УДК 004.056
DOI: 10.33764/2618-981X-2019-6-1-128-133

ВОЗМОЖНЫЕ ПОДХОДЫ К КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Кирилл Евгеньевич Щелкин
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (905)936-36-63, e-mail: shchelkin94@gmail.com

Полина Александровна Звягинцева
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, ст. преподаватель кафедры информационной безопасности, тел. (923)135-79-78, e-mail: polinasgugit@mail.ru

Валентин Валерьевич Селифанов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности, тел. (923)247-25-81, e-mail: sfo1@mail.ru

Рассматриваются основные аспекты категорирования объектов критической информационной инфраструктуры, вне зависимости, значимый объект или нет, в особенности тех объектов, которые являются уже аттестованными или прошедшими классификацию информационной системы ранее.

Ключевые слова: категорирование, объект критической информационной инфраструктуры, безопасность критической информационной инфраструктуры.

POSSIBLE APPROACHES TO CATEGORIZATION OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Kirill E. Shchelkin
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone:(905)936-36-63, e-mail: shchelkin94@gmail.com

Polina A. Zvyagintseva
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Senior Lecturer, Department of Information Security, phone: (923)135-79-78, e-mail: polinasgugit@mail.ru

Valentin V. Selifanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Associate Professor, Department of Information Security, phone: (923)247-25-81, e-mail: sfo1@mail.ru

The main aspects of categorization of critical information infrastructure objects, regardless of whether an object is significant or not, are considered, in particular those objects that are already certified or have passed classification of information system earlier.

Key words: categorization, critical information infrastructure object, security of critical information infrastructure.

С началом действия Федерального закона от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [1] (далее – 187-ФЗ) субъекты, на которые распространяются нормы данного закона, должны организовать целый комплекс мероприятий по соблюдению положений данного нормативного акта [8], а также появился новый сегмент в отрасли защиты информации, соответственно, новые субъекты и объекты взаимодействия, которые необходимо категорировать в соответствии с новыми постановлениями и приказами. В связи с этим необходимо рассмотреть особенности категорирования и их варианты.

В соответствии со статьей 2 187-ФЗ, под значимым объектом критических информационных инфраструктур (далее – ЗОКИИ) понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры, функционирующие в двенадцати сферах.

В той же статье приводится понятие субъекта критической информационной инфраструктуры. Субъектами критической информационной инфраструктуры являются органы государственной власти, государственные учреждения, юридические лица и индивидуальные предприниматели, у которых в собственности имеются информационные системы (далее – ИС), информационно-телекоммуникационные сети (далее – ИТКС), автоматизированные системы управления (далее – АСУ ТП), функционирующие в 12 сферах.

При этом, основную роль законодатель отводит значимым объектам информационной инфраструктуры, т. е. объектам, которым в соответствии с постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127 «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» [2] (далее – ПП № 127) присвоена одна из трех категорий значимости.

При этом рассматриваемые объекты, зачастую, уже существовали до вступления в силу 187-ФЗ, к тому же прошли соответствующую классификацию и, как правило, имеют соответствующую систему защиты информации и класс защищенности.

Таким образом, задача категорирования и обеспечения безопасности ЗОКИИ часто будет сводиться к дополнительной классификации (категорированию), доработке и модернизации систем защиты информации информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления. В рамках данной работы рассмотрим наиболее распространенные информационные системы – государственные информационные системы.

Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [5] (далее – 149-ФЗ), статья 13, государственные информационные системы (далее – ГИС) – это федеральные и региональные информационные системы, созданные на основании,

соответственно, федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов. При формировании требований к защите информации согласно Приказу ФСТЭК России № 17 п. 14 [4] (далее – Приказ № 17), информационная система подлежит классификации и, в связи с выходом 187-ФЗ, подлежит категорированию. К значимым объектам критической информационной инфраструктуры будут относиться информационные системы, имеющие соответствующий уровень значимости, сопоставимые с перечнем из ПП № 127, и масштаб системы, определяющийся исходя из Приложения № 1 Приказа № 17, и при этом относящиеся к сфере (или сферам), прописанным в 187-ФЗ.

В данном случае, чтобы отнести ГИС к ЗОКИИ, требуются уровни значимости первый или второй (именно для значимых объектов), а также масштабы системы федеральный и региональный, исходя из понятия государственной информационной системы.

Определим критерии, по которым возможно присвоить уровень значимости ЗОКИИ. Уровень значимости будет определяться исходя из нарушения одного из свойств информации и степени ущерба. Есть три вида степени ущерба: высокий, средний и низкий. Отличает их только то, что в результате нарушения меняются возможные последствия:

– существенно-негативные последствия, которые наносят высокую степень ущерба;

– умеренно-негативные последствия, которые наносят среднюю степень ущерба;

– незначительно-негативные последствия, которые наносят низкую степень ущерба.

Но практически все эти последствия совпадают с показателями перечня критериев значимости объектов критической информационной инфраструктуры, а это следующие критерии значимости:

– социальная;

– политическая;

– экономическая.

Масштаб информационной системы определяется из Приложения № 1 п. 3 Приказа № 17. Их три: федеральный, региональный и объектовый. В данной работе рассматриваются федеральный и региональный масштабы информационных систем.

Рассмотрим подробнее масштаб каждой системы:

– ГИС имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях;

– ГИС имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или несколь-

ких муниципальных образованиях и (или) подведомственных и иных организациях [9].

Исходя из класса защищенности информационной системы, можно определить соответствие с таблицей из приложения Приказа № 17, наверняка под действие закона, в первую очередь, попадут системы с классом защищенности К1 и К2 [10], но категорию значимости объекта КИИ назначит орган государственной власти или орган местного самоуправления, которому принадлежит ГИС.

Сопоставляя классификационные признаки, а именно масштаб системы и уровень значимости из Приложения № 1 Приказа № 17 с положениями, приведенными в ПП № 127, получаем следующие соответствия, приведенные в табл. 1.

Таблица 1

Сопоставление классификационных признаков

Уровень значимости	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ1	I	I, II	II
УЗ2	I, II	II, III	III
УЗ3	II, III	III, без категории	III, без категории

Помимо ГИС, информационные системы персональных данных (далее – ИСПДн) так же могут являться ЗОКИИ, согласно Статье 13 п. 1, 152-ФЗ [6]: «Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных».

Не все ИСПДн могут являться ЗОКИИ, а только те, которые имеют первый и второй уровень защищенности персональных данных.

Основанием для сопоставления уровней защищенности ИСПДн с ЗОКИИ является пункт 5 Приказа ФСТЭК России № 239: «Для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие Требования применяются с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 [7] (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257) [3]».

Чтобы окончательно доказать, что ИСПДн или ГИС могут являться ЗОКИИ, необходимо сопоставить классификационные признаки между ними. ГИС имеет три класса защищенности информации. Соотнесем каждый класс с критерием значимости, учитывая сферы деятельности (табл. 2).

В итоге процесс категорирования для субъектов КИИ, которым принадлежат информационные системы, которые уже являются ГИС или ИСПДн, может включать в себя следующие этапы:

Таблица 2

Сопоставление классификационных признаков с категориями объектов КИИ

Сфера деятельности	ИС	Масштаб ИС	Класс защищенности	Категория
Наука	ГИС	Федеральная	К1	I, II

– ответ на вопрос, является ли организация субъектом КИИ;

– определение всех процессов в организации (процессы могут быть управленческие, технологические, финансово-экономические, производственные и т. д.);

– выделение из всех процессов именно критических процессов;

– выделение объектов, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов и (или) осуществляют управление, контроль или мониторинг критических процессов;

– оценка, исходя из перечня показателей критериев значимости и учитывая дополнительные исходные данные, к какой категории относятся объекты КИИ;

– составление Акта категорирования объектов КИИ для отправки во ФСТЭК.

Исходя из данных, приведенных в статье, делаем вывод, что категорирование ИС, АСУ ТП или ИТКС будет удобнее, чем кажется, особенно тех объектов, которые уже прошли аттестацию или классификацию ранее.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон от 26.07.2017 № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/42128, свободный (дата обращения: 10.03.2019).

2. Постановление 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 Российской Федерации и их значений» [Электронный ресурс]. – Режим доступа:http://publication.pravo.gov.ru/Document/View/0001201802130006, свободный (дата обращения: 10.03.2019).

3. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». [Электронный ресурс]. – Режим доступа: https://minjust.consultant.ru/documents/38914, свободный (дата обращения: 10.03.2019).

4. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс]. – Режим доступа: https://fstec.ru/normotvor-cheskaya/akty/53-prikazy/702, свободный (дата обращения: 10.03.2019).

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный (дата обращения: 10.03.2019).

6. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный (дата обращения: 10.03.2019).

7. Правительство Российской Федерации. Постановление от 1 ноября 2012 г. № 1119 об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/, свободный (дата обращения: 10.03.2019).

8. Пошаговая инструкция от экспертов по реализации 187-ФЗ [Электронный ресурс]. – Режим доступа: https://ru-bezh.ru/gossektor/news/18/11/20/poshagovaya-instrukcziya-ot-ekspertov-po-realizaczii-187-fz.

9. Организационные и технические меры защиты информации в государственной информационной системе [Электронный ресурс]. – Режим доступа: http://ace-net.ru/judgment/73-.

10. Методический документ «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11 фев 2014 г.) [Электронный ресурс]. – Режим доступа: https://www.dokipedia.ru/document/5173382.