МЕТОДИКА РАБОТ
ПО ОПРЕДЕЛЕНИЮ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И КАТЕГОРИЙ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Содержание

Перечень сокращений 3
Перечень терминов 4
1 ОБЩИЕ ПОЛОЖЕНИЯ 9
2 НОРМАТИВНЫЕ ССЫЛКИ 10
3 ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОПРЕДЕЛЕНИЮ ОСНОВАНИЙ ДЛЯ ОТНЕСЕНИЯ ИСИР ОИВ/ОРГАНИЗАЦИИ К ОБЪЕКТАМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ 11
3.1. Определение сфер деятельности организации. 11
3.2. Определение деятельности в организации по обеспечению взаимодействия объектов КИИ 12
4. МЕРОПРИЯТИЯ ПО ИНВЕНТАРИЗАЦИИ И КАТЕГОРИРОВАНИЮ ОБЪЕКТОВ КИИ 14
4.1. Инвентаризация объектов КИИ 14
4.1.2 Формирование перечня процессов 14
4.1.3 Определение критичности процессов 16
4.1.4 Формирование перечня объектов 16
4.2. Категорирование объектов КИИ 17
4.2.1 Анализ возможных действий нарушителей 18
4.2.2 Анализ угроз безопасности информации и типов компьютерных атак 18
4.2.3 Оценка масштаба последствий и соотнесение со значениями показателей категорий 18
4.2.4 Определение категории значимости объекта КИИ 20
4.2.6 Оформление акта категорирования объекта КИИ 20

Перечень сокращений

В настоящем документе используются сокращения, приведенные в таблице 1.

Таблица 1 − Перечень сокращений

Сокращение	Обозначение
АСУ	Автоматизированная система управления
ИС	Информационная система
ИСиР	Информационные системы и ресурсы
ИТКС	Информационно-телекоммуникационная сеть
КИИ	Критическая информационная инфраструктура
ЛВС	Локальная вычислительная сеть
ОКВЭД	Общероссийский классификатор видов экономической деятельности
ОКОГУ	Общероссийский классификатор органов государственной власти и управления
РФ	Российская Федерация
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных

Перечень терминов

В настоящем документе используются термины, приведенные в таблице 2.

Таблица 2 − Перечень терминов

Термин	Определение	Источник
Автоматизированная система управления	Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Безопасность информации	Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Безопасность критической информационной инфраструктуры	Состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Вредоносное программное обеспечение	Компьютерная программа, предназначенная для нанесения вреда (ущерба) владельцу (пользователю) компьютерной информации, хранящейся на средстве вычислительной техники, путем ее несанкционированного копирования, уничтожения, модификации, блокирования или нейтрализации используемых на средств защиты, или для получения доступа к вычислительным ресурсам самого средства вычислительной техники с целью их несанкционированного использования	Стандарт СТО.ФСБ.КК 1-2018 «Компьютерная экспертиза. Термины и определения»
Государственные информационные системы	Федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Термин	Определение	Источник
Доступ к информации	Возможность получения информации и ее использования	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Доступность информации (ресурсов информационной системы)	Состояние информации [ресурсов автоматизированной информационной системы], при котором субъекты, имеющие право доступа, могут реализовать их беспрепятственно	Р 50.1.056-2005 Техническая защита информации. Основные термины и определения
Значимый объект критической информационной инфраструктуры	Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Информационная система	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Информационно-телекоммуникационная сеть	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Инцидент информационной безопасности	Одно или несколько нежелательных или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности	ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

Термин	Определение	Источник
Компьютерная атака	Целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Компьютерный инцидент	Факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Критическая информационная инфраструктура	Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Нарушитель безопасности информации	Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации	ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
Несанкционированный доступ к информации	Доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или	Руководящий документ Защита от несанкционированного доступа к информации Термины и определения

Термин	Определение	Источник
	автоматизированными системами.	Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г.
Обладатель информации	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Объект критической информационной инфраструктуры	Информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления субъекта критической информационной инфраструктуры	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
Оператор информационной системы	Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Распространение информации	Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц	Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
Субъекты критической информационной инфраструктуры	Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым 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, в	Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Термин	Определение	Источник
	области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей	
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации	ГОСТ Р 50922-2006 Защита информации. Основные термины и определения
Целостность информации	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право	Р 50.1.056-2005 Техническая защита информации. Основные термины и определения

1 Общие положения

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.

Настоящий документ содержит методику работ по отнесению информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, принадлежащих на праве собственности, аренды или на ином законном основании к объектам критической информационной инфраструктуры с последующим установлением одной из категорий значимости объектов критической информационной инфраструктуры, либо решений об отсутствии оснований для их отнесения к объектам критической информационной инфраструктуры.

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).

В соответствии с требованиями 187-ФЗ, субъект КИИ обязан направить сведения о результатах категорирования своих объектов КИИ во ФСТЭК[1] России. Форма направления сведений определена приказом 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».

[1] Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

2 Нормативные ссылки

Настоящие Методические рекомендации разработаны с учетом требований законодательства Российской Федерации:

– 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»;

– 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.

3 Основные мероприятия по определению оснований для отнесения ИСиР организации к объектам критической информационной инфраструктуры

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.

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.
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.

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.

2. В случае выявления соответствующих объектов инфраструктуры, уточняем наличие у Организации явных поручений на уровне законодательных актов и нормативных требований, возлагающих на Организацию обязанности по обеспечению информационного взаимодействия между сторонними ИСиР. В случае наличия указанных обязательств, запрашиваем владельцев сторонних ИСиР 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.

Результат:

Заключение Рабочей группы о наличии/отсутствии оснований для отнесения ИСиР 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 организации к объектам критической информационной инфраструктуры в соответствии с законодательством Российской Федерации.

Заключение об отсутствии оснований может оформляться по консолидированной форме на все ИСиР организации сразу.

Желательно оформление отдельного заключения о наличии/отсутствии оснований по каждой информационной системе организации в отдельности.

4. Мероприятия по инвентаризации и категорированию объектов КИИ

4.1. Инвентаризация объектов КИИ

В случае принятия решения о наличии оснований для отнесения ИСиР 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».

4.1.2 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.

4.1.3 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.

4.1.4 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.

Результат:

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

№	*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*

Пример

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

Перечень объектов, подлежащих категорированию оформляется по форме, приведенной в таблице 4, рекомендованной ФСТЭК России. Утверждается и направляется в экспедицию центрального аппарата ФСТЭК России по адресу: 105066, г. Москва, ул. Старая Басманная, д. 17 на бумажном носителе и на электронном носителе информации.

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.

4.2. Категорирование объектов КИИ

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.

4.2.1 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.

4.2.2 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.

4.2.3 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 бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет Российской Федерации, осуществляемых субъектом критической информационной инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период);

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.

4.2.4 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).

Результат:

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

4.2.6 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.