Министерство науки и высшего образования РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

Е.М. Давыдова, А.Ю. Якимук

ОРГАНИЗАЦИЯ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Учебно-методическое пособие
для студентов направлений подготовки
10.00.00 Информационная безопасность

Томск
2022

УДК 004.056
ББК 32.973.26-018.2
Д 64

Рецензент:
Конев А.А., доцент кафедры комплексной информационной безопасности электронно-вычислительных систем ТУСУР, канд. техн. наук

Давыдова, Елена Михайловна
К 64 Организация защиты объектов критической информационной инфраструктуры: учебно-методическое пособие / Е.М. Давыдова, А.Ю. Якимук. – Томск: Томск. гос. ун-т систем упр. и радиоэлектроники, 2022. – 20 с.

Настоящее учебно-методическое пособие содержит описания практических и самостоятельных работ по дисциплине «Организация защиты объектов критической информационной инфраструктуры» для направлений подготовки, входящих в укрупненную группу специальностей и направлений 10.00.00 Информационная безопасность.

УДК 004.056
ББК 32.973.26-018.2

Содержание

Введение

С 01 января 2018 года вступил в силу Федеральный закон от 26.07.2017 № 187ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — 187-ФЗ), регулирующий отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

В соответствии с требованиями законодательства, субъекты КИИ должны присвоить одну из категорий значимости принадлежащим им объектам КИИ. Если объект КИИ не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

Критерии значимости, показатели их значений, а также порядок осуществления категорирования определены в Постановлении Правительства РФ 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» (далее — ПП-127).

Целью преподавания дисциплины является формирование компетенций, необходимых специалистам, для обеспечения безопасности значимых объектов критической инфраструктуры.

Задача изучения дисциплины: изучение принципов выделения объектов, угроз, а также определение способов и средств защиты объектов критической инфраструктуры.

Самостоятельная работа

Ознакомиться с нормативными актами по обеспечению безопасности объектов критической информационной инфраструктуры:

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Постановление Правительства РФ 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»;

– Постановление Правительства РФ от 13.04.2019 № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127»;

– Приказ ФСТЭК России от 22 декабря 2017 г. № 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»;

– Информационное сообщение ФСТЭК России по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий от 24 августа 2018 г. № 240/25/3752;

– Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.;

– Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры;

– Информационное сообщение ФСТЭК России о методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации от 4 мая 2018 г. № 240/22/2339.

Практическая работа №1
Мероприятия по определению оснований для отнесения организации к объектам критической информационной инфраструктуры

1 Цель работы

Целью данной практической работы является изучение основных мероприятий по определению оснований для отнесения организации к объектам критической информационной инфраструктуры.

2 Краткие теоретические сведения

В соответствии с определением в 187-ФЗ, субъект КИИ – это:

1) государственный орган, государственное учреждение, российское юридическое лицо и (или) индивидуальный предприниматель, которому на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере:

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

2) российское юридическое лицо и (или) индивидуальный предприниматель, который обеспечивает взаимодействие указанных систем или сетей. ***(Важно:*** *к государственным органам и государственным учреждениям не применимо.***)**

3 Ход работы

3.1. Определение сфер деятельности организации.

В 187-ФЗ установлены 13 сфер (областей деятельности), которые подпадают под его область действия. По определению, к субъектам КИИ

относятся те организации, которые владеют объектами, функционирующими в указанных сферах, а не организации, работающие в данных областях.

При этом ФСТЭК России был предложен метод, основанный на определение сферы деятельности организации в соответствии с:

– ОКВЭД и ОКОГУ;

– лицензиями, сертификатами и иными разрешительными документами на виды деятельности;

– учредительными документами, уставами, положениями организации, где прописаны основные и вспомогательные виды деятельности.

Соответственно, если в любом из данных источников присутствует указание на рассматриваемые сферы деятельности, то по мнению ФСТЭК России, присутствуют признаки того, что организация является субъектом КИИ.

1. В Лицензиях / Уставе / кодах ОКВЭД и ОКОГУ организации выявляем деятельность в областях, соответствующих 187-ФЗ.
2. Анализируем область функционирования используемых ИСиР (Распоряжения Правительства Москвы по созданию ИСиР, государственные программы, проектную документацию на создание ИСиР и подобное).
3. Определяем ИСиР, используемые для реализации соответствующего вида деятельности, указанного в уставе, лицензии или ОКВЭД.
4. Анализируем на предмет принадлежности данных ИСиР Организации (право собственности, аренда, договор пользования, хозяйственного ведения, право оперативного управления и т. д.).

Если выявлена ИСиР, удовлетворяющая указанным параметрам, то принимается решение о признании организации субъектом КИИ.

Пример 1

ГКУ ИАЦ в сфере здравоохранения города Москвы

Код ОКВЭД 72.1 «Научные исследования и разработки в области естественных и технических наук» и код ОКОГУ 2300229 «Органы исполнительной власти субъектов Российской Федерации / - здравоохранения»

Необходимо выявить ИСиР автоматизирующие процессы в сферах науки и здравоохранения.

Пример 2

АО «Электронная Москва» имеет лицензии Роскомнадзора на следующие услуги связи:

Услуги связи по предоставлению каналов связи

Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации

Услуги на телематические услуги связи

Необходимо выявить ИСиР автоматизирующие процессы оказание услуг связи.

3.2. Определение деятельности в организации по обеспечению взаимодействия объектов КИИ

В качестве обеспечения взаимодействия объектов КИИ может рассматриваться:

– предоставление вычислительных мощностей для объектов КИИ и каналов взаимодействия с ними (ЦОД);

– предоставление телекоммуникационных услуг, в рамках которых осуществляется взаимодействие объектов КИИ;

– предоставление иных информационных услуг для обеспечения взаимодействия с объектами КИИ.

Частными случаями таких субъектов являются операторы сетей связи или ИС, предназначенных для обеспечения работы государственных ИС или взаимодействия с объектами энергетического комплекса — для данных лиц ответственность за обеспечение взаимодействия объектов КИИ указывается в документации на системы/каналы связи, а также в их обязанностях.

В более неопределенных случаях, когда Организация предоставляет вычислительные мощности и каналы связи для широкого круга заказчиков, детальной информации о том, что инфраструктура может использоваться для организации взаимодействия КИИ, может не быть. Однако, незнание данной информации не освобождает организацию от ответственности.

1. Проводим анализ наличия объектов инфраструктуры, находящейся в собственности Организации, которая используется в интересах сторонних лиц и для организации информационного взаимодействия систем, не принадлежащих самой Организации.

Пример 3

Права собственника и оператора АИС СУДИР возложены на ДИТ.

При этом, СУДИР обеспечивает предоставление доступа к информационным системам и ресурсам, принадлежащих другим ОИВ города Москвы на основе централизованного управления учетными данными участников информационного взаимодействия и реализации технологии однократной аутентификации пользователей информационных систем города Москвы

2. В случае выявления соответствующих объектов инфраструктуры, уточняем наличие у Организации явных поручений на уровне

законодательных актов и нормативных требований (Распоряжения Правительства Москвы и т.д.), возлагающих на Организацию обязанности по обеспечению информационного взаимодействия между сторонними ИСиР. В случае наличия указанных обязательств, запрашиваем владельцев сторонних ИСиР (ОИВ и их организаций) об отнесении данных систем к объектам КИИ (включена ли данная ИСиР в Перечень объектов КИИ, подлежащих категорированию сторонней организации). В случае положительного ответа, Организация признается субъектом КИИ.

3. В случае наличия инфраструктуры Организации, которая используется для информационного обмена сторонними ИСиР, делается запрос владельцам данных систем об их отнесении к объектам КИИ (включена ли данная ИСиР в Перечень объектов КИИ, подлежащих категорированию сторонней организации). В случае положительного ответа, делается уточнение наличия компонентов инфраструктуры и сетей передачи данных, используемых для указанного взаимодействия и находящихся в собственности Организации. В случае положительного заключения Организация признается субъектом КИИ.

4. Организация рассматривает свою инфраструктуру (или ее часть, непосредственно задействованную в обеспечении взаимодействия объектов КИИ) в качестве объекта КИИ.

Пример 4

Организация владеет и обслуживает ЦОД, в котором размещаются ИСиР ОИВ Москвы, в сфере транспорта или здравоохранения.

Выявлено, что некоторые из размещаемых в ЦОД ИСиР относятся к объектам КИИ. Программно-аппаратное обеспечение компонентов ИС является собственностью ОИВ Москвы, в сфере транспорта или здравоохранения. При этом, для взаимодействия между данными ИС, а также с внешними системами и пользователями используются каналы передачи данных и коммутационное оборудование ЦОД, которые принадлежат Организации. В данном случае ***Организация является субъектом КИИ****, как обеспечивающая взаимодействие объектов КИИ.*

ВАЖНО: *Сеть электросвязи Организации, непосредственно задействованная в обеспечении взаимодействия объектов КИИ, не должна рассматриваться в качестве объекта КИИ и в Перечень объектов КИИ, подлежащих категорированию, не включается.*

Пример 5

Организация предоставляет услуги технической поддержки и сопровождения ОИВ Москвы, в сфере транспорта или здравоохранения.

Работники Организации администрируют ИС, ИТС и АСУ, являющихся объектами КИИ, управляют сетевыми компонентами, отвечают за работоспособность и взаимодействие систем.

В данном случае Организация ***не является субъектом КИИ****, так как ее работники обеспечивают «поддержку» работоспособности систем, но фактически взаимодействие объектов КИИ обеспечивается программно-аппаратными компонентами, не находящимися в собственности у Организации.*

Заключение Рабочей группы о наличии/отсутствии оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры и рекомендаций по включению их в Перечень объектов с последующим установлением одной из категорий значимости объектов критической информационной инфраструктуры, либо об отсутствии оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры в соответствии с законодательством Российской Федерации.

Заключение об отсутствии оснований может оформляться по консолидированной форме на все ИСиР ОИВ/организации сразу. Но желательно оформление отдельного заключения о наличии/отсутствии оснований по каждой информационной системе ОИВ/организации в отдельности.

Практическая работа №2
Проведение инвентаризации объектов КИИ

1 Цель работы

Целью данной практической работы является изучение процедуры инвентаризации объектов критической информационной инфраструктуры.

2 Краткие теоретические сведения

В случае принятия решения о наличии оснований для отнесения ИСиР ОИВ/организации к объектам критической информационной инфраструктуры, необходимо провести предварительный анализ угроз безопасности информации и реализованных меры по обеспечению безопасности. Провести предварительную оценку масштаба возможных последствий в случае возникновения компьютерных инцидентов в ИСиР в соответствии с перечнем показателей критериев значимости, утвержденных ПП-127. Сформировать предложение Рабочей группы о присвоении данной ИСиР категории значимости либо об отсутствии необходимости присвоения одной из таких категорий, а также перечень необходимых мер по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

Подготовленные материалы служат основаниями для принятия окончательных решений Комиссией по определению объектов критической информационной инфраструктуры и категорий значимости объектов критической информационной инфраструктуры.

В соответствии с ПП-127, категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в областях (сферах), установленных пунктом 8 статьи 2 Федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

3 Ход работы

3.1. Формирование перечня процессов

Анализируется устав и учредительные документы, иные положения организации, где прописаны основные и вспомогательные виды деятельности, имеющиеся лицензии, сертификаты и иные разрешительные документы на виды деятельности — из них выписываются все указанные функции и виды деятельности.

Анализируется организационная структура Организации, анализируются положения об отделах и/или запрашивается информация об

обязанности и функциях подразделений Организации. Данная информация используется для детализации или расширения перечня функций Организации, полученного на первом шаге.

Для каждой выявленной функции / осуществляемого вида деятельности формируется перечень процессов, реализуемых в рамках этой функции / вида деятельности.

В соответствии с ПП-127, необходимо формировать перечень процессов, с учетом их соотнесения с отраслями / областями деятельности, которые обозначены в 187-ФЗ. Субъекты КИИ определяются через 13 сфер функционирования ИС / АСУ / ИТКС.

Пример 6

Процессы ДИТ в сфере связи:

Постановление Правительства Москвы №105-ПП «Об утверждении Положения о Департаменте информационных технологий города Москвы»

- Создание и эксплуатации городской мультисервисной транспортной сети (ГМТС) Правительства Москвы.

- Организация работ по подготовке технических условий, согласованию и оформлению разрешительной документации для выполнения работ по прокладке волоконно-оптических линий для системы обеспечения безопасности города Москвы и комплексной автоматизированной системы обеспечения безопасности населения города Москвы.

- Утверждение порядка разработки и согласования схемы размещения таксофонов на территории города Москвы.

- Согласование передачи прав пользования, владения, распоряжения линейно-кабельными сооружениями связи и сетями связи и иным движимым и недвижимым имуществом, необходимым для их эксплуатации, находящимся в собственности города Москвы.

- Определение порядка пользования, владения, распоряжения линейно-кабельными сооружениями связи и сетями связи и иным движимым и недвижимым имуществом, необходимым для их эксплуатации, находящимся в собственности города Москвы.

- Утверждение по согласованию с Департаментом городского имущества города Москвы порядка приемки во временную эксплуатацию вновь построенных или реконструированных за счет средств бюджета города Москвы линейно-кабельных сооружений связи и сетей связи и иного движимого и недвижимого имущества, необходимого для их эксплуатации.

- Обеспечение содержания, обслуживания и временной эксплуатации бесхозяйных линейно-кабельных сооружений связи и сетей связи и иного движимого и недвижимого имущества, необходимого для их эксплуатации, до признания прав собственности города Москвы на такое имущество.

- Обращение в уполномоченный орган государственной власти с целью постановки на учет бесхозяйных линейно-кабельных сооружений связи и сетей связи, а также государственной регистрации прав собственности города Москвы на линейно-кабельные сооружения связи и сети связи и иное движимое и недвижимое имущество, необходимое для их эксплуатации, в том числе бесхозяйные линейно-кабельные сооружения и сети связи и иное движимое и недвижимое имущество, необходимое для их эксплуатации.

- Обеспечение выдачи технических условий при строительстве и/или реконструкции линейно-кабельных сооружений и сетей связи, вновь возводимых и/или реконструируемых на территории города Москвы за счет средств бюджета города Москвы.

- Утверждение рекомендуемой формы договора на размещение таксофона.

3.2 Определение критичности процессов

Для каждого выявленного процесса должна быть проведена оценка критичности его нарушения с точки зрения возможных негативных социальных, политических, экономических, экологических последствий, последствий для обеспечения обороны страны, безопасности государства и правопорядка.

В связи с тем, что критерии оценки критичности нарушения процессов в ПП-127 явно не заданы, то будем использовать перечень критериев значимости объектов и их значения из Приложения 1 к ПП-127 (минимальные показатели категории значимости). Определяем для каждого рассматриваемого процесса, способно ли его нарушение повлечь последствия, соответствующие, минимальным показателям критериев значимости из ПП-127.

Пример 7

Остановка процесса «Утверждение порядка разработки и согласования схемы размещения таксофонов на территории города Москвы» не приводит к прекращению или нарушению функционирования сетей связи и не приводит к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

3.3 Формирование перечня объектов

Для каждого критичного процесса определяется перечень ИСиР, которые осуществляют:

- обработку информацию, необходимую для критических процессов;
- управление критическим процессом;
- контроль или мониторинг критических процессов.

Важно:

Обработка – систематическое выполнение операций над данными, необходимыми для обеспечения критического процесса.

Управление – поддержание критического процесса в рабочем состоянии в рамках заданных значений характеристик критического процесса.

Контроль – сравнение (сопоставление) фактических (текущих) значений характеристик критического процесса с заданными значениями этих характеристик.

Мониторинг – постоянное (регулярное) наблюдение за значениями характеристик критического процесса.

Сформирован Перечень ИСиР, подлежащих категорированию и оформлен в табличной форме (таблица 3).

Пример 8

№	*Наименование ИСиР*	*Тип ИСиР*	*Назначение*	*Сфера деятельности, в которой функционирует ИСиР*
1	*Система №1*	*Информационная система*	*Мониторинг*	*Связь*
2	*Система №2*	*Информационная система*	*Обработка*	*Здравоохранение*

Комиссия по категорированию принимает окончательное решение о формировании перечня объектов, подлежащих категорированию.

Таблица 4.

№	Наименование объекта	Тип объекта [1]	Сфера (область) деятельности, в которой функционирует объект [2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1.					
2.					

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

[3] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

Практическая работа №3
Проведение категорирования объектов КИИ

1 Цель работы

Целью данной практической работы является изучение процедуры категорирования объектов критической информационной инфраструктуры.

2 Краткие теоретические сведения

Определение категорий значимости объектов КИИ осуществляется на основании показателей критериев значимости и их значений, утвержденных ПП-127.

При категорировании осуществляется:

– анализ возможных источников угроз и действий предполагаемых нарушителей;

– анализ возможных угроз и типов компьютерных атак;

– оценка масштаба последствий угроз и соотнесение со значениями показателей категорий;

– определение категории значимости объекта КИИ;

– оформление акта категорирования.

3 Ход работы

3.1 Анализ возможных действий нарушителей

Данная информация получается экспертным путем. В случае, если для рассматриваемой ИСиР существует модель угроз и нарушителей, то используются данные из нее. Также могут использоваться существующие данные из моделей угроз и моделей нарушителей для схожих ИСиР, функционирующих в Организации.

3.2 Анализ угроз безопасности информации и типов компьютерных атак

Для каждой ИСиР проводится анализ возможных угроз и их последствий. В случае, если для рассматриваемой ИСиР существует модель угроз и нарушителей, то используются данные из нее. Также могут использоваться существующие данные из моделей угроз и моделей нарушителей для схожих ИСиР, функционирующих в Организации.

3.3 Оценка масштаба последствий и соотнесение со значениями показателей категорий

Для рассматриваемой ИСиР необходимо определить возможные последствия нарушений, основываясь на выявленных возможных угрозах ИБ, типах компьютерных атак, назначение ИСиР и автоматизируемого процесса. Для рассматриваемой ИСиР должны выбираться те типы последствий, которые могут стать следствием реализации вероятных угроз для данной ИСиР. В качестве последствий рассматриваем:

1) причинение ущерба жизни и здоровью людей;

2) прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов обеспечивающие водо-, тепло-, газо- и электроснабжение населения;

3) прекращение или нарушение функционирования объектов транспортной инфраструктуры;

4) прекращение или нарушение функционирования сети связи;

5) отсутствие доступа к государственной услуге;

6) прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия);

7) нарушение условий международного договора РФ, срыв переговоров или подписания планируемого к заключению международного договора РФ, оцениваемые по уровню международного договора РФ;

8) возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший 5-летний период);

9) возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период);

Важно: для периода **2019-2021** это 20 388, 65 млрд. рублей. Соответственно, если оцениваемый ущерб бюджетам РФ менее 20 388,65 млн. рублей, то принимается решение об отсутствии необходимости присвоения категории значимости. В иных случаях необходимо руководствоваться таблицей 5:

Таблица 5.

Категория значимости	**3**	**2**	**1**
Ущерб, млрд. руб	до 1019,43, включительно	от 1019,43 до 2038,86, включительно	более 2038,86

10) прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации

системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений);

11) вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосфере, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия);

12) прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра;

13) снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры;

14) прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка.

При оценке масштабов последствий и соотнесении со значениями показателей категорий следует использовать (для соответствующих ИСиР):

– договоры на оказание соответствующих услуг (учет количества потребителей и подключаемых территориальных объектов);

– паспорта объектов (систем);

– ТЗ на объекты;

– результаты категорирования объектов транспортной инфраструктуры;

– декларация промышленной безопасности;

– паспорта безопасности опасного производственного объекта;

– декларация безопасности объектов;

– паспорта безопасности объектов топливно-энергетического комплекса;

– результаты категорирования объектов, оказывающих негативное воздействие на окружающую среду;

– результаты классификации сетей электросвязи.

Полученная оценка масштабов последствий должна соотноситься со значениями показателей критериев значимости и для каждого показателя должна быть определена соответствующая категория значимости.

Должны быть рассмотрены наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты критической информационной инфраструктуры, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба.

Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей и т. д.), оценка производится по каждому из значений показателя критериев значимости.

В случае если показатель критерия значимости неприменим для ИСиР или ИСиР не соответствует ни одному показателю и их значениям (оцененный масштаб ниже минимального показателя критерия значимости), категория значимости данной ИСиР не присваивается.

3.4 Определение категории значимости объекта КИИ

Объекту КИИ присваивается категория значимости, соответствующая наивысшему значению из присвоенных категорий при соотнесении возможного ущерба с показателями категорий значимости (самая высокая категория – первая, самая низкая – третья).

Важно: эта информация используется комиссией по категорированию для принятия и оформления окончательного решения по ИСиР.

Результат:

Собрана в формализованном виде информация по ИСиР, рекомендованных к отнесению к объектам КИИ.

3.5 Оформление акта категорирования объекта КИИ

Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры.

Допускается оформление единого акта по результатам категорирования нескольких объектов критической информационной инфраструктуры, принадлежащих одному субъекту критической информационной инфраструктуры.

Литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Постановление Правительства РФ 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».

3. Информационное сообщение ФСТЭК России по вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий от 24 августа 2018 г. № 240/25/3752.

4. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г.

5. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры.

6. Информационное сообщение ФСТЭК России о методических документах по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации от 4 мая 2018 г. № 240/22/2339.

7. Методические рекомендации по категорированию объектов критической информационной инфраструктуры сферы здравоохранения. Версия 1.0 (утв. Министерством здравоохранения РФ 5 апреля 2021 г.)