критической информационной инфраструктуры должен создать систему безопасности значимых объектов. Система безопасности должна включать в себя набор организационных и технических мер в соответствии с Требованиями, утвержденными ФСТЭК [3]. Они определяют базовый набор мер для каждой категории значимости.

В рамках создания системы безопасности субъектом критической информационной инфраструктуры необходимо разработать:

– модель угроз;

– проект системы защиты значимого объекта;

– рабочую документацию на значимый объект по части обеспечения его безопасности.

Модель угроз включает в себя описание источников угроз, уязвимости объектов, способы реализации угроз и возможные последствия.

Проект системы защиты включает в себя перечень субъектов и объектов доступа, политики управления доступом, перечень организационных и технических мер, перечень средств защиты с указанием мест установки и параметров настройки. Рабочая документация включает в себя описание системы защиты, порядок и параметры их настройки, а также правила эксплуатации программных и программно-аппаратных средств и средств защиты.

В случае, если объект критической информационной инфраструктуры является государственной информационной системой, то настоящие Требования [3] применяются с учетом Требований, утвержденных приказом ФСТЭК № 17. Для объектов критической информационной инфраструктуры, обрабатывающих персональные данные, настоящие Требования [3] применяются с учетом Требований, утвержденных постановлением Правительства от 1 ноября 2012 г. № 1119. В случае, если объект критической информационной инфраструктуры обрабатывает информацию, составляющую государственную тайну, то его защита осуществляется в соответствии с законодательством РФ о государственной тайне.

Для незначимых объектов критической информационной инфраструктуры настоящие Требования [3] применяются по решению субъекта критической информационной инфраструктуры.

Всю информацию, необходимую для обеспечения безопасности критической информационной инфраструктуры, субъект может получить от ФСТЭК. К такой информации может относиться информация об угрозе безопасности информации, уязвимостях программного обеспечения, оборудования и технологиях.

Библиографический список

1. О безопасности критической информационной инфраструктуры Российской Федерации : Федер. закон от 26.07.2017 № 187-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/, свободный (дата обращения: 12.10.2018).
2. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : Постановление Правительства РФ от 08.02.2018 № 127. – URL: http://www.consultant.ru/document/cons_doc_LAW_290595/#dst100074, свободный (дата обращения: 12.10.2018).
3. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 09.08.2018). – URL: https://fstec.ru/component/attachments/download/1902, свободный (дата обращения: 12.10.2018).

Образец цитирования:

Чернов, Д. В. Обзор нормативно-правовых актов в области обеспечения безопасности критической информационной инфраструктуры / Д. В. Чернов, А. П. Иванов // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–3. – DOI 10.21685/2587-7704-2018-4-1-7.