Безопасность объектов критической информационной инфраструктуры организации

Общие рекомендации

(версия 2.0)

Москва, 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Принятый в середине 2017 года и вступивший в силу с 01 января 2018 года Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее по тексту - Закон «О безопасности КИИ») еще с самого выхода в свет породил массу вопросов, связанных с его практическим применением.

В этой связи, Ассоциацией руководителей служб информационной безопасности (АРСИБ) была выдвинута инициатива по созданию постоянно действующей рабочей группы и подготовке методического пособия рассчитанного на специалистов практиков, целью которого является формулировка рекомендаций (дорожной карты) для работников служб безопасности, информационной безопасности и подразделений информационно-технического обеспечения, дающих понимание того, что такое критическая информационная инфраструктура (далее по тексту – КИИ) и какие шаги необходимо предпринять для обеспечения безопасности КИИ на уровне организации.

В главах данного пособия, авторы, специалисты практики в сфере информационной безопасности, концентрируются на рассмотрении проблемных вопросов, касающихся практического применения Закона «О безопасности КИИ».

Как следует из определения, сформулированного в статье 2 Закона «О безопасности КИИ», КИИ представляет собой совокупность всех принадлежащих российским организациям, органам государственной власти, государственным учреждениям и индивидуальным предпринимателям объектов КИИ и обеспечивающих их взаимодействие сетей электросвязи.

В целом, алгоритм, связанный с обеспечением безопасности объектов КИИ в организации, можно представить следующим образом - Рисунок 1.

Рисунок 1. Дорожная карта по выполнению требований Федерального закона «О безопасности критической информационной инфраструктуры»

В соответствии с предложенной Дорожной картой, в главах данного пособия рассматриваются следующие вопросы:

- Сбор первичных данных о субъекте и объектах КИИ. Проблемы идентификации организации в качестве субъекта КИИ. Выявление различных видов объектов КИИ (главы 1 и 2).
- Проблемные вопросы категорирования объектов КИИ (глава 3)
- Обеспечение безопасности значимых объектов КИИ. Создание и функционирование системы обеспечения информационной безопасности (глава 4).
- Взаимодействие с ГосСОПКА в рамках исполнения обязанностей, возложенных на субъекта КИИ (глава 5)
- Аутсорсинг ИТ-услуг для субъектов КИИ (глава 6).

Данное пособие предназначено для работников субъектов КИИ, задействованных в процессах обеспечения безопасности объектов КИИ, а также может быть использовано при обучении и повышении осведомленности в вопросах безопасности КИИ иных работников.

ГЛАВА 1. СУБЪЕКТЫ КИИ: ПОНЯТИЕ, ОПРЕДЕЛЕНИЕ ПРИНАДЛЕЖНОСТИ

Понятие «субъект КИИ» содержится в статье 2 Закона «О безопасности КИИ». Под субъектами КИИ понимаются:

1. Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели (далее по тексту – организация):

- функционирующие в одной или нескольких сферах деятельности: здравоохранение, наука, транспорт, связь, энергетика, банковская сфера, сферы финансового рынка, топливно-энергетический комплекс, атомная энергетика, оборонная, ракетно-космическая, горнодобывающая, металлургическая и химическая промышленность;
- которым принадлежат (на праве собственности, аренды, ином законном основании) объекты КИИ.

2. Российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие систем и (или) сетей (ИС, ИТКС, АСУ) принадлежащих субъектам КИИ.

Таким образом, закон предусматривает два вида субъектов КИИ - владельцы объектов КИИ и координаторы взаимодействия этих объектов.

С точки зрения практического применения следует иметь в виду, что при определении является ли организация субъектом КИИ, необходимо оценивать именно ее сферу деятельности, а не сферу функционирования принадлежащих ей систем (ИС, АСУ, ИТКС).

При этом, важным становится вопрос о том, как определить ту сферу, в которой функционирует организация?

В качестве исходных данных для определения сферы функционирования организации, необходимо использовать учредительные документы, в которых содержатся заявленные ей виды экономической

деятельности, а также документы, дающие разрешение на право осуществления конкретного вида деятельности, т.е. лицензии.

Для определения к каким сферам относятся заявленные в уставных документах виды деятельности, целесообразно использовать Общероссийский классификатор видов экономической деятельности (ОКВЭД), который в качестве характерных черт видов экономической деятельности использует атрибуты, характеризующие сферу деятельности. Например, раздел J. «Деятельность в области информации и связи», очевидно, что если у организации в числе заявленных видов деятельности будут те, которые вошли в этот раздел, то она будет функционировать в сфере связи.

Помимо функционирования организации в одной или нескольких из перечисленных в Законе «О безопасности КИИ» сферах, необходимым условием является наличии у нее на праве собственности, аренды или ином законном основании (по сути владение на законном основании) ИС, АСУ или ИТКС. Если у организации таковых нет, например, она осуществляет заявленные виды деятельности без применения технологий автоматизации, то она не будет являться субъектом КИИ.

В целом, пошаговый алгоритм определение принадлежности организации (предприятия, учреждения и т.п.) к субъектам КИИ выглядит следующим образом:

1. Подготовить необходимый набор исходных документов для проведения анализа (см. рисунок 2).

• Устав организации • Положение об организации	Единый государственный реестр юридических лиц (ЕГРЮЛ) Единый государственный реестр индивидуальных предпринимателей (ЕГРИП)	Лицензии и иные разрешительные документы на осуществление конкретных видов деятельности (выполнение работ, оказание услуг).	Общероссийский классификатор видов экономической деятельности (ОКВЭД)

Рисунок 2. Набор документов для определения является ли организация субъектом КИИ

2. Уточнить коды ОКВЭД на выпускаемую продукцию, выполняемы работы, оказываемые услуги и т.п.
3. Составить сводную (инвентаризационную) таблицу всех принадлежащих организации систем: ИС, АСУ, ИТКС (таблица 1).

Таблица 1. Инвентаризационная таблица систем

№	Наименование ИС (АСУ, ИТКС)	ОКВЭД 2*	Относимость к КИИ**

Примечание к таблице:

* Код ОКВЭД 2 проставляется, если ИС (АСУ, ИТС и т.п.) участвует в создании продукции (сырья, услуг и т.п.) или обеспечивает взаимодействие таких ИС (АСУ, ИТС и т.п.).

** Отметка «Относимость к КИИ» ставится, если вид экономической деятельности по ОКВЭД попадает в перечисленную в п.8 ст. 2 Закона «О безопасности КИИ» сферу.

Таблица 2. Пример заполнения инвентаризационной таблицы систем

№	Наименование ИС (АСУ, ИТКС)	ОКВЭД 2*	Относимость к КИИ**
1	Бухгалтерия 1С	69.20.2	-
2	АСУ металлургического цеха	24.10.1	+
3	ИС конструкторского отдела	72.19.2	+
п/п…	ИС склада	52.10.9	-

Таким образом, указанная в примере организация будет являться субъектом КИИ, функционирующим в сферах металлургической промышленности и науки.

ГЛАВА 2. ОБЪЕКТЫ КИИ: ТИПЫ И ВИДЫ

Объекты КИИ - это имеющиеся у субъектов КИИ системы. Выделяют три вида систем:

- Информационная система (ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (статья 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Наиболее распространенными видами информационных систем являются государственные информационные системы (ГИС) и информационные системы персональных данных (ИСПДн).
- Информационно-телекоммуникационная сеть (ИТКС) - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (статья 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Самыми распространенными видами информационно-телекоммуникационных сетей являются корпоративные информационные сети и сеть международного обмена «Интернет».
- Автоматизированная система управления (АСУ). Один из видов автоматизированных систем. Автоматизированная система – это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90. Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения (утв. и введен в

действие Постановлением Госстандарта СССР от 27.12.1990 N 3399). Наиболее распространенными являются автоматизированные системы управления технологическими процессами (АСУТП) промышленных предприятий.

По мнению авторов, объекты КИИ можно классифицировать следующим образом:

1. По значимости, объекты КИИ подразделяются на следующие виды:

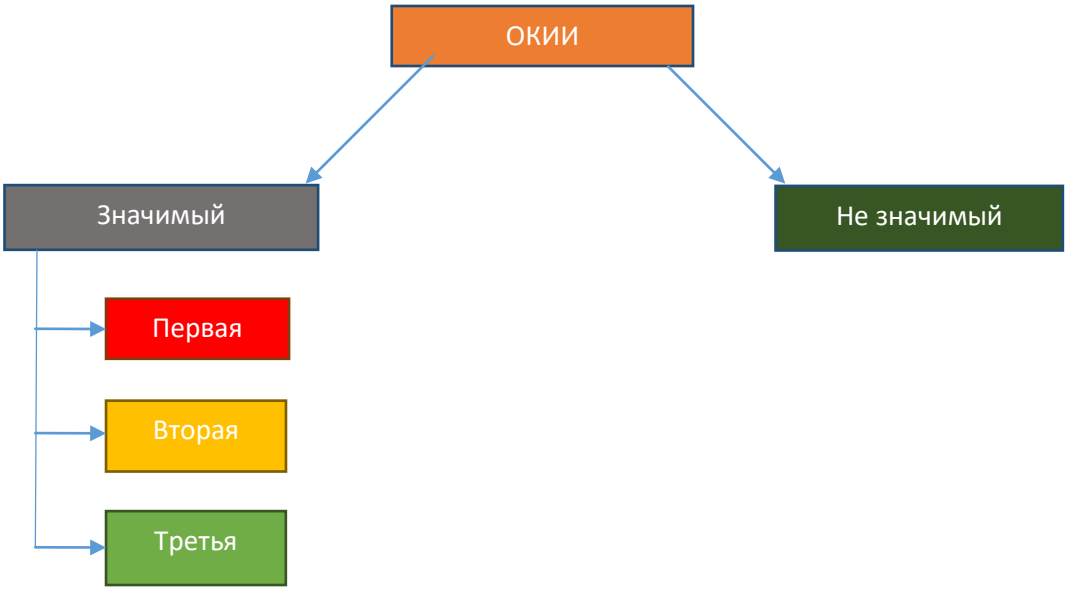

Рисунок 3. Классификация ОКИИ по значимости

С точки зрения значимости, объекты КИИ подразделяются на два вида: «значимый» и «не значимый», а значимые объекты делятся на три целевых уровня защищенности - «категории значимости» (в соответствии с ч. 3 ст. 7 Закона «О безопасности КИИ»): максимальный целевой уровень защищенности - первый, минимальный - третий.

От уровня защищенности значимого объекта КИИ, которому он должен соответствовать (т.н. «целевой уровень безопасности объекта защиты»), зависит набор организационных и технических мер, обеспечивающих блокирование (нейтрализацию) угроз безопасности информации, последствиями которых может быть прекращение или нарушение его функционирования.

Что касается объектов КИИ не отнесенных к значимым, то для них не требуется построения дополнительной системы безопасности, состав и содержание мер защиты информации для указанных объектов регламентирован в нормативно-правовых актах, регулирующих вопросы безопасности конкретного вида систем: ИСПДн, АСУТП и т.п.

При этом, помимо требований по обеспечению безопасности значимых объектов КИИ, действующее законодательство предусматривает права и обязанности субъектов КИИ (как владельцев значимых, так и не значимых объектов КИИ) которые закреплены в статье 9 Закона «О безопасности КИИ»:

Права субъекта КИИ:

1) получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации[1], информацию, необходимую для обеспечения безопасности значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или ином законном основании, в том числе об угрозах безопасности обрабатываемой такими объектами информации и уязвимостях программного обеспечения, оборудования и технологий, используемых на таких объектах;

2) в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской

---

1 В соответствии с Указом Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. № 1085» ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

Федерации[2], получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

3) при наличии согласия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Помимо прав, на все субъекты КИИ возлагаются следующие обязанности:

1) незамедлительно информировать о компьютерных инцидентах ФСБ России, а также Центральный банк Российской Федерации (в случае, если субъект критической информационной инфраструктуры осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном ими порядке;

2) оказывать содействие должностным лицам ФСБ России, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

---

2 В соответствии с Указом Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

С практической точки зрения, для выполнения возложенных на субъекта КИИ обязанностей, необходимо разработать регламент по реагированию на компьютерные инциденты (дополнить соответствующим разделом уже имеющийся регламент реагирования на инциденты информационной безопасности) в котором предусмотреть:

- алгоритм действий в случае нарушения функционирования объекта КИИ или безопасности, обрабатываемой таким объектом информации;
- порядок информирования ФСБ России и (или) Центрального банка РФ;
- правила взаимодействия и оказания содействия должностным лицам ФСБ России в ходе расследования инцидента и ликвидации его последствий.

Субъекты КИИ, которым принадлежат значимые объекты, также обязаны:

1. Соблюдать требования по обеспечению безопасности значимых объектов КИИ, установленные ФСТЭК России. Данные требования установлены приказом ФСТЭК России от 25.12.2017 № 239. В дальнейших параграфах данного пособия будут рассмотрены наиболее значимые из них.
2. Выполнять предписания должностных лиц ФСТЭК России, об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта КИИ, выданные этими лицами в соответствии со своей компетенцией. Данная обязанность предусматривает исполнение выданных по результатам государственного контроля (плановых и внеплановых проверок) предписаний об устранении выявленных нарушений. Порядок осуществления государственного контроля установлен Постановлением Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры».

3. Реагировать на компьютерные инциденты в порядке, утвержденном ФСБ России, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ. Для выполнения данной обязанности необходимо регламентировать (в разработанном и утвержденном локальном нормативном акте) план действий персонала в случае возникновения компьютерного инцидента, в том числе направленных на ликвидацию его последствий, а также регламент взаимодействия с ФСБ России (Национальным координационным центром по компьютерным инцидентам). Наиболее важные моменты осуществления взаимодействия будут рассмотрены в следующих главах.
4. Обеспечивать беспрепятственный доступ должностным лицам ФСТЭК России, к значимым объектам КИИ при реализации ими своих полномочий. В соответствии с постановлением Правительства РФ от 17 февраля 2018 г. № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» должностные лица ФСТЭК России при проведении проверок вправе:

- знакомиться с документами, касающимися обеспечения безопасности значимых объектов КИИ;
- получать доступ к значимым объектам КИИ и проводить оценку эффективности принимаемых мер по обеспечению безопасности с использованием сертифицированных программных и аппаратно-программных средств контроля, в том числе имеющихся у субъекта КИИ. Однако, следует отметить, что возможность и порядок использования таких средств контроля, проверяющие обязаны согласовать с руководителем субъекта КИИ или уполномоченным им должностным лицом. По оценкам экспертов, на практике, при проведении инструментального анализа защищенности, сотрудники

ФСТЭК России будут стараться использовать имеющиеся у субъекта КИИ средства контроля защищенности и просить обеспечить их функционирование работников субъекта.

2. По сфере функционирования можно выделить:

- здравоохранение;
- наука;
- транспорт;
- связь;
- энергетика;
- банковская сфера;
- сфера финансовых рынков
- топливно-энергетический комплекс;
- атомная энергетика;
- оборонная промышленность;
- ракетно-космическая промышленность;
- горнодобывающая промышленность;
- металлургическая промышленность;
- химическая промышленность.

С точки зрения практического применения следует учитывать, что, как правило, для конкретной сферы будет преобладающим какой-то один вид объекта КИИ (см. таблицу 1).

Таблица 3. Классификация объектов КИИ по сфере функционирования

ИС	АСУ	ИТКС
Здравоохранение Наука Транспорт Банковская сфера Иные сферы финансового рынка	Топливно-энергетический комплекс Энергетика Атомная энергетика Оборонная промышленность Ракетно-космическая промышленность Горнодобывающая промышленность Металлургическая промышленность Химическая промышленность	Связь

Пояснение к таблице: ИС - информационные системы; АСУ - автоматизированные системы управления; ИТКС - информационно-телекоммуникационные сети.

При «поиске» и категорировании объекта КИИ, следует обращать внимание на систему, характерную для сферы функционирования: с большей вероятностью именно она будет обрабатывать информацию, необходимую для обеспечения критических процессов, и (или) осуществлять управление, контроль или мониторинг критических процессов.

Рассмотрим в качестве примера сферу металлургии. Как правило, на металлургических предприятиях есть АСУ, которые осуществляют управление технологическими и (или) производственными процессами (АСУТП и АСУП), также есть информационные бухгалтерские системы по учету заработной платы и кадров. Оба класса систем функционируют в сфере металлургии и поэтому являются объектами КИИ.

Однако, нарушение и (или) прекращение работы АСУТП (АСУП), как правило, может привести к негативным социальным, экономическим, экологическим последствиям, а нарушение работоспособности ИС бухгалтерии, как правило, нет.

3. По виду системы объекты КИИ подразделяются на следующие виды:

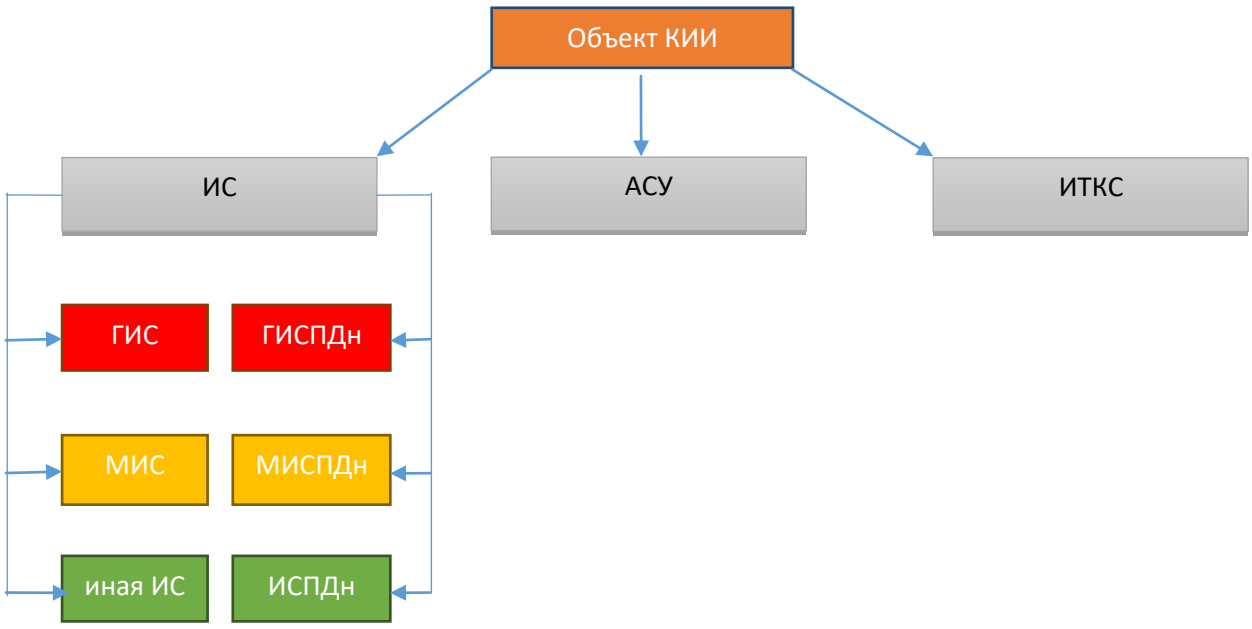

Рисунок 4. Классификация объектов КИИ по виду системы

Пояснение к рисунку: ГИС - государственная информационная система, МИС - муниципальная информационная система, ИСПДн - информационная система персональных данных, ГИСПДн - государственная информационная система персональных данных, МИСПДн - муниципальная система персональных данных.

С практической точки зрения важность правильного определения вида системы позволяет понять, какой перечень мер необходимо применять для обеспечения безопасности объекта КИИ (таблица 4).

В таблице 4 приведен перечень основных нормативно-правовых актов, предусматривающих меры обеспечения безопасности объектов КИИ. Следует отметить, что перечисленные в таблице нормативно-правовые акты, касающиеся иных ИС, не являются исчерпывающими - приведены лишь документы, регламентирующие требования к информационным системам, обрабатывающим наиболее распространенные виды тайн: коммерческая, налоговая, банковская.

Таким образом, правильное определение типа объекта КИИ позволяет определить набор мер, необходимых для создания системы безопасности, а также избежать ошибок при категорировании.

Таблица 4. Основные нормативно-правовые акты, устанавливающие меры защиты объекта КИИ

Не значимый						Значимый						
АСУ	149-ФЗ		31			149-ФЗ		31	235	239		
ИТКС	149-ФЗ		351			149-ФЗ		351	235	239		
ИС												
ГИС	149-ФЗ		17			149-ФЗ	17	235	239			
МИС	149-ФЗ		17			149-ФЗ	17	235	239			
Иные ИС	149-ФЗ	98-ФЗ	НК РФ	395-1	382-П	149-ФЗ	98-ФЗ	НК РФ	395-1	382-П	235	239
ГИС ПДн	149-ФЗ	152-ФЗ	1119	17	378	149-ФЗ	152-ФЗ	1119	17	378	235	239
МИС ПДн	149-ФЗ	152-ФЗ	1119	17	378	149-ФЗ	152-ФЗ	1119	17	378	235	239
ИС ПДн	149-ФЗ	152-ФЗ	1119	21	378	149-ФЗ	152-ФЗ	1119	21	378	235	239

Пояснение к таблице:

НК РФ - Налоговый кодекс Российской Федерации

98-ФЗ - Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

149-ФЗ - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

152-ФЗ - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

395-1 - Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»

1119 - Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

351 - Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

17 - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

21 - Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

31 - Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» и (или) Приказ ФСТЭК России от 28.02.2017 № 31 «Об утверждении Требований к обеспечению защиты информации, содержащейся в информационных системах управления производством, используемых организациями оборонно-промышленного комплекса».

235 - Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования»

239 - Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ»

378 - Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

382-П - Положение Банка России от 9 июня 2012 г. № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

В рамках предложенной типологии, отдельное внимание следует уделить такому виду объектов КИИ, как муниципальные информационные системы.

Дело в том, что органы местного самоуправления не являются субъектами КИИ:

- основной вид деятельности органов местного самоуправления (администраций) по ОКВЭД: 84.11.3 «Деятельность органов местного самоуправления по управлению вопросами общего характера».
- в соответствии с частью 4 статьи 34 Федерального закона от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» органы местного самоуправления не входят в систему органов государственной власти, т.е. не являются государственными органами.

При этом, следует иметь в виду, что муниципальные информационные системы не обязательно должны принадлежать органу местного самоуправления. Действующее законодательство не содержит прямого нормативного определения муниципальных информационных систем, а дает его косвенно, в форме классификации.

Так, в соответствии с ч. 1 ст. 13 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные системы включают в себя государственные, муниципальные и иные информационные системы. В свою очередь, муниципальные информационные системы – это информационные системы, созданные на основании решения органа местного самоуправления.

Таким образом, де-юре, безусловно, единственным определяющим признаком муниципальной информационной системы является ее создание на основании решения органа местного самоуправления.

При этом, согласно правоприменительной практике, под созданием, по сути, следует понимать правовое регулирование соответствующим нормативным актом.

Таким образом, муниципальная информационная система может принадлежать, по сути, любому российскому юридическому лицу, например, подведомственной организации или муниципально-частному партнеру.

ГЛАВА 3. КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КИИ

Определение термина «категорирование» содержится в ч. 1 ст. 7 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Под «категорированием» понимается установление соответствия объекта КИИ критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Таким образом, категорирование - это некая процедура, в ходе которой объект КИИ оценивается по некоторой совокупности показателей и исходя из значений этих показателей ему присваивается категория значимости, либо принимается мотивированное решение о ее отсутствии. На основании установленной категории значимости (при ее наличии) определяется базовый набор мер по обеспечению безопасности.

Процедура категорирования определяется Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 8 февраля 2018 г. № 127), далее по тексту – Правила категорирования.

Следует отметить, что Правила категорирования определяют именно процедуру категорирования и не дают толкование дефинициям «объект КИИ» и (или) «субъект КИИ», т.е. содержат нормы процессуального, а не материального права.

Авторы обращают внимание на важность данного момента, т.к. в практике им нередко приходилось сталкиваться с таким мнением, что ИС, АСУ или ИТКС, которые не обрабатывают информацию, необходимую для обеспечения критических процессов и не осуществляют управление, контроль или мониторинг критических процессов, якобы, не являются объектами КИИ. Данная точка зрения представляется неверной. Перечисленные системы являются объектами КИИ, однако они не подлежат

включению в перечень объектов КИИ, подлежащих категорированию и, соответственно, самому категорированию.

Процедуру категорирования можно схематично представить следующим образом (рисунок 5).

Рисунок 5. Проведение процедуры категорирования

В целом, проведение процедуры категорирования детально прописано в Постановлении 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», однако в рамках осуществления данной процедуры у субъектов КИИ, на практике возникает достаточно большое количество вопросов. Рассмотрим данную процедуру более подробно, сосредоточив внимание на проблемных вопросах, с которыми сталкивались авторы в процессе своей практической деятельности, и возможных путях их решения:

1. Формирование комиссии по категорированию. Первым шагом процедуры категорирования является создание комиссии по

категорированию, которая работает на постоянной основе и прекращает свою деятельность только в том случае, если организация прекращает быть субъектом КИИ - эти случаи перечислены в п.11.3 Правил категорирования. Комиссия создается приказом (пример приказа приведен в Приложении 5). При этом, поскольку комиссия постоянно действующая и должна осуществлять свою работу не только в процессе категорирования существующих на текущий момент объектов КИИ, но и при категорировании вновь создаваемых объектов КИИ, а также периодическом пересмотре категорий значимости (п. 21 Правил категорирования), по мнению авторов, необходимо регламентировать и планировать ее деятельность. Для этого следует разработать и поддерживать в актуальном состоянии План работы постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры, а также Положение о постоянно действующей комиссии по категорированию.

Проблемные вопросы, с которыми сталкиваются субъекты КИИ, при создании комиссии по категорированию:

- *Кто должен возглавлять комиссию по категорированию?* Пунктом 13 Правил категорирования установлено, что комиссию по категорированию возглавляет руководитель субъекта КИИ или уполномоченное им лицо. При этом, относительно того, кто должен быть уполномоченным лицом, единой позиции нет. Исходя из практического опыта авторов, можно сказать, что данным лицом является, как правило, работник, отвечающий за безопасность организации (руководитель службы безопасности, руководитель службы информационной безопасности, заместитель директора по безопасности и т.п.), либо главный инженер промышленного предприятия. По мнению авторов, уполномоченным лицом должен быть работник из числа топ менеджмента, в чьи функциональные обязанности входит курирование вопросов обеспечения безопасности.

- *Какие дополнительные специалисты должны входить в комиссию помимо перечисленных в п. 11 Правил категорирования?* Постановлением

Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127», Правила категорирования были дополнены пунктом 11.1. следующего содержания: «По решению руководителя субъекта критической информационной инфраструктуры в состав комиссии могут быть включены иные работники, в том числе работники финансово-экономического подразделения».

Указанное дополнение позволяет включать в комиссии всех имеющихся у субъекта КИИ специалистов, знания и навыки которых необходимы для корректного расчета и оценки показателей критериев значимости. Прежде всего это касается специалистов финансово-экономического подразделения, необходимых для расчета показателей экономической значимости (раздел 3) и представления их для рассмотрения членами комиссии по категорированию, а также специалистов юридических подразделений для проверки корректности соблюдения процедуры и оформления документов.

- *Можно ли создавать разные комиссии в филиалах территориально распределенной организации*?

Ранее уже упоминавшееся Постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127 дополнило Правила категорирования пунктом 11.2. следующего содержания: «По решению руководителя субъекта критической информационной инфраструктуры, имеющего филиалы, представительства, могут создаваться отдельные комиссии для категорирования объектов критической информационной инфраструктуры в этих филиалах, представительствах. В этом случае комиссия субъекта критической информационной инфраструктуры координирует и контролирует деятельность комиссий по категорированию».

На практике, ранее существовавшая проблема с необходимостью создания больших (по количеству участников) комиссий, теперь трансформировалась в проблему управления территориально

распределенными комиссиями и их контроля. Во избежание конфликтов между комиссией по категорированию субъекта КИИ и комиссиями по категорированию в филиалах (представительствах), связанных со сферами ответственности, по мнению авторов, целесообразно регламентировать функциональные обязанности, полномочия и ответственности в Положении о постоянно действующей комиссии по категорированию.

Этап 2. Подготовка перечня объектов КИИ подлежащих категорированию. В соответствии с п. 14 Правил категорирования для формирования перечня объектов КИИ подлежащих категорированию комиссии по категорированию необходимо:

а) определить процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта КИИ.

б) выявить те из них, которые являются критическими, т.е. их нарушение и (или) прекращение может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

в) выявить объекты КИИ, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, для включения в перечень объектов;

То есть, в перечень объектов КИИ, подлежащих категорированию, включаются только те объекты, которые обрабатывают информацию, необходимую для обеспечения критических процессов и (или) осуществляют их управление, контроль или мониторинг, а, следовательно, они и подлежат категорированию.

На практике, нередко возникает следующий вопрос *«что первично перечень объектов КИИ или перечень процессов?»*. Напомним, что в соответствии со ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» объекты КИИ - это ИС, ИТКС, АСУ субъектов КИИ и ничего

более. Иными словами, если даже объект КИИ не обеспечивает критические процессы, он, всё-таки, не перестает быть объектом КИИ. Поэтому, составление «перечня объектов КИИ» (не нужно путать с «перечнем объектов КИИ подлежащих категорированию») лежит вне рамок самой процедуры категорирования, а должно, по мнению авторов, предшествовать ей и проводится в процессе определения принадлежности организации к субъектам КИИ (см. главу 1)

В рамках же самой процедуры категорирования осуществляется выявление критических процессов, а затем из перечня объектов КИИ вычленяются объекты КИИ, подлежащие категорированию.

Как определить, относится процесс к критическим или нет? Поскольку категорированию подлежат только объекты КИИ, которые автоматизируют критические процессы, на практике перед субъектом КИИ встает вопрос о том, как определить, что тот или иной процесс является критическим.

Действующее законодательство в области КИИ не содержит методики выявления критических процессов, а значит, вопрос отнесения того или иного процесса к критическому остается исключительно на усмотрение субъекта КИИ.

В связи с этим возникают разные подходы к выявлению критических процессов:

1. Субъект может обосновать, что критические процессы у него отсутствуют, а, следовательно, нет и объектов КИИ подлежащих категорированию. Такой подход вполне может иметь практическое применение, однако, по мнению автора, при возникновении компьютерного инцидента с резонансными последствиями, субъект рискует быть подвергнут наказанию со стороны контрольно-надзорных органов.

2. К критическим следует относить полностью все процессы исходя из той логики, что нарушение какого-либо процесса может, прямо или косвенно, привести к возникновению неблагоприятных последствий (вреда).

Недостатком данного подхода, по мнению автора, является то, что при нем рассматриваются сценарии, возникновение которых на практике, весьма маловероятно. В результате, значимость объектов КИИ переоценивается.

3. К критическим относятся только те процессы, которые обеспечивают основные виды деятельности субъекта. Основные виды деятельности субъекта, как правило, содержатся в его уставных документах. Если следовать данному подходу, субъекту необходимо проанализировать Устав и ЕГРЮЛ и выделить в нем виды деятельности, задекларированные как основные. Далее для составления перечня объектов КИИ подлежащих категорированию следует определить, какие объекты участвуют в автоматизации указанных видов деятельности.

Наиболее близким к общей логика действующего законодательства является третий подход, с небольшим уточнением. Выявление критических процессов, по мнению авторов, должно базироваться на осуществляемых субъектом КИИ видах деятельности, и учитывать последствия, указанные в Перечне показателей критериев значимости объектов КИИ (утв. постановлением Правительства РФ от 08.02.2018 № 127):

- проводится идентификация управленческих, технологических, производственных, финансово-экономических и иных процессов в рамках осуществляемых видов деятельности: основного и дополнительных;
- из выявленных в п. 1 процессов определяются те, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

Этап 3. Категорирование (присвоение объекту КИИ категории, либо принятие мотивированного решения об отсутствии необходимости в ее присвоении).

Данный этап, по сути, разбивается еще на два самостоятельных этапа:

Этап 3.1. Рассмотрение возможных действий нарушителей в отношении объектов КИИ и анализ угроз безопасности.

В рамках данного этапа проводится рассмотрение возможных действий нарушителей и анализ угроз безопасности по отношению к имеющимся у организации объектам КИИ. Данный анализ может проводиться как на основании уже имеющихся для данных объектов моделей угроз и нарушителей, например, подготовленных ранее в рамках мероприятий по обеспечения безопасности персональных данных или автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, так и на основании описания возможных действий нарушителей и угроз безопасности объектам информатизации организации, содержащегося, например в Политике информационной безопасности организации.

При этом, на практике получило распространение такое мнение, что на этапе категорирования необходимо разработать модели угроз и нарушителей для каждого из объектов КИИ.

Нормативное требование по разработке модели угроз содержится в п. 11 Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», что свидетельствует о том, что разработка моделей угроз и нарушителей должна осуществляться в отношении значимых объектов КИИ, т.е. тех объектов в отношении которых уже завершена процедура категорирования и которым присвоена одна из категорий значимости.

Иными словами, не следует путать перечень возможных действий нарушителя и перечень актуальных угроз с моделями угроз и нарушителя. На этапе категорирования достаточно указанных перечней, подготовленных на основании уже имеющихся моделей, содержащихся в уже имеющихся

документах или составленных в рамках работы комиссии по категорированию, разработка же моделей угроз и нарушителей необходима перед проектированием системы обеспечения безопасности объектов, имеющих категорию значимости (см. главу 4).

Этап 3.2. Оценка объектов КИИ в соответствии с показателями критериев значимости и присвоение каждому из объектов КИИ категории, либо принятие решения об отсутствии необходимости ее присвоения.

На данном этапе комиссия оценивает объекты КИИ по всем показателям критериев значимости утвержденным постановлением Правительства РФ от 08.02.2018 № 127 и, в зависимости от полученных в ходе оценки значений, принимает решение о присвоении объекту КИИ одной из категории значимости, либо об ее отсутствии. Здесь следует отметить следующие важные, с практической точки зрения, моменты:

1. В практической деятельности получила распространение точка зрения о том, что категорий значимости четыре (0,1,2,3). Эта точка зрения ошибочна. Частью 3 ст. 7 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» устанавливается три категории значимости объектов критической информационной инфраструктуры - первая, вторая и третья.

Субъекты КИИ присваивают одну из категорий значимости объектам КИИ. Если объект КИИ не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий. Иными словами, можно говорить о том, что существует два вида объектов КИИ: «значимые» и «не значимые», а значимые объекты КИИ имеют три категории (см. главу 2).

2. Оценка каждого конкретного объекта КИИ по показателям критериев значимости осуществляется членами комиссии по категорированию, как правило (во всяком случае автор пока не встречал

иного), экспертным методом. Каких-либо утвержденных методик проведения расчетов по данным показателям, в настоящее время, нет.

При этом, перед проведение оценки в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры включенных в перечень объектов КИИ, подлежащих категорированию, рекомендуется провести оценку применимости указанных показателей к субъекту КИИ в целом, как в примере представленном в таблице 5, чтобы сразу же исключить те показатели, которые явно не будут применимы ни к одному из принадлежащих организации объектов КИИ.

Таблица 5. Пример анализа применимости показателей критериев значимости к субъекту КИИ

Показатель	**Критерии определения критичности**	**Применимость к субъекту КИИ**
Социальная значимость	Причинение ущерба жизни и здоровью людей	Критерий применим
	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения	Критерий применим.
	Прекращение или нарушение функционирования объектов транспортной инфраструктуры	Критерий неприменим. Субъект КИИ не предоставляет транспортные услуги.
	Прекращение или нарушение функционирования сети связи	Критерий неприменим. Субъект КИИ не предоставляет услуги связи.
	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в	Критерий неприменим. Субъект не предоставляет государственных услуг.

Показатель	Критерии определения критичности	Применимость к субъекту КИИ
	течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	
Политическая значимость	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	Критерий неприменим. Субъект КИИ не обеспечивает функционирование государственных органов.
	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации.	Критерий неприменим. Субъект КИИ не участвует в международной деятельности.
Экономическая значимость	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием	Критерий неприменим. Субъект КИИ не является государственной корпорацией, государственным унитарным предприятием, государственной компанией, стратегическим акционерным обществом, стратегическим предприятием, не входит в перечень стратегических предприятий и стратегических акционерных обществ.
	Возникновение ущерба бюджетам Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджеты Российской Федерации, осуществляемых субъектом критической информационной	Критерий применим.

Показатель	Критерии определения критичности	Применимость к субъекту КИИ
	инфраструктуры (процентов прогнозируемого годового дохода федерального бюджета, усредненного за планируемый трехлетний период)	
	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.	Критерий неприменим. Субъект КИИ не является финансово-кредитным учреждением, банком.
Экологическая значимость	Вредные воздействия на окружающую среду	Критерий применим
Значимость для	Прекращение или	Критерий неприменим. Субъект

Показатель	Критерии определения критичности	Применимость к субъекту КИИ
обеспечения обороны страны, безопасности государства и правопорядка	нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	КИИ не является пунктом управления или ситуационным центром.
	Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом КИИ	Критерий неприменим. Субъект не поставляет и не выпускает продукцию по государственным оборонным заказам.
	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка	Критерий неприменим. Субъект КИИ не эксплуатирует информационные системы в области обеспечения обороны страны, безопасности государства и правопорядка

Как осуществлять присвоение категории значимости объекту КИИ: с учетом мер защиты или без?

В настоящее время рядом экспертов высказывается мнение о том, что при присвоении объекту КИИ категории значимости, необходимо учитывать принятые на объекте меры защиты.

При этом, на практике, нередки ситуации, когда меры защиты изначально встроены в объект КИИ при его создании, реализуются с момента ввода его в эксплуатацию и не отделимы от объекта КИИ (архитектурные компоненты).

В то же время, согласно пп. «д» п. 5 Правил, оценка масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ производится в соответствии с перечнем показателей критериев значимости, и никак иначе.

Иными словами, реализация мер обеспечения информационной безопасности не оказывает влияние на присвоение объекту КИИ категории значимости. При определении категории значимости в расчет берутся последствия от уже реализованной гипотетической компьютерной атаки и сравниваются с перечнем показателей критериев значимости – какому показателю соответствует, такая категория и присваивается. Логика этого вполне очевидна и понятна, в расчет категории значимости берутся те последствия, к которым приведет успешная реализация в отношении объекта КИИ компьютерной атаки. В свою очередь, меры защиты лишь позволяют избежать указанной атаки или существенно затруднить ее реализацию и не могут влиять на причиненный в результате нее ущерб.

Этап 4. Подготовка итоговых документов по результатам категорирования. По итогам своей работы, комиссия по категорированию подготавливает два документа:

1. Акт о категорировании. Перечень информации о субъекте и объектах КИИ, которая должна быть включена в акт определяется п. 16 Правил категорирования.

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта КИИ и только им, т.е. председатель комиссии, осуществляет подписание акта и предоставляет его на утверждение руководителю организации. Если председатель комиссии по категорированию и руководитель организации одно и то же лицо, то акт будет содержать две его подписи: подпись председателя комиссии и гриф утверждения документа.

Субъект критической информационной инфраструктуры обеспечивает хранение акта до вывода из эксплуатации объекта критической

информационной инфраструктуры или до изменения категории значимости. Направление акта во ФСТЭК России не требуется.

2. Сведения о результатах присвоения объекту КИИ одной из категорий значимости, либо об отсутствии необходимости присвоения ему одной из таких категорий (далее по тексту – Сведения о категорировании). Данные сведения в течение 10 дней со дня утверждения акта направляются во ФСТЭК России. Форма сведений о категорировании утверждена приказом ФСТЭК России от 22.12.2017 № 236.

Таким образом, важно понимать, что акт категорирования и сведения о категорировании это два абсолютно разных документа и действия, осуществляемые с ними, также различны.

При этом, следует отметить следующие, важные с практической точки зрения, моменты:

- Сведения о категорировании по своему содержанию дублируют ту информацию, которая должна включаться в акт о категорировании в обязательном порядке. Поэтому, допустимо использовать формы сведений о категорировании при оформлении акта (актов). По сути, нужно просто поменять название документа и добавить подписи членов комиссии.
- Допускается оформление единого акта по результатам категорирования нескольких объектов КИИ, принадлежащих одному субъекту КИИ (п. 16 Правил категорирования), но при этом сведения о категорировании готовятся по установленной форме в отношении каждого из объектов КИИ и направляются в бумажной и электронной форме во ФСТЭК России.

Алгоритм направления сведений о категорировании во ФСТЭК России следующий:

- сведения о категорировании направляются во ФСТЭК России в бумажной (в одном экземпляре) и электронной форме по адресу: 105066, г. Москва, ул. Старая Басманная, д. 17;

- к направляемым во ФСТЭК России сведениям о категорировании в обязательном порядке готовится сопроводительное письмо (примерная форма приведена в Приложении 6), к нему прикладываются бумажные экземпляры сведений о категорировании, а также машинный носитель с их электронными копиями;
- если сведения о категорировании содержат информацию ограниченного доступа, то гриф (ограничительная пометка) проставляется в соответствии с порядком конфиденциального делопроизводства, утвержденным в организации.

Следует отметить, что в процессе работы комиссии, помимо актов и сведений могут появляться и иные документы, свидетельствующие о ее работе и соблюдении процедуры категорировании. Примерный перечень таких документов приведен в Приложении 3.

Сроки категорирования

Согласно п. 15 Правил максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом КИИ перечня объектов.

Постановлением Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» на субъектов КИИ, государственных органов и государственных учреждений, возложена обязанность утвердить перечень объектов КИИ, подлежащих категорированию до 1 сентября 2019 года. Таким образом, указанные субъекты КИИ обязаны завершить процедуру категорирования до 1 сентября 2020 года.

Относительно субъектов КИИ – российских юридических лиц и (или) индивидуальных предпринимателей, срок утверждения перечня объектов КИИ, подлежащих категорированию (до 1 сентября 2020 года) носит рекомендательный характер.

Таким образом, по мнению авторов, поскольку срок законодательно не установлен (не обязателен), субъект КИИ из числа российских юридических лиц и (или) индивидуальных предпринимателей, вправе сам выбирать приемлемый для него срок подготовки и отправки перечня. С учетом того, что формирование перечня объектов КИИ является одним из этапов процесса категорирования (п. 5 Правил категорирования) можно говорить о том, что, по сути, реальный срок категорирования в большинстве случаев будет превышать один год, а в ряде случаев будет составлять и несколько лет.

При этом, следует иметь в виду, что в ходе процедуры категорирования может измениться реестр объектов КИИ подлежащих категорированию, например, появятся новые объекты КИИ, либо часть будет выведена из эксплуатации и т.п. Результатом чего может стать несовпадение информации, содержащейся в итоговых документах категорирования и направленном ранее во ФСТЭК России перечне объектов КИИ, что, по мнению авторов, непременно повлечет вопросы регулятора.

Действующее законодательство не предусматривает обязанность субъекта по направлению измененного перечня объектов КИИ, однако, по мнению автора, во избежание претензий регулятора, целесообразно подготовить новую редакцию перечня, пояснительную записку с приложением приказов о вводе в эксплуатацию (выводе из эксплуатации) объекта КИИ и направить весь этот комплект документов регулятору совместно со сведениями о категорировании.

ГЛАВА 4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Основываясь на материале предыдущих глав, мы определили, что организация относится (или нет) к субъектам КИИ, провели категорирование и установили категории значимости принадлежащим ей объектам КИИ. Следующим шагом является создание системы обеспечения информационной безопасности значимых объектов КИИ, т.н. «СОИБ ЗОКИИ».

Целью СОИБ ЗОКИИ является обеспечение его устойчивого функционирования. Средства и методы должны соответствовать категории значимости, необходимо следить за их адекватностью для противодействия текущим угрозам и угрозам завтрашнего дня. Система обеспечения безопасности, запущенная однажды, закончит функционирование только в процессе вывода значимого объекта КИИ из эксплуатации. Всё промежуточное время СОИБ эволюционирует и развивается. В целом алгоритм создания и функционирования СОИБ ЗОКИИ можно представить следующим образом (рисунок 6).

Рисунок 6. – Алгоритм создания и функционирования СОИБ ЗОКИИ

Согласно представленному на рисунке 6 алгоритму, стадией, предшествующей созданию СОИБ ЗОКИИ, является категорирование: именно на данной стадии мы определяем необходимость создания СОИБ (есть или нет ЗОКИИ), выявляем сами объекты защиты, определяем их целевой уровень безопасности (категорию значимости).

Следующей стадией идет непосредственно **создание СОИБ ЗОКИИ**, состоящее из следующих этапов:

Этап 1. Планирование. На данном этапе устанавливаются требования, которые необходимо выполнить для обеспечения безопасности каждого ЗОКИИ и формируется план мероприятий.

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» ФСТЭК России устанавливает требования по обеспечению безопасности ЗОКИИ.

Требования к созданию СОИБ ЗОКИИ установлены приказом ФСТЭК России от 21 декабря 2017 г. № 235, в котором определены состав сил

обеспечения информационной безопасности их структура и функции, требования к ним. Что важнее всего, им вменяется в обязанности «проводить анализ угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры и выявлять уязвимости в них». Это не творческий процесс, а показатель квалификации специалистов, уровня их осведомленности об уязвимостях, знаний об угрозах. Ошибочные или недостаточные результаты анализа приведут к неверной реализации СОИБ КИИ.

Определены требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности ЗОКИИ.

Отдельное внимание уделено организационно-распорядительным документам по безопасности ЗОКИИ, которые являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта КИИ. При этом, положения, определяющие порядок и правила обеспечения безопасности ЗОКИИ, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования ЗОКИИ. Примерный состав организационно-распорядительных документов субъекта КИИ приведен в Приложении 3.

Приказом ФСТЭК России от 25 декабря 2017 г. № 239 утверждены требования по обеспечению безопасности ЗОКИИ.

Одним из ключевых и проблемных на практике требований, установленных данным приказом, является моделирование угроз безопасности ЗОКИИ. Проблема в том, что на сегодняшний день утвержденная методика по моделированию угроз и действий нарушителей для объектов КИИ отсутствует.

ФСТЭК России в Информационном сообщении от 4 мая 2018 г. № 240/22/2339 сообщает, что в связи с внесением изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004

г. № 1085, и определением ФСТЭК России федеральным органом исполнительной власти, уполномоченным в области безопасности критической информационной инфраструктуры, с 1 января 2018 г. ФСТЭК России утратила полномочия в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

Учитывая изложенное, в соответствии с решением директора ФСТЭК России от 3 мая 2018 г. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 18 мая 2007 г., и Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 19 ноября 2007 г., признаны утратившими силу.

При этом Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., а также Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., могут применяться субъектами КИИ:

- для моделирования угроз безопасности информации на ЗОКИИ;
- до тех пор, пока ФСТЭК России не утверждены аналогичные методические документы по безопасности объектов КИИ.

При этом следует отметить, что информационные сообщения не являются нормативно-правовыми актами и не имеют юридической силы.

Приказом ФСТЭК России от 25.12.2017 г. № 239 (п.11.1) утверждены требования к содержанию модели угроз для ЗОКИИ, в соответствии с которыми модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта.

В свою очередь описание каждой угрозы безопасности информации должно включать:

- источник угрозы безопасности информации;
- уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;
- возможные способы (сценарии) реализации угрозы безопасности информации;
- возможные последствия от реализации (возникновения) угрозы безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации должен использоваться банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России.

Таким образом, по сути п. 11.1 Приказа ФСТЭК России от 25.12.2017 г. № 239 устанавливает требования и подходы, которыми необходимо руководствоваться при моделировании угроз безопасности ЗОКИИ.

При этом, по мнению авторов, опираться на методики и базовые модели угроз разработанные ФСТЭК России для ключевых систем информационной инфраструктуры на текущий момент стратегически не верно, т.к. методические документы в части моделирования угроз безопасности информации объектов КИИ, которые планируются к утверждению ФСТЭК России (согласно Информационному сообщению от 4 мая 2018 г. № 240/22/2339) будут опираться на требования, действующего законодательства по безопасности КИИ, в частности Приказа ФСТЭК России от 25.12.2017 г. № 239, а, следовательно, подготовленные модели угроз и нарушителей безопасности для ЗОКИИ, после утверждения методических документов, потребуют уточнения, а не полного пересмотра.

Кроме того, важно отметить, что модель угроз безопасности информации может разрабатываться для нескольких ЗОКИИ, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы

безопасности информации, что достаточно удобно, когда число ЗОКИИ составляет несколько сотен или даже тысяч.

После определения актуальных угроз, перед проектированием СОИБ ЗОКИИ необходимо проведение т.н. «диагностического аудита» (в общей теории менеджмента более известного как «GAP анализ»), целью которого является определение тех мер по защите информации, которые уже приняты в отношении данного объекта КИИ, и тех, которые необходимо будет реализовать в процессе создания СОИБ.

Для проведения указанного аудита необходимо взять весь перечень ЗОКИИ, и сопоставить уже принятые меры по обеспечению безопасности каждого из объектов КИИ с мерами, перечисленными в приказе ФСТЭК России от 25 декабря 2017 г. № 239: первоначально определить, какие меры выполняются, а какие нет (по принципу - «да»/«нет»), затем понять как и насколько полно они выполняются.

Результатом проведения «Диагностического аудита» будет являться понимание того, какая часть обязательных мер по обеспечению безопасности «значимого» объекта КИИ уже реализована, а какая требует реализации в процессе создания СОИБ, какая часть мер может быть «закрыта» встроенными средствами защита, а для какой потребуется применение наложенных.

По итогам проведенного анализа и формирования требований к СОИБ ЗОКИИ подготавливается и утверждается руководителем субъекта КИИ план мероприятий по обеспечению безопасности ЗОКИИ (п. 29-31 приказа ФСТЭК России от 21 декабря 2017 г. № 235).

Этап 2. Реализация. На данном этапе осуществляется внедрение организационных и технических мер, реализация плана мероприятий по обеспечению безопасности ЗОКИИ (п. 34 приказа ФСТЭК России от 21 декабря 2017 г. № 235).

Организационные и технические меры по обеспечению безопасности ЗОКИИ (состав подробно приведен в приложении к приказу ФСТЭК России № 239 от 25 декабря 2017 г.):

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);
- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- реагирование на инциденты информационной безопасности (ИНЦ);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

Приказ ФСТЭК России от 26 марта 2019 № 60 (о внесении изменений в Приказ от 25 декабря 2017 № 239) внес изменения в т.н. «нулевые меры»: заменил требования по «разработке политик» на требования по «регламентации правил и процедур». Кроме того, в защиту машинных носителей информации (ЗНИ) добавились съемные машинные носители информации. Немного уменьшили количество мер в базовом наборе для объектов первой категории значимости. Однако, входящие в состав значимого объекта первой категории значимости программные и

программно-аппаратные средства, осуществляющие хранение и обработку информации, теперь должны размещаться на территории Российской Федерации.

Приказ ФСТЭК России от 9 августа 2018 г. № 138 внес изменения в требования приказов ФСТЭК России № 31 и № 239 исключив разночтение состава мер защиты информации.

Сравним меры приказов ФСТЭК России № 239, № 31 и № 17 (таблица 6):

Таблица 6. - Сравнительный анализ мер приказов ФСТЭК России № 239/31/17

Приказ ФСТЭК России № 239	**Приказ ФСТЭК России № 31**	**Приказ ФСТЭК России № 17**
ИАФ	ИАФ	ИАФ
УПД	УПД	УПД
ОПС	ОПС	ОПС
ЗНИ	ЗНИ	ЗНИ
АУД	АУД	**РСБ**
АВЗ	АВЗ	АВЗ
СОВ	СОВ	СОВ
ОЦЛ	ОЦЛ	**АНЗ**
ОДТ	ОДТ	ОЦЛ
ЗТС	ЗТС	ОДТ
ЗИС	ЗИС	**ЗСВ**
ИНЦ	**ИНЦ**	ЗТС
УКФ	**УКФ**	ЗИС
ОПО	**ОПО**	
ПЛН	**ПЛН**	
ДНС	**ДНС**	
ИПО	**ИПО**	

Пояснение к таблице:
Зелёным общее для 239 и 31 и 17
Синим - общее для 239 и 31
Красным - оригинальное для 17

Углубимся в пункты, по которым наблюдаются различия (см. таблицу 7):

Таблица 7. – Сравнение приказа ФСТЭК России №237 и приказа ФСТЭК России № 17.

Из приказа ФСТЭК № 239	Из приказа ФСТЭК № 17
V. Аудит безопасности (АУД)	***V. Регистрация событий безопасности (РСБ)***
Регламентация правил и процедур аудита безопасности	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
Инвентаризация информационных ресурсов	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
Анализ уязвимостей и их устранение	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
Генерирование временных меток и (или) синхронизация системного времени	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти
Регистрация событий безопасности	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
Контроль и анализ сетевого трафика	Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления
Защита информации о событиях безопасности	Защита информации о событиях безопасности
Мониторинг безопасности	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей
Реагирование на сбои при регистрации событий безопасности	***VIII. Контроль (анализ) защищенности информации (АНЗ)***

Из приказа ФСТЭК № 239	Из приказа ФСТЭК № 17
Анализ действий пользователей	Разработка правил и процедур (политик) контроля (анализа) защищенности
Проведение внутренних аудитов	Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей
Проведение внешних аудитов	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
XIV. Управление обновлениями программного обеспечения (ОПО)	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
Регламентация правил и процедур управления обновлениями программного обеспечения	Контроль состава технических средств, программного обеспечения и средств защиты информации
Поиск, получение обновлений программного обеспечения от доверенного источника	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей
Контроль целостности обновлений программного обеспечения	***XI. Защита среды виртуализации (ЗСВ)***
Тестирование обновлений программного обеспечения	
Установка обновлений программного обеспечения	

Таким образом, по итогам анализа требований приказов ФСТЭК России № 239, № 31, № 17 можно сделать следующий вывод: если у субъекта КИИ уже в полном объеме реализованы меры приказа ФСТЭК России от 14 марта 2014 г. № 31 (с изменениями приказа ФСТЭК от 9 августа 2018 г. №138), обеспечить соответствие приказу ФСТЭК России от 25 декабря 2017 г. № 239 будет не сложно (обращаем внимание на внесенные изменения).

Труднее придется субъектам КИИ, выполнившим лишь требования приказа ФСТЭК России от 11 февраля 2013 г. № 17. Им потребуется реализовать ряд обеспечительных мер:

- планирование мероприятий по обеспечению безопасности (ПЛН);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- реагирование на инциденты информационной безопасности (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

Приказом ФСТЭК России от 27 марта 2019 г. № 64 (о внесении изменений в Приказ ФСТЭК России от 21 декабря 2017 №235) закреплена ответственность за обособленные подразделения (филиалы, представительства). Системы обеспечения информационной безопасности создаются с учетом ЗОКИИ в обособленных подразделениях.

Кроме того, с 01.01.2021 вводятся требования квалификации и стажа для специалистов по безопасности: «наличие у руководителя структурного подразделения по безопасности высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе профессиональной переподготовки по направлению «Информационная безопасность» (со сроком обучения не менее 360 часов), наличие стажа работы в сфере информационной безопасности не менее трех лет.

Наличие у штатных работников структурного подразделения по безопасности, штатных специалистов по безопасности высшего профессионального образования по направлению подготовки (специальности) в области информационной безопасности или иного высшего профессионального образования и документа, подтверждающего прохождение обучения по программе повышения квалификации по

направлению «Информационная безопасность» (со сроком обучения не менее 72 часов);

Прохождение не реже одного раза в 5 лет обучения по программам повышения квалификации по направлению «Информационная безопасность». Таким образом, у субъекта КИИ есть небольшой запас времени в срочном порядке подтянуть персонал на соответствие требованиям.

СОИБ ОКИИ не завершается стадией реализации, мы не просто наблюдаем за ней – необходимы постоянный контроль и регулярное совершенствование системы. Причем, это требования самого Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (статья 4) - принципами обеспечения безопасности критической информационной инфраструктуры, в том числе, является непрерывность и комплексность.

Опираясь на данный принцип, **функционирование СОИБ ЗОКИИ** строится с использованием классического «цикла совершенствования», более известного в теории менеджмента как «Цикл Деминга» или «PDCA»: «планирование» - «реализация» - «мониторинг и контроль» - «совершенствование».

При этом, стадии «планирования» и «реализации» характерны как для вновь создаваемой СОИБ, так и для уже функционирующей.

Этап 3. Мониторинг и контроль. Ключевым для данного этапа, по мнению авторов, является аудит информационной безопасности.

По сути, основная цель проведения аудита информационной безопасности, определить, какое положение дел в области обеспечения информационной безопасности существует сейчас и какие дальнейшие действия необходимо предпринять для создания либо улучшения системы защиты информации.

Схематично этапы проведения аудита информационной безопасности можно представить в следующем виде - рисунок 7. Данная

последовательность действий выработана на основе ГОСТ Р ИСО 19011-2012 и опыта авторов.

В части организации и проведения аудита информационной безопасности ЗОКИИ необходимо обратить внимание на следующие моменты:

1. Обязательность проведения аудита информационной безопасности ЗОКИИ.

Согласно п. 35 и п. 36 «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» (утв. приказом ФСТЭК России от 21 декабря 2017 г. № 235) в рамках контроля состояния безопасности ЗОКИИ должен осуществляться внутренний контроль организации работ по обеспечению их безопасности, и эффективности принимаемых организационных и технических мер.

В ходе проведения контроля проверяется выполнение требований нормативных правовых актов в области обеспечения безопасности КИИ, а также организационно-распорядительных документов по безопасности ЗОКИИ, иными словами, проводится т.н. «Комплаенс аудит».

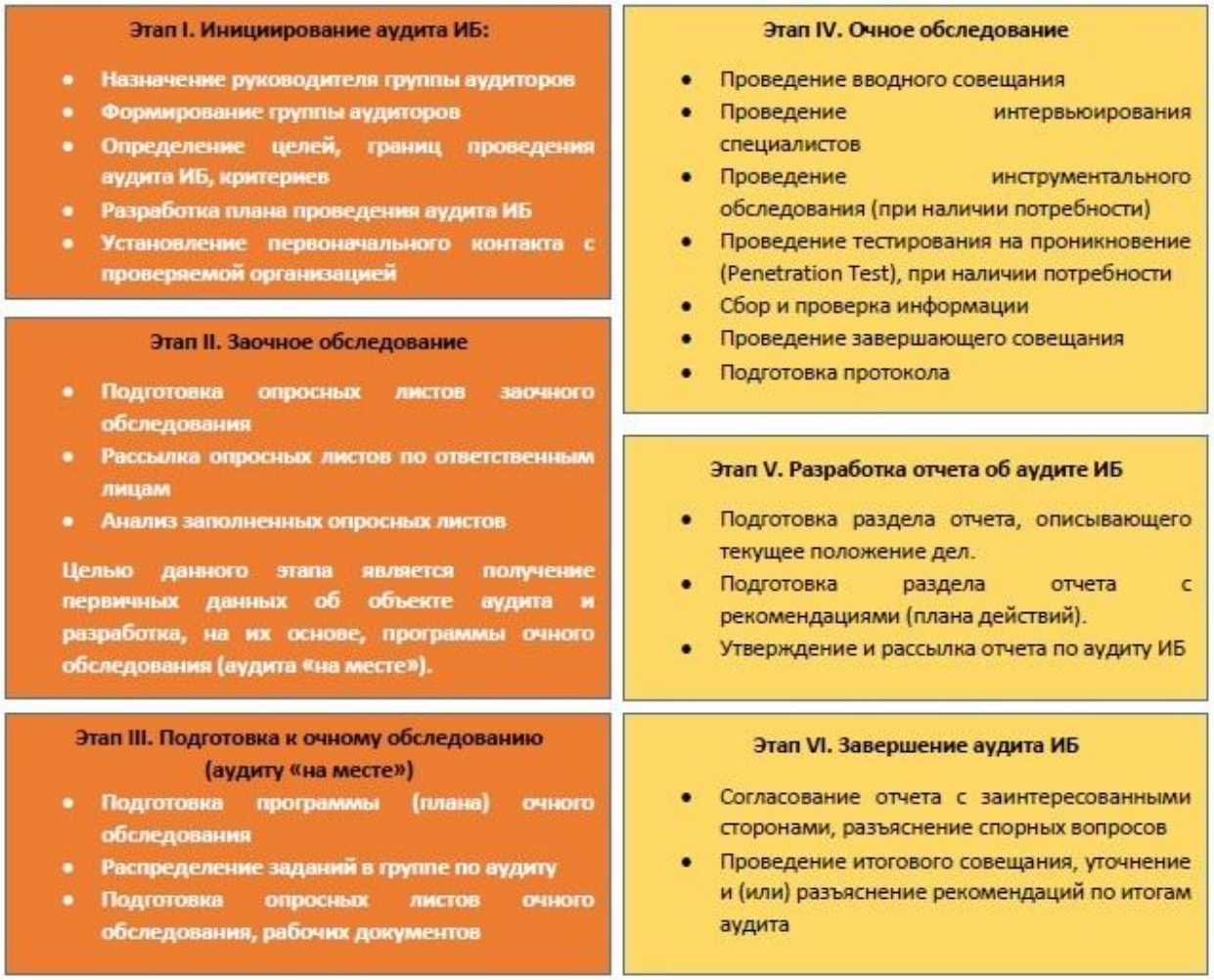

Рисунок 7. – Этапы проведения аудита ИБ

Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности ЗОКИИ могут применяться средства контроля (анализа) защищенности – это т.н. «Инструментальный аудит» (анализ защищенности).

Контроль проводится ежегодно комиссией, назначаемой субъектом КИИ. В случае проведения по решению руководителя субъекта КИИ внешней оценки (внешнего аудита) состояния безопасности ЗОКИИ внутренний контроль может не проводиться.

Замечания, выявленные по результатам внутреннего контроля или внешней оценки (внешнего аудита), подлежат устранению в порядке и сроки, установленные руководителем субъекта КИИ (уполномоченным лицом).

Таким образом, законодательно предусмотрена обязательность проведения аудита информационной безопасности ЗОКИИ в форме внутреннего аудита, проводимого силами работников субъекта КИИ, либо внешнего аудита, проводимого специализированной организацией.

2. Уверенность в том, что объект КИИ действительно хорошо защищен и вероятность возникновения компьютерного инцидента мала может обеспечить только проведение инструментального аудита (анализ уязвимостей), включающего тестирование на проникновение (Penetration Test).

Анализ уязвимостей ЗОКИИ является обязательным как на этапе создания (до ввода в эксплуатацию), так и в ходе его эксплуатации (п. 12.6., п.13, п. 13.2., п. 13.8 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утв. приказом ФСТЭК России от 25 декабря 2017 г. № 239).

Анализ уязвимостей проводится в целях выявления недостатков (слабостей) в подсистеме безопасности ЗОКИИ и оценки возможности их использования для реализации угроз безопасности информации.

При этом, важно обратить внимание на то, что согласно вышеупомянутым требованиям, анализу подлежат уязвимости кода, конфигурации и архитектуры значимого объекта.

Анализ уязвимостей проводится для всех программных и программно-аппаратных средств, в том числе средств защиты информации ЗОКИИ.

По результатам анализа уязвимостей должно быть подтверждено, что в ЗОКИИ, отсутствуют уязвимости, как минимум содержащиеся в банке данных угроз безопасности информации ФСТЭК России, или выявленные уязвимости не приводят к возникновению угроз безопасности информации, а в идеале, чтобы тестирование на проникновение подтвердило отсутствие возможности успешного проведения компьютерной атаки со стороны потенциального злоумышленника.

При проведении анализа уязвимостей применяются следующие способы их выявления:

- анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности;
- анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации;
- выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством анализа состава установленного программного обеспечения и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации;
- выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности;
- тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

Применение способов и средств выявления уязвимостей осуществляется с учетом особенностей функционирования ЗОКИИ.

Таким образом, проведение аудита ИБ является базовой мерой обеспечения безопасности для ЗОКИИ, влияющей на принятие решения о модернизации СОИБ. Результаты аудита, как правило, составляют основу для формирования технического задания и технического проектирование необходимых систем (подсистем) защиты или доработки существующих.

Этап 4. Совершенствование. Система защиты должна противостоять угрозам не только сегодня, но и завтра. Кроме того, не достаточно одного лишь факта внедрения процессов, обеспечивающих функционирование

системы безопасности, процессы должны непрерывно совершенствоваться, повышая свою зрелость (см. таблицу 8).

Таблица 8. - Уровень зрелости процессов информационной безопасности по методологии ISF (Information Security Forum)

Уровень	Обозначение уровня зрелости	Описание
0	Несуществующий	Процесс ИБ не выполняется
1	Примитивный	Процесс ИБ выполняется на нерегулярной основе
2	Начальный	Процесс ИБ выполняется на регулярной основе и поддерживается на уровне планирования (включая привлечение заинтересованных сторон и использование соответствующих стандартов и руководств)
3	Формализованный	Процесс ИБ выполняется, планируется и имеется достаточный объем организационных ресурсов для поддержки и управления
4	Управляемый	Процесс ИБ выполняется, планируется, управляется и контролируется
5	Оптимизированный	Процесс ИБ выполняется, планируется, управляется, измеряется при помощи количественных показателей (метрик) и постоянно совершенствуется

В рамках совершенствования безопасности ЗОКИИ структурное подразделение по безопасности, специалисты по безопасности должны проводить анализ функционирования системы безопасности и состояния безопасности ЗОКИИ, по результатам которого разрабатывать предложения по развитию системы безопасности и меры по совершенствованию безопасности ЗОКИИ.

Процесс совершенствование выражается в осязаемом виде: разработка предложений по корректировке плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак реализуется в виде - Перечня предложений. Модернизация

(совершенствование) систем безопасности значимых объектов КИИ в виде - Плана модернизации.

Силы СОИБ проходят регулярное повышение квалификации. Средства СОИБ обновления, не забывая про исключение влияния подсистемы безопасности на функционирование значимого объекта. Организационно-распорядительная документация – обновление и приведение в соответствие законам и подзаконным нормативным актам.

ГЛАВА 5. ВЗАИМОДЕЙСТВИЕ С ГОССОПКА

В целях выполнения требований статьи 5 и 9 Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и **в соответствии с**:

- Указом Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
- Концепцией государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - ГосСОПКА), утвержденной Президентом Российской Федерации 12.02.2014 г. № К1274.
- Указом Президента Российской Федерации от 22.12.2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».
- Методическими рекомендациями ФСБ России от 24.12.2016 г. № 149/2/7-200 «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (далее - Методические рекомендации).

субъекту КИИ необходимо обеспечить взаимодействие с ГосСОПКА по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

В сфере функционирования ГосСОПКА применяются следующие **основные термины и определения:**

- ГосСОПКА представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
- Под информационными ресурсами Российской Федерации понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.
- К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся:

  - подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА;

  - организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования ГосСОПКА, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее - НКЦКИ);

  - подразделения и должностные лица субъектов КИИ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.
- Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на

компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

Нормативно-правовые акты по вопросам взаимодействия с ГосСОПКА

- Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам».
- Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (далее - Приказ ФСБ России № 367).
- Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области

реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (далее - Приказ ФСБ России № 368).

- Приказ ФСБ России от 06.05.2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».
- Приказ ФСБ России от 19.06.2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации».
- Приказ ФСБ России от 19.06.2019 г. № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (далее - Приказ ФСБ России № 282).
- Методические рекомендации по обнаружению компьютерных атак на информационные ресурсы (предоставляется по запросу в НКЦКИ).
- Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов (предоставляется по запросу в НКЦКИ).

- Методические рекомендации по проведению мероприятий по оценке степени защищенности от компьютерных атак (предоставляется по запросу в НКЦКИ).
- Требования к подразделениям и должностным лицам субъектов ГосСОПКА (предоставляется по запросу в НКЦКИ).
- Типовой Регламент взаимодействия при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак (предоставляется по запросу в НКЦКИ).

Структура ГосСОПКА

Основной организационно-технической составляющей ГосСОПКА являются центры обнаружения, предупреждения и ликвидации последствий компьютерных атак, организованные по ведомственному и территориальному принципам.

Центры подразделяются на главный центр ГосСОПКА, региональные центры, территориальные центры, центры органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (далее - ведомственные центры) и корпоративные центры.

Главный центр ГосСОПКА, региональные и территориальные центры ГосСОПКА создаются силами ФСБ России. Зоной ответственности данных центров являются информационные ресурсы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (далее - органы государственной власти), а также информационные ресурсы указанного федерального органа исполнительной власти.

Главным центром ГосСОПКА является Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ). Официальный адрес сайта в сети Интернет НКЦКИ: http://gov-cert.ru/.

Ведомственные центры создаются заинтересованными органами государственной власти. Зоной ответственности таких центров являются принадлежащие органам государственной власти информационные ресурсы.

Также, ведомственные центры могут создаваться и эксплуатироваться в интересах органов государственной власти, организациями, осуществляющими лицензируемую деятельность в области защиты информации. Функционирование ведомственного центра обеспечивается органом государственной власти, создавшим этот центр.

Корпоративные центры могут создаваться государственными корпорациями, операторами связи и другими организациями, осуществляющими лицензируемую деятельность в области защиты информации. Функционирование корпоративного центра обеспечивается организацией, создавшей такой центр.

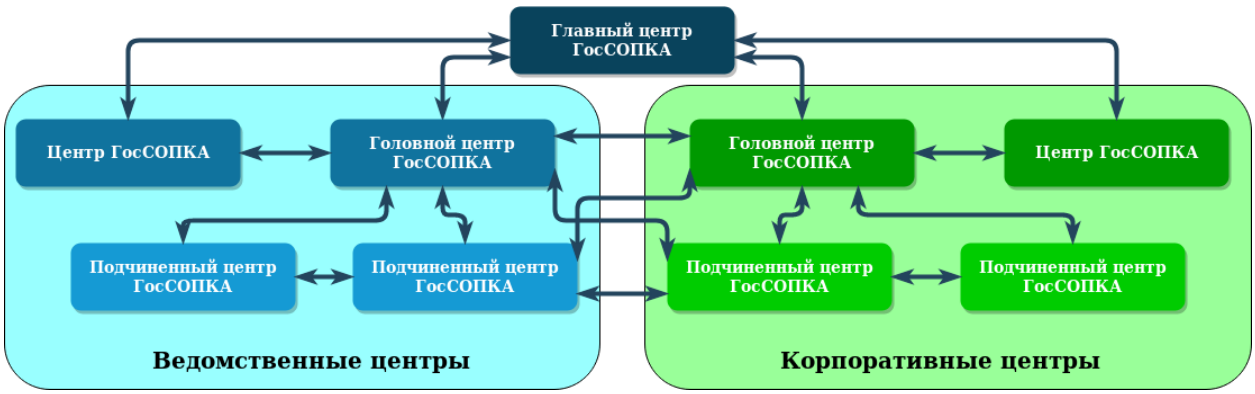

Рисунок 8. Структура ГосСОПКА

К основным задачам центров ГосСОПКА относятся:

- Обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы.
- Проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;

- Проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы.
- Сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах.
- Осуществление взаимодействия между центрами.
- Информирование заинтересованных лиц и субъектов ГосСОПКА по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Взаимодействие субъекта КИИ с ГосСОПКА возможно в двух вариантах:

- Создать и организовать взаимодействие собственного ведомственного (корпоративного) центра (сегмента) ГосСОПКА.
- Организовать взаимодействие через ведомственный (корпоративный) центр (сегмент) ГосСОПКА (возложение части функций субъекта КИИ на внешнего контрагента).

Создание и организация взаимодействия собственного ведомственного (корпоративного) центра (сегмента) ГосСОПКА включает следующие мероприятия:

- Направить запрос в НКЦКИ на получение Методических рекомендаций с описанием инициативы по созданию ведомственного (корпоративного) центра (сегмента) ГосСОПКА и приложением копий лицензий ФСБ России и ФСТЭК России в области защиты информации.
- После получение Методических рекомендаций разработать пакет документов (положение о ведомственном (корпоративном) центре (сегменте) ГосСОПКА с отражением класса центра, регламент деятельности центра, штатное расписание центра и должностные инструкции специалистов центра) в соответствии с Требованиями к

подразделениям и должностным лицам субъектов ГосСОПКА и направить его в НКЦКИ.

- Заключить соглашение с НКЦКИ о взаимодействии ведомственного (корпоративного) центра (сегмента) ГосСОПКА в области обнаружения, предупреждения и ликвидации последствий компьютерных атак.
- Выполнить организационные и технические требования к процессам, персоналу, технологиям при создании центра (сегмента) ГосСОПКА в соответствии с нормативными правовыми актами по вопросам взаимодействия с ГосСОПКА.
- Развернуть специализированные средства взаимодействия сегмента ГосСОПКА с главным или головным центром ГосСОПКА (в приоритете для значимых объектов КИИ).

Организация взаимодействия через ведомственный (корпоративный) центр (сегмент) ГосСОПКА (возложение части функций субъекта КИИ на внешнего контрагента) включает следующие мероприятия:

- Заключить соглашение (договор) со сторонней организацией, осуществляющей лицензируемую деятельность в области защиты информации, в рамках которой функционирует ведомственный (корпоративный) центр (сегмент) ГосСОПКА, который будет выполнять возлагаемые субъектом КИИ функции (в предмете соглашения должны быть прописаны конкретные решаемые задачи) согласно пункту 7.3.3 Методических рекомендаций.
- Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности ведомственного (корпоративного) центра ГосСОПКА.

Базовый комплект документации ведомственного (корпоративного) центра (сегмента) ГосСОПКА:

- Положение о ведомственном (корпоративном) центре (сегменте) ГосСОПКА.

- Штатное расписание ведомственного (корпоративного) центра (сегмента) ГосСОПКА.
- Должностные инструкции специалистов ведомственного (корпоративного) центра (сегмента) ГосСОПКА.
- Регламент реагирования на компьютерные инциденты.
- План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее - План реагирования).
- Перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных атак.
- Журнал учета компьютерных инцидентов (в случае отсутствия средства учета и обработки компьютерных инцидентов (IRP-система).
- План проведения тренировки по отработке мероприятий Плана реагирования.
- Перечень информации, передаваемой в ГосСОПКА.
- Регламент взаимодействия при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак (взаимодействие с ГосСОПКА и (или) субъектами КИИ).
- Заявка в ФСБ России на согласование установки средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее — Средства ОПЛ).
- Информационное письмо в НКЦКИ о приемке в эксплуатацию Средств ОПЛ.
- Регламент по порядку доступа к эксплуатируемым Средствам ОПЛ.
- Документация на Средства ОПЛ (договора, накладные, формуляры, сертификаты, акты установки, эксплуатационная документация, приказ об организации хранения средств).

Схема взаимодействия с ГосСОПКА

В соответствии с Приказами ФСБ России № 282, 367, 368 определена схема взаимодействия с ГосСОПКА, которая представлена на рисунке № 9 и описана в Таблице № 9. При организации взаимодействия с ГосСОПКА необходимо также учитывать Типовой Регламент взаимодействия при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также Требования к подразделениям и должностным лицам субъектов ГосСОПКА.

Взаимодействие с ГосСОПКА возможно следующими способами:

1. С использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ.

2. В случае отсутствия подключения к технической инфраструктуре, информация передается субъектом КИИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: http://cert.gov.ru.

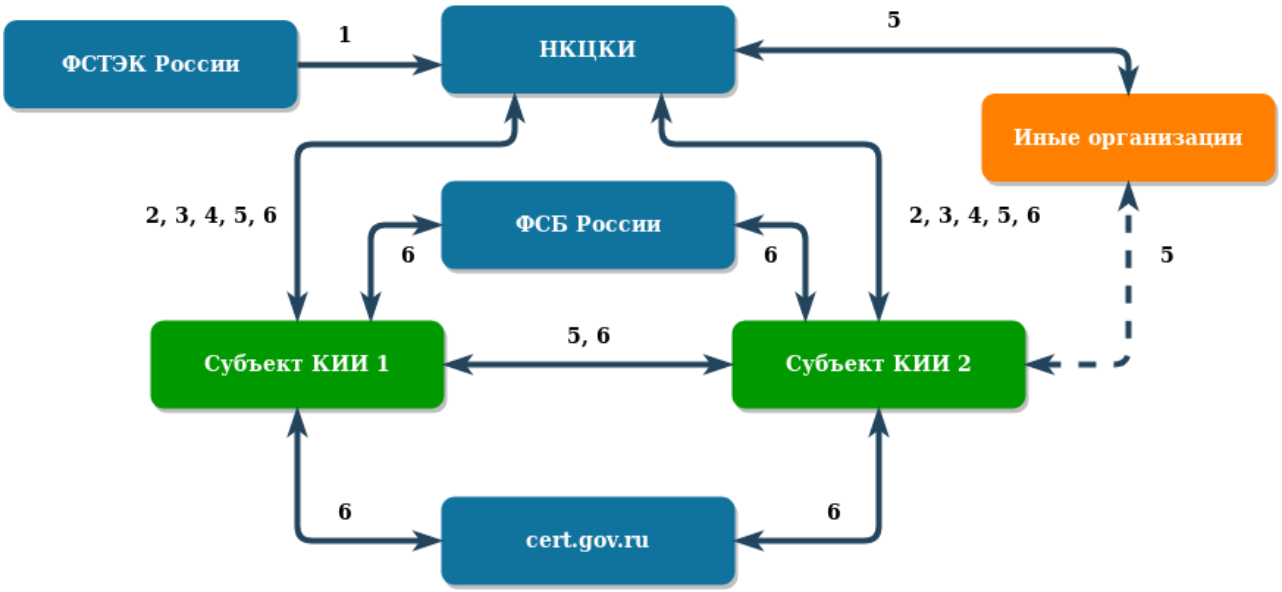

Рисунок № 9. Схема взаимодействия с ГосСОПКА

Под иными организациями, указанными на схеме, подразумеваются: уполномоченные органы иностранных государств, международные, международные неправительственные организации и иностранные организации, осуществляющие деятельность в области реагирования на компьютерные инциденты.

Таблица № 9. Описание схемы взаимодействия с ГосСОПКА

№ п/п	Описание передаваемой информации	Срок	Требования нормативных правовых актов
1	Информация, указанная в п. 1-4 Перечня информации, утв. Приказом ФСБ России № 367	Не реже 1 раза в месяц и не позднее месячного срока (при выполнении условий)	п. 1 Порядка представления информации, утв. Приказом ФСБ России № 367
2	Информация о компьютерных инцидентах (п. 5 Перечня информации, утв. Приказом ФСБ России № 367)	3 часа для значимого объекта КИИ 24 часа для иных объектов КИИ	п. 4 Порядка информирования ФСБ России, утв. Приказом ФСБ России № 282 п. 5-6 Порядка представления информации, утв. Приказом ФСБ России № 367
3	Информация о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак	48 часов	п. 14 Порядка информирования ФСБ, утв. Приказом ФСБ России № 282
4	Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (п. 6 Перечня информации, утв. Приказом ФСБ России № 367)	Достаточный для своевременного реагирования на компьютерные инциденты	п. 7-9 Порядка представления информации, утв. Приказом ФСБ России № 367
5	Информация о компьютерных инцидентах (п. 5 Перечня информации, утв. Приказом ФСБ России № 367)	Достаточный для своевременного реагирования на компьютерные инциденты	Порядок обмена информацией о компьютерных инцидентах, утв. Приказом ФСБ России № 368
6	Информации о средствах и способах проведения компьютерных атак и о методах их предупреждения	Не позднее 24 часов с момента получения НКЦКИ такой информации.	Порядок получения субъектами КИИ информации о средствах и способах проведения компьютерных атак, утв.

№ п/п	Описание передаваемой информации	Срок	Требования нормативных правовых актов
	и обнаружения	Достаточный для своевременного реагирования на компьютерные инциденты	Приказом ФСБ России № 368

ГЛАВА 6. АУТСОРСИНГ УСЛУГ

По-прежнему много вопросов вызывает вопрос отнесения организации к субъектам КИИ при предоставлении ИТ-услуг по сервисной модели. Основные типы таких организаций:

- облачные провайдеры, которые являются операторами связи;
- облачные провайдеры, оказывающие услуги по моделям IaaS[3], PaaS[4], SaaS[5];
- дата-центры, предоставляющие сервис colocation[6].

6.1. Является ли субъектом КИИ облачный провайдер?

Если аутсорсер (облачный провайдер) является оператором связи, то он однозначно относится к субъектам КИИ в соответствии с ФЗ-187. Если нет, то, по мнению автора, все зависит от модели предоставления услуг.

Дата-центры, предоставляющие сервис colocation, не являются субъектом КИИ. Организации субъекты КИИ, размещающие в дата-центре свое оборудование, должны прописать в договорах требования к аутсорсеру (например, по доступности, обеспечению непрерывности функционирования каналов связи, систем охлаждения и электропитания) в соответствии с ФЗ-187 и подзаконными актами для своих объектов КИИ и регламент проведения проверок выполнения этих требований. Если коммерческий дата-центр не принимает мер по соблюдению требований 187-ФЗ, то размещать в нем объекты КИИ нельзя.

Облачные провайдеры, предлагающие услуги по модели IaaS так же не являются субъектами КИИ. А развертывающим на их инфраструктуре свои

---

3 IaaS (Infrastructure as a Service) - инфраструктура как услуга.
4 PaaS (Platform as a Service) - платформа как услуга
5 SaaS (Software as a Service) - программное обеспечение как услуга
6 Размещение оборудования в дата центре

ИС субъектам КИИ следует выставить требования как к дата-центру, так и к используемой ИТ-инфраструктуре.

Сложнее ситуация с облачными провайдерами, предлагающими услуги по моделям PaaS и SaaS. Здесь надо смотреть на конкретные платформы и сервисы. Например, предлагаемая по модели PaaS система 1С может рассматриваться как принадлежащий облачному провайдеру объект КИИ. Некоторые банки полностью перенесли в «облако» свои автоматизированные банковские системы (АБС). Соответственно облачный провайдер, предлагающий АБС по модели SaaS, является владельцем КИИ и тоже попадает под действие соответствующего законодательства.

Кроме того, в случае с операторами IaaS-, PaaS- и SaaS-услуг нужно обратить внимание на код ОКВЭД-2 63.11 «Деятельность по обработке данных, предоставление услуг по размещению информации и связанная с этим деятельность», который входит в раздел «Деятельность в области информации и связи». Использование кода ОКВЭД-2 может быть основанием для отнесения облачного провайдера к субъектам КИИ.

Облачным провайдерам необходимо заранее обратить внимание на требования по обеспечению ИБ (в первую очередь, на приказы ФСТЭК № 235 от 21.12.2007 и № 239 от 25.12.2017), выполнение которых может потребовать дополнительных затрат, в том числе и временных (например, в случае размещения субъекта КИИ с самой высокой категорией значимости).

6.2 Может ли субъект КИИ полностью переложить ответственность на аутсорсера?

Даже полный переход на использование модели SaaS не спасет банк от необходимости проводить работу по ФЗ-187, хотя и облегчит ему жизнь, так как основные работы по выполнению обеспечения безопасности лягут на облачного провайдера. То же можно сказать и про компании, выделившие свои ИТ-подразделения на инсорсинг.

Формально они могут защищать свою позицию перед регулятором. В соответствии со ст. 2 № 187-ФЗ к субъектам критической инфраструктуры относятся российские юридические лица, «которым на праве собственности, аренды или на ином законном основании **принадлежат** информационные системы …», а в случае передачи КИИ на баланс инсорсинговой компании, компания под определение субъекта КИИ не подходит, даже если ее деятельность попадает в список указанных ФЗ-187 отраслей.

Однако, в случае выставленных претензий предстоит непростой судебный процесс с регулятором, а как показывает практика, суды чаще прислушиваются к его мнению. Например, регулятор может посчитать частью ИС терминал, через который сотрудники компании удаленно подключаются к дата-центру облачного провайдера или инсорсинговой компании.

Таким образом, на сегодняшний день, нельзя дать однозначный ответ на вопрос отнесения к субъектам КИИ организаций, оказывающих услуги в части предоставления вычислительных мощностей. Представляется, что более-менее приемлемый ответ на данный вопрос возможно будет получить по прошествии некоторого времени, когда появится практика прохождения контрольно-надзорных мероприятий.

ЗАКЛЮЧЕНИЕ

В данном пособии авторы постарались в сжатой форме изложить основные положения вступившего в законную силу с 01 января 2018 года Федерального закона «О безопасности критической информационной инфраструктуры» и принятых во исполнении него подзаконных нормативно правовых актов. При этом, основной акцент в процессе рассмотрения был сделан на встречавшихся в практике авторов проблемных вопросах, с учетом которых формулировались основанные на своей, возможно пока и небольшой, практике рекомендации по обеспечению безопасности объектов КИИ, так как основная идея авторов пособия заключалась в том, чтобы создать некое наставление, которое бы позволило совершить меньше ошибок.

Данное пособие подготовлено коллективом авторов - членов Ассоциации руководителей служб информационной безопасности:

Глава 1 – Константин Саматов, Михаил Кашаев

Глава 2 - Константин Саматов

Глава 3 - Лев Палей, Константин Саматов

Глава 4 - Радмир Нафиков, Константин Саматов

Глава 5 - Александр Мишурин

Глава 6 - Николай Носов

Приложения 2,6 – Константин Саматов

Приложения 3,4,5 – Михаил Кашаев

Редакционная коллегия: Виктор Минин, Сергей Петренко, Сергей Чучаев, Александр Полещук, Кристина Костромина.

Данный материал - это описание опыта и знаний авторов, которыми они поделились. Здесь собрано то, что было осмыслено, понято, что было опробовано на практике и принесло нужный результат. Но не всё. В следующем «издании» будет еще больше практического материала, работа

над проблематикой КИИ указанного коллектива авторов не является законченной. Созданная на базе Ассоциации руководителей служб информационной безопасности рабочая группа продолжит свою работу в данном направлении и поделится результатами с сообществом специалистов в области информационной безопасности в следующей версии данного пособия.

В планах рабочей группы периодически перевыпускать данную методичку, постепенно ее расширяя и дополняя новыми материалами. В основном практическими материалами, но где есть необходимость и теоретическими (для лучшего понимания проблематики). Какова будет периодичность выхода «реинкарнаций» пока точно неизвестно: возможно раз в полгода или раз в год – это зависит от объемов новых материалов и объемов изменений. Точно можно сказать только одно – пособие всегда будет распространяться бесплатно. Также, Ассоциация не делает никаких ограничений на распространение данного материала, в его исходном виде.

За помощь в подготовке данного пособия, АРСИБ выражает огромную благодарность работникам 2 Управления ФСТЭК России, а также 8 Центра ФСБ России.

ПРИЛОЖЕНИЕ 1. ОТВЕТЫ РЕГУЛЯТОРА НА СПОРНЫЕ ВОПРОСЫ

Данные ответы получены на официальный запрос АРСИБ во ФСТЭК России:

Вопрос 1: Каким образом желательно составить перечень по системам (ИС, ИТКС, АСУ)? Например, автоматизированные системы цеха оставить полностью (АСУ Цеха) или стоит все-таки делить по агрегатам (АСУ агрегата1, АСУ агрегата2 и т.д.)?

Ответ: Решение о степени детализации объектов критической информационной инфраструктуры принимается субъектом критической информационной инфраструктуры самостоятельно с учетом определений терминов «информационная система», «информационно-телекоммуникационная сеть» и «автоматизированная система управления», приведенных в пунктах 3 и 4 статьи 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в пункте 1 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ), а также на основании эксплуатационной и технической документации на указанные объекты критической информационной инфраструктуры.

Вопрос 2: Необходимо составлять перечень абсолютно всех систем предприятия, в том числе и самых незначительных?

Ответ: В соответствии с подпунктами «а» - «г» пункта 5 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. №127 (далее – Правила), в перечень объектов критической информационной инфраструктуры, подлежащих категорированию, включаются только объекты критической информационной инфраструктуры, реализующие управленческие,

технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка, оцениваемым в соответствии с Перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значениями, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 127.

Вопрос 3: При определении критичности объектов какой временной диапазон необходимо взять для оценки ущерба?

Ответ: При оценке критичности объекта в соответствии с подпунктом «д» пункта 5 Правил необходимо рассматривать последствия компьютерных инцидентов, наступивших в течении максимального периода времени, требуемого на восстановление штатных (проектных) параметров работы объекта критической информационной инфраструктуры.

Вопрос 4: Что делать с объектами КИИ не имеющими категорию значимости: как их учитывать, как это фиксировать, оформлять и т.п.?

Ответ: В соответствии с пунктом 16 Правил решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте критической информационной инфраструктуры (в том числе об объекте, в отношении которого принято решение об отсутствии необходимости присвоения категории значимости), результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории

значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

В соответствии с пунктом 17 Правил субъект критической информационной инфраструктуры направляет в ФСТЭК России сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Вопрос 5: Верно ли утверждение, что критичность процесса должна оцениваться Субъектом КИИ с точки зрения возникновения при их нарушении и (или) прекращении последствий социального, политического, экономического, экологического характера или последствий для обеспечения обороны страны, безопасности государства и правопорядка? (критерии, определенные в ПП-127)

Ответ: В соответствии с пунктом 5 Правил критические процессы – это управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

Таким образом, определение критичности процесса - это оценка возможности возникновения каких-либо негативных социальных, политических, экономических, экологических последствий для обеспечения обороны страны, безопасности государства и правопорядка в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры.

Вопрос 6: Выделенный на предприятии Объект КИИ должен иметь документально зафиксированные границы и подтверждение создания (например, «Акт о введении системы Х в эксплуатацию», проект с описанием

ее архитектуры), или допускается объединять несколько отдельных систем в один объект КИИ? В случае, если допускается объединение, описание вновь созданного Объекта КИИ должно фиксироваться документально (например, в Техническом паспорте Объекта КИИ, Отчете об инвентаризации и т.д.) или достаточно приказа Комиссии по категорированию, где зафиксировано решение об объединении?

Ответ: Решение о возможности рассмотрения нескольких информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления субъекта критической информационной инфраструктуры в качестве одного объекта критической информационной инфраструктуры принимается субъектом критической информационной инфраструктуры в соответствии с критериями, приведенными в пункте 1 настоящего документа.

При этом информация о рассмотрении нескольких информационных систем, информационно-телекоммуникационных сетей или автоматизированных систем управления в качестве одного объекта критической информационной инфраструктуры должна содержаться в сведениях о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Вопрос 7: В п.6.2 Сведений (форма утверждена приказом ФСТЭК России № 236) указано, что следует перечислить основные угрозы безопасности. Под основными понимаются все актуальные угрозы в соответствии с Банком данных угроз ФСТЭК России, или допускается делать выборку наиболее критичных угроз среди актуальных?

Ответ: В соответствии с Формой направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденной приказом ФСТЭК России от 22 декабря 2017 г. № 236, в пункте 6.2 сведений о результатах присвоения

объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий под основными угрозами безопасности информации понимаются все угрозы безопасности информации, признанные комиссией по категорированию актуальными.

Вопрос 8: Перечень основных угроз безопасности информации в п.6.2 Сведений (форма утверждена приказом ФСТЭК России №236) необходимо приводить в виде полного наименования угроз или достаточно указать идентификатор УБИ.Х в соответствии с Банком данных угроз ФСТЭК России?

Ответ: В соответствии с Формой направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденной приказом ФСТЭК России от 22 декабря 2017 г. № 236, в пункте 6.1 сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий достаточно указать идентификаторы основных угроз безопасности информации в соответствии с Банком данных угроз безопасности информации.

Вопрос 9: Следует ли заполнять п.9 «Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ» Сведений (форма утверждена приказом ФСТЭК России №236) при передаче сведений об объекте КИИ, которому не была присвоена категория значимости?

Ответ: В соответствии с подпунктом «и» пункта 17 Правил в составе сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий приводятся организационные и технические меры, применяемые для обеспечения

безопасности объекта критической информационной инфраструктуры, либо информация об отсутствии необходимости применения указанных мер.

Учитывая изложенное, вне зависимости от того, присвоена ли объекту критической информационной инфраструктуры категория значимости, в пункте 9.1 сведений о результатах присвоения ему одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий в соответствии с Формой направления сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденной приказом ФСТЭК России от 22 декабря 2017 г. № 236, указываются организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта), а в пункте 9.2 – технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25 декабря 2017 г. № 239.

Вопрос 10: В п.9 «Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ» Сведений (форма утверждена приказом ФСТЭК России №236) необходимо указывать только меры, выполненные в полном объеме? Или меры, выполненные частично, также можно приводить с указанием степени (границ) выполнения?

Ответ: В соответствии с Формой направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденной приказом ФСТЭК России от 22

декабря 2017 г. № 236, в разделе 9 сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий указываются только принятые организационные и технические меры по обеспечению безопасности значимого объекта критической информационной инфраструктуры.

В случае, если мера не реализована (например, проекты регламентов, инструкций, руководств разработаны, но не утверждены, или средства защиты информации установлены, но не настроены), она не является принятой и не указывается в разделе 9 указанных сведений.

В случае, если мера реализована, но частично (например, в части выполнения меры ИПО.0 «Разработка политики информирования и обучения персонала» разработана, утверждена и внедрена политика информирования персонала, но политика обучения персонала не реализована, или в части выполнения меры ИАФ. 1 «Идентификация и аутентификация пользователей и инициируемых ими процессов» осуществляется идентификация и аутентификация пользователей, но не осуществляется идентификация и аутентификация процессов, инициируемых пользователями), она является принятой. В данном случае в разделе 9 указанных сведений приводится информация о степени реализации меры (например, «разработана, утверждена и внедрена политика информирования персонала по вопросам обеспечения безопасности значимых объектов критической информационной инфраструктуры» и «осуществляется идентификация и аутентификация пользователей»).

Вопрос 11: В случае, если какие-либо технические меры из п.9 «Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта КИИ» Сведений (форма утверждена приказом ФСТЭК России №236) закрыты компенсирующими

организационными мероприятиями, сведения об этих мерах надо приводить в п.9.2 или переносить в п.9.1?

Ответ: В соответствии с Формой направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденной приказом ФСТЭК России от 22 декабря 2017 г. № 236, в пункте 9.1 сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий указываются только принятые организационные меры обеспечения безопасности значимого объекта критической информационной инфраструктуры, а в пункте 9.2 – только принятые технические меры.

Вопрос 12: При изменении какого-либо пункта Сведений (форма утверждена приказом ФСТЭК России №236) – например, сведений о применяемых мерах защиты (ведь планируется постепенное создание полноценной системы защиты информации), либо при выводе объекта КИИ из эксплуатации, каков для Субъекта КИИ порядок информирования ФСТЭК России об этих изменениях? Какой приемлемый период для информирования о происшедших изменениях?

Ответ: В соответствии с законодательством о безопасности критической информационной инфраструктуры сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий представляются в ФСТЭК России только в следующих случаях:

- присвоение или не присвоение категории значимости объекту критической информационной инфраструктуры в соответствии с частью 4 статьи 7 Федерального закона № 187-ФЗ;

- устранение в соответствии с частью 9 статьи 7 Федерального закона № 187-ФЗ выявленных ФСТЭК России недостатков в результате проверки сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, осуществленной в соответствии с частью 6 статьи 7 Федерального закона № 187-ФЗ;

- изменение категории значимости значимого объекта критической информационной инфраструктуры в одном из случаев, приведенных в части 12 статьи 7 Федерального закона № 187-ФЗ;

- пересмотр установленной категории значимости значимого объекта критической информационной инфраструктуры в соответствии с пунктом 21 Правил.

В указанных случаях сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий представляются в ФСТЭК России в сроки, предусмотренные Федеральным законом № 187-ФЗ и Правилами.

Законодательством о безопасности критической информационной инфраструктуры информирование ФСТЭК России об изменениях сведений об объекте критической информационной инфраструктуры в иных случаях не предусмотрено.

Вопрос 13: Категория значимости может быть изменена в случае изменения значимого объекта (№187-ФЗ, ст.12, п.12,2). О какого рода изменениях идет речь?

Ответ: В соответствии с пунктом 2 части 12 статьи 7 Федерального закона № 187-ФЗ в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория

значимости, категория значимости, к которой отнесен указанный объект критической информационной инфраструктуры, может быть изменена.

К таким изменениям могут относиться любые изменения, оказывающие влияние на масштаб возможных последствий по показателям критериев значимости объектов критической информационной инфраструктуры, приведенных в Перечне показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденных постановлением Правительства Российской Федерации от 8 февраля 2018 г. №127, в случае возникновения компьютерных инцидентов на значимом объекте критической информационной инфраструктуры

Вопрос 14: Порядок обработки замечаний от ФСТЭК (после отправки Перечня объектов КИИ и после отправки сведений об объектах КИИ).

Ответ: В случае если субъекту критической информационной инфраструктуры поступили замечания ФСТЭК России по результатам рассмотрения перечня объектов критической информационной инфраструктуры, подлежащих категорированию, ему необходимо:

- доработать этот перечень с учетом замечаний, приведенных в письме ФСТЭК России;

- повторно представить этот перечень в ФСТЭК России в сроки, приведенные в письме ФСТЭК России.

В случае если субъекту критической информационной инфраструктуры из ФСТЭК России поступили сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий с мотивированным обоснованием причин возврата, данному субъекту в соответствии с частью 9 статьи 7 Федерального закона № 187-ФЗ необходимо не более чем в десятидневный срок устранить

отмеченные недостатки и повторно направить такие сведения в ФСТЭК России.

ПРИЛОЖЕНИЕ 2. ВОПРОСЫ (КЕЙСЫ) ИЗ ПРАКТИКИ ЭКСПЕРТОВ

1. Отнесение к субъектам КИИ

Вопрос 1: Является ли страховая компания субъектом КИИ?

Ответ: Согласно ст. 76 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» некредитными финансовыми организациями признаются лица, осуществляющие, в частности, деятельность субъектов страхового дела (пп. 9 абз. 1 ст. 76).

Таким образом, страховые организации признаются субъектами, функционирующими в сфере финансовых рынков.

В соответствии со ст. 2 № 187-ФЗ к субъектам КИИ относятся организации, которым на праве собственности, аренды или на ином законном основании принадлежат ИС/АСУ/ИТКС, функционирующие, в частности, в сферах финансового рынка.

Таким образом, страховые организации, в большинстве случаев являются субъектами КИИ, поскольку функционируют в одной из указанных в №187-ФЗ сфер (в финансовой сфере).

Для более точного ответа на поставленный вопрос, является ли конкретная страховая организация субъектом КИИ, следует проанализировать виды деятельности, которые она осуществляет, и определить имеет ли организация на праве собственности, аренды или ином законном основании: ИС/ИТКС/АСУ.

Вопрос 2: Являются ли органы местного самоуправления (ОМСУ) субъектами КИИ?

Ответ: Органы местного самоуправления не являются субъектами КИИ:

• вид деятельности органов местного самоуправления (администраций) по ОКВЭД: 84.11.3 «Деятельность органов местного самоуправления по управлению вопросами общего характера».

• в соответствии с частью 4 статьи 34 Федерального закона от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» органы местного самоуправления не входят в систему органов государственной власти, т.е. не являются государственными органами.

При этом, следует иметь в виду, что такой вид объектов КИИ, как муниципальные информационные системы не обязательно должны принадлежать органу местного самоуправления.

В соответствии с ч. 1 ст. 13 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» муниципальные информационные системы – это информационные системы, созданные на основании решения органа местного самоуправления.

Таким образом, де-юре, безусловно, единственным определяющим признаком муниципальной информационной системы является ее создание на основании решения органа местного самоуправления, а значит, муниципальная информационная система может принадлежать по сути любому российскому юридическому лицу, например, подведомственной организации или муниципально-частному партнеру и, соответственно, являться объектом КИИ.

Вопрос 3: Что предпринять, если ни один из ОКВЭД организации не попал в сферы действия, указанные в п. 8 ст. 2 187-ФЗ?

Ответ: Если ни один из заявленных в ОКВЭД видов деятельности организации не попадает в перечисленные в п. 8 ст. 2 187-ФЗ сферы, то необходимо это документально зафиксировать. Для этого, в организации создается комиссия, которая проводит работу по определению принадлежности организации к субъектам КИИ и, по ее итогам, изготавливает мотивированное решение (см. ниже пример). Данный документ хранится у организации, направление его во ФСТЭК России не требуется.

Пример акта по ОМСУ

АКТ

по результатам определения принадлежности организации к субъектам критической информационной инфраструктуры

Комиссия в составе:

созданная приказом №_____ от ____._____. провела оценку принадлежности Администрации муниципального образования г. _____ к субъектам критической информационной инфраструктуры.

По результатам проведенного анализа комиссия установила:

1. Основной вид деятельности Администрации по Общероссийскому классификатору видов деятельности (ОКВЭД) 84.11.3 «Деятельность органов местного самоуправления по управлению вопросами общего характера», следовательно, Администрация не функционирует ни в одной из сфер, представленных в пункте 8 статьи 2 187-ФЗ.
2. В соответствии с частью 4 статьи 34 Федерального закона от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» органы местного самоуправления не входят в систему органов государственной власти, таким образом, Администрация не является государственным органом.
3. Организации не принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах, представленных в пункте 8 статьи 2 187-ФЗ.
4. Организация не осуществляет взаимодействие систем, перечисленных в пункте 8 стати 2 187-ФЗ:

Комиссия решила:

В соответствии с пунктом 8 статьи 2 ФЗ №187 Администрация г. _____ не является субъектом критической информационной инфраструктуры.

Председатель комиссии
Члены комиссии

2. Категорирование объектов КИИ

Вопрос 1: Как корректно посчитать показатель 9 из перечня показателей критериев значимости (ущерб бюджетам РФ)?

Ответ:

Шаг 1. Берется Федеральный закон «О федеральном бюджете на 2019 и плановый период 2020 и 2021 годов» там есть прогнозируемый общий объем доходов федерального бюджета за 2019, 2020, 2021 годы - складываем три этих значения и получаем усредненный доход за планируемый трехлетний период.

Шаг 2. Считаем ущерб как сумму недополученных доходов в бюджеты всех уровней (по тем бюджетам, куда субъект платит налоги) в результате компьютерного инцидента.

Шаг 3. Делим сумму ущерба (Шаг 2) на усредненный доход (Шаг 1) и умножаем на 100% - получаем значение показателя критерия значимости по п. 9 ПП 127.

Вопрос 2: С кем нужно согласовывать Перечень объектов КИИ, подлежащих категорированию?

Ответ: В соответствии с п. 15 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв.

Постановлением Правительства РФ от 08.02.2018 № 127) перечень объектов подлежит согласованию с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в сфере, в которой функционирует субъект КИИ.

Государственные органы, выполняющие функции по разработке, проведению и реализации государственной политики и (или) нормативно-правовому регулированию:

- Министерство энергетики Российской Федерации – топливно-энергетический комплекс, нефтехимическая промышленность;
- Федеральная служба по экологическому, технологическому и атомному надзору – в области атомной энергии;
- Министерство здравоохранения Российской Федерации – здравоохранение;
- Министерство транспорта Российской Федерации – транспорт;
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации – связь;
- Министерство финансов Российской Федерации – банковская сфера и иные сферы финансового рынка;
- Министерство науки и высшего образования Российской Федерации – наука
- Министерство промышленности и торговли Российской Федерации – оборонная промышленность.

Российские юридические лица, выполняющие функции по разработке, проведению и реализации государственной политики и (или) нормативно-правовому регулированию:

- Государственная корпорация «Росатом» - в области атомной энергии;
- Государственная корпорация по космической деятельности «Роскосмос» - ракетно-космической промышленности.

Вопрос 3: В каком виде и куда нужно направлять Перечень объектов КИИ, подлежащих категорированию?

Ответ: Законодательно форма представления перечня объектов КИИ, подлежащих категорированию не утверждена. Информационным сообщением ФСТЭК России от 24 августа 2018 г. № 240/25/3752 «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» предложена следующая Рекомендованная форма перечня объектов КИИ, подлежащих категорированию:

Приложение 1
к информационному сообщению
ФСТЭК России
от 24 августа 2018 г. № 240/25/3752

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

_____
Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____
Подпись руководителя субъекта или уполномоченного им лица / Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

«____» _____ 20____ г.
Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	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.					
…					
n.					

[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.

Кроме того, указанным информационным сообщением рекомендуется:

1. Направлять во ФСТЭК России утвержденный руководителем субъекта критической информационной инфраструктуры (или уполномоченным лицом) перечень объектов критической информационной инфраструктуры,

подлежащих категорированию: 105066, г. Москва, ул. Старая Басманная, д. 17.

2. Прикладывать при направлении во ФСТЭК России электронную копию перечня объектов критической информационной инфраструктуры, подлежащих категорированию, для сокращения срока оценки перечня (формат docx, xlsx).

Вопрос 4: Установлена ли форма акта категорирования?

Ответ: Установленной формы акта категорирования нет. При этом, п. 16 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 08.02.2018 № 127) устанавливает, что акт должен содержать сведения об объекте КИИ, сведения о присвоенной объекту КИИ категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Следует также учитывать, что перечисленная выше информация входит в состав Сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, регламентированных п. 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 08.02.2018 № 127).

Таким образом, информация из сведений может быть перенесена в акт и утверждена членами комиссии по категорированию.

Вопрос 5: Вправе ли уполномоченное руководителем субъекта КИИ лицо утвердить акт по результатам категорирования?

Ответ: В соответствии с п.16 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 08.02.2018 № 127), акт по результатам категорирования подписывается членами комиссии по категорированию и

утверждается руководителем субъекта критической информационной инфраструктуры.

Таким образом, уполномоченное руководителем субъекта КИИ лицо не вправе утвердить акт по результатам категорирования. Указанное лицо вправе:

- входить в состав постоянно действующей комиссии по категорированию (пп. «а», п. 1 Правил категорирования);
- возглавлять постоянно-действующую комиссию по категорированию (п. 13 Правил категорирования);
- подписывать акт по результатам категорирования (п. 17 Правил категорирования);
- подписывать Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (приказ ФСТЭК России от 22 декабря 2017 г. № 236).

3. Взаимодействие с ГосСОПКА

Вопрос 1: Какие лицензии нужны для подключения к ГосСОПКА?

Ответ: Для подключения к ГосСОПКА лицензии не требуются. Подключение к ГосСОПКА осуществляется в рамках исполнения обязанностей, возложенных на субъект КИИ ст. 9 187-ФЗ, либо в рамках соглашения по взаимодействию между ФСБ России и корпоративным (ведомственным) центром ГосСОПКА.

Вопрос 2: Нужно ли субъекту КИИ подключаться к ГосСОПКА?

Ответ: В явном виде действующее законодательство не предусматривает обязанности по подключению субъекта КИИ к технической инфраструктуре НКЦКИ. Часть 2 статьи 9 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской

Федерации» предусматривает лишь обязанность субъекта КИИ информировать о компьютерных инцидентах ФСБ России (по сути - НКЦКИ) и (или) Центральный банк Российской Федерации (в случае, если субъект КИИ осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном ими порядке.

Порядок информирования определен приказом ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации» (далее – Приказ ФСБ России № 282).

Согласно Приказу ФСБ России № 282, информирование осуществляется путем направления информации в НКЦКИ в соответствии с определенными НКЦКИ форматами представления информации о компьютерных инцидентах в ГосСОПКА с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами КИИ, а также с иными, не являющимися субъектами КИИ, органами и организациями, в том числе иностранными и международными.

В случае отсутствия подключения к данной технической инфраструктуре информация передается субъектом КИИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: http://cert.gov.ru.

Таким образом, Приказ ФСБ России № 282 делает акцент на необходимости использования при информировании технической инфраструктуры НКЦКИ и допускает в качестве «запасного варианта» альтернативные способы предоставления информации в ГосСОПКА.

Кроме того, для значимых объектов КИИ субъекту необходимо создать и обеспечить функционирование системы безопасности, одной из задач

которой является непрерывное взаимодействие с ГосСОПКА (п. 4 ч. 2 ст. 10 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

Помимо нормативных требований следует учитывать, что обнаруживать и предотвращать компьютерные атаки, а также хранить, накапливать, защищать информацию об инцидентах и передавать ее в ГосСОПКА целесообразнее с использованием технических средств. Также, следует отметить, что ГосСОПКА не только собирает информацию, но и предоставляет актуальную информацию об атаках на ресурсы субъекта и другую необходимую для обеспечения безопасности объектов КИИ информацию, которую лучше получать оперативно.

Вопрос 3: Как (каким образом) можно подключиться к ГосСОПКА (технической инфраструктуре НКЦКИ)?

Ответ: Защищенное подключение может быть осуществлено одним из следующих способов:

1. Субъект КИИ имеет и установил лицензионное программное обеспечение ViPNet Client сети 10976 с классом защиты КС3. При выполнении этого условия в НКЦКИ направляется запрос с необходимой информацией для получения файла с настройками.

2. Субъект КИИ имеет лицензию на программное обеспечение или программно-аппаратный комплекс ViPNet Coordinator с классом защиты КС3 ViPNet-сети с номером 10976. После установки ViPNet Coordinator в НКЦКИ направляется запрос с необходимой информацией для получения файла с настройками.

3. Если у субъекта КИИ развернута своя ViPNet-сеть, он направляет запрос в НКЦКИ на получение файла для установления межсетевого взаимодействия собственной ViPNet-сети с ViPNet-сетью 10976 (НКЦКИ).

Вопрос 4: Нужно ли субъекту КИИ создавать свой центр ГосСОПКА?

Ответ: Законодательно такая необходимость не определена. Более того, на практике уже достаточное количество субъектов КИИ осуществляют свое взаимодействие с ГосСОПКА через центры мониторинга и реагирования на инциденты.

Вопрос 5: В какой срок нужно сообщить об инциденте в НКЦКИ?

Ответ: согласно приказу ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации», для значимых объектов КИИ срок составляет 3 часа с момента обнаружения инцидента, для иных объектов КИИ – 24 часа с момента обнаружения инцидента (аналогичные сроки и для информирования Банка России).

При этом, следует отметить, что обязанность по передаче информации в ГосСОПКА, распространяется на всех субъектов КИИ, независимо от вида принадлежащих им объектов: как владельцев объектов с категорией значимости, так и объектов без категории.

4. Банки и организации, функционирующие в сфере финансовых рынков.

Вопрос 1: Банки должны передавать информацию об инцидентах напрямую в ГосСОПКА или через FinCERT?

Ответ: Согласно приказу ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации», информация о компьютерном инциденте также направляется в Банк России с использованием технической инфраструктуры Банка России.

Вопрос 2: Каким образом можно подключиться к технической инфраструктуре FinCERT?

Ответ: субъекты КИИ, функционирующие в банковской сфере или иных сферах финансовых рынков, имеют возможность передавать информацию о компьютерных инцидентах через техническую инфраструктуру Центрального банка России (FinCERT).

Технически, взаимодействие с FinCERT строится следующим образом:

- заключается соглашение о взаимодействии (оно типовое);
- для взаимодействия организуется защищенное соединение с использованием сертифицированных средств криптографической защиты информации. Предлагается три программных продукта: Континент TLS, ViPNet CSP, КриптоПро CSP;
- после заключения соглашения участнику настраивается учетная запись – выдается логин и пароль;
- по логину и паролю участник получает доступ в личный кабинет. Посредством этого же кабинета можно осуществлять информирование FinCERTa, направлять в FinCERT запросы, взаимодействовать с другими участниками, подключенными к FinCERT, передавать информацию в ГосСОПКА.

Передача информации в ГосСОПКА осуществляется с использованием форматов передачи данных, утвержденных ФСБ России.

Вопрос 3: Какие требования в части КИИ распространяются на операторов по переводу денежных средств (операторов услуг информационного обмена).

Ответ: Федеральный закон от 2 августа 2019 г. № 264-ФЗ «О внесении изменений в Федеральный закон «О национальной платежной системе» и Федеральный закон «О Центральном банке Российской Федерации (Банке России)» дополнил статью 9.1 Федерального закона «О платежной системе» нормой следующего содержания: «Информационные системы операторов по

переводу денежных средств, с использованием которых осуществляется прием электронных средств платежа и обмен информацией с иностранными поставщиками платежных услуг, информационные системы операторов услуг информационного обмена, с использованием которых осуществляется взаимодействие с иностранными поставщиками платежных услуг, должны соответствовать требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Согласно данной норме, все информационные системы, задействованные в процессе обмена информацией с иностранными поставщиками платежных услуг, должны соответствовать требованиям по обеспечению безопасности значимых объектов КИИ, независимо от того, прошли они процедуру категорирования или нет, и независимо от того, принадлежат они субъектам КИИ или нет. Требования по обеспечению безопасности значимых объектов КИИ утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239. В соответствии с п. 6 приказа ФСТЭК № 239 безопасность значимых объектов обеспечивается субъектами КИИ в рамках функционирования систем безопасности значимых объектов, создаваемых субъектами КИИ. Создание и функционирование систем безопасности значимых объектов КИИ определяется приказом ФСТЭК России от 21 декабря 2017 г. № 235.

Таким образом, данная норма возлагает на операторов по переводу денежных средств (операторов услуг информационного обмена), независимо от их принадлежности к субъектам КИИ, обязанности по обеспечению безопасности информационных систем задействованных в процессе обмена информацией с иностранными поставщиками платежных услуг по требованиям предъявляемым к значимым объектам КИИ.

ПРИЛОЖЕНИЕ 3. ПРИМЕРНЫЙ СОСТАВ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ СУБЪЕКТА КИИ

Норма законодательства	Разрабатываемые документы
Раздел 1. ФЗ №187	
Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты критической информационной инфраструктуры в письменном виде в десятидневный срок со дня принятия ими соответствующего решения направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме (ч. 5 ст. 7)	Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (форма утверждена Приказом ФСТЭК России от 22 декабря 2017 г. № 236)
Разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры (пункт 4 ч 1 ст. 9)	План проведения мероприятий по обеспечению безопасности значимых объектов КИИ
Незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (пункт 1 ч 2 ст. 9)	План реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, либо раздел в Регламенте по реагированию на инциденты информационной безопасности: «Информирование и взаимодействие с уполномоченными органами», где прописывается как осуществляется взаимодействие с регуляторами.
В случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность. (пункт 3 ч 2 ст. 9)	Документы по внедрению, приемке и эксплуатации средств. Порядок хранения и учета средств.
Реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти,	План реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак, либо раздел в

уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры. (пункт 3 ч 3 ст. 9)	Регламенте по реагированию на инциденты информационной безопасности
Восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации (пункт 3 ч 2 ст. 10)	• План по восстановлению функционирования • Правила резервного копирования
Раздел 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»	
Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию (пункт 11):	Приказ о создании комиссии (Приложение 5)
Комиссия по категорированию в ходе своей работы (пункт 14):	• Перечень процессов в рамках функций (полномочий) или видов деятельности • Перечень критических процессов
а) определяет процессы, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры; б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры	
в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;	Перечень объектов КИИ, подлежащих категорированию
г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники	Перечень возможных действий нарушителей в отношении объектов КИИ

угроз безопасности информации;	
д) анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;	Перечень угроз безопасности и уязвимостей программного обеспечения объектов КИИ
е) оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;	Акт (протокол работы комиссии) оценки возможных последствий
ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.	Акт категорирования объектов КИИ
Раздел 3. Приказ ФСТЭК России от 21 декабря 2017 г. № 235	
Руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо, на которое возложены функции обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее - уполномоченное лицо), создает систему безопасности, организует и контролирует ее функционирование. (пункт 8).	Приказ о создании системы безопасности, назначении ответственных (подразделений) отвечающих за функции обеспечения безопасности КИИ, определении системы контроля
Руководитель субъекта критической информационной инфраструктуры определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов критической информационной инфраструктуры в зависимости от количества значимых объектов критической информационной инфраструктуры, а также особенностей деятельности субъекта критической информационной инфраструктуры. (пункт 9).	Приказ об определении функциональных обязанностей должностных лиц (подразделений), либо внесение корректировок в должностные инструкции ответственных работников.
Руководитель субъекта критической информационной инфраструктуры создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее - структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение	Приказ о назначении ответственных за обеспечение безопасности значимых объектов КИИ

безопасности значимых объектов критической информационной инфраструктуры (далее - специалисты по безопасности). (пункт 10).	
Субъект критической информационной инфраструктуры должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности критической информационной инфраструктуры и о возможных угрозах безопасности информации. (пункт 15).	Регламент по повышению осведомленности персонала по вопросам обеспечения безопасности значимых объектов КИИ. Приложение. План проведения занятий.
Средства защиты информации должны применяться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на средства защиты информации. (пункт 20).	Накладные на приобретение, сертификаты (для сертифицированных средств защиты информации), паспорт-формуляр, инструкции.
Порядок применения средств защиты информации определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов с учетом особенностей деятельности субъекта критической информационной инфраструктуры. (пункт 22).	Инструкция оператору, пользователю, системному администратору и т.п.
Субъектом критической информационной инфраструктуры в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры. (пункт 23).	Политика, Положение, Регламент и т.п. определяющие порядок и правила обеспечения безопасности значимых объектов КИИ
Контроль (*мероприятий по обеспечению безопасности*) проводится ежегодно комиссией, назначаемой субъектом критической информационной инфраструктуры. Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается руководителем субъекта	• Приказ о назначении комиссии • Положение (методика) о работе комиссии • План работы комиссии. • Акт по результатам работы.

критической информационной инфраструктуры (уполномоченным лицом). (пункт 36).	
Раздел 4. Приказ ФСТЭК России от 25 декабря 2017 г. № 239	
На стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта проводятся (пункт 8): а) установление требований к обеспечению безопасности значимого объекта; б) разработка организационных и технических мер по обеспечению безопасности значимого объекта; в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие; г) обеспечение безопасности значимого объекта в ходе его эксплуатации; д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.	Результаты реализации мероприятий, проводимых для обеспечения безопасности значимого объекта на стадиях (этапах) его жизненного цикла, подлежат документированию. Состав и формы документов определяются субъектом критической информационной инфраструктуры.
Разработка организационных и технических мер по обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по созданию (модернизации) значимого объекта и (или) обеспечению его безопасности, в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта и должна включать (пункт 11): а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);	• Рекомендации по корректировке архитектуры значимого объекта и организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации; • Модель угроз безопасности информации для объекта КИИ или группы объектов КИИ.
б) проектирование подсистемы безопасности значимого объекта;	• Техническое задание (частное техническое задание); • Технический проект.
в) разработку рабочей (эксплуатационной) документации на значимый объект КИИ (в части обеспечения его безопасности).	• Описание архитектуры подсистемы безопасности значимого объекта; • Порядок и параметры настройки программных и программно-

	аппаратных средств, в том числе средств защиты информации; • Правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).
Установка и настройка средств защиты информации должна проводиться в соответствии с проектной и рабочей (эксплуатационной) документацией (пункт 12.1)	Акт установки средств защиты
Разрабатываемые организационно-распорядительные документы по безопасности значимого объекта должны определять правила и процедуры реализации отдельных организационных и (или) технических мер (политик безопасности) (пункт 12.2)	Правила (инструкции) безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами.
При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляются (пункт 12.3):	• Приказ по организации контроля физического доступа к программно-аппаратным средствам значимого объекта и его линиям связи; • Правила (Регламент) разграничения доступа, определяющие права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств; • Приказ о назначении администратора безопасности значимого объекта; • Порядок и План отработки действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.
Предварительные испытания значимого объекта и его подсистемы безопасности (пункт 12.4)	• Программа и методики предварительных испытаний работоспособности подсистемы безопасности значимого объекта и отдельных средств защиты информации, • Акт (протокол) оценки влияния подсистемы безопасности на функционирование значимого

	объекта при проектных режимах его работы • Приказ о вводе в опытную эксплуатацию значимого объекта и его подсистемы безопасности.
Опытная эксплуатация значимого объекта и его подсистемы безопасности (пункт 12.5)	• Программа и методики опытной эксплуатации, включая проверку функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер • Проверка знаний и умений пользователей и администраторов, необходимых для эксплуатации значимого объекта и его подсистемы безопасности (журнал или зачетная ведомость).
Приемочные испытания значимого объекта и его подсистемы безопасности (пункт 12.ж)	• Программа и методики приемочных испытаний. • Акт приемки значимого объекта в эксплуатацию. • Приказ о вводе в действие значимого объекта и его подсистемы безопасности.
Реагирование на компьютерные инциденты (пункт 13.5)	• Приказ о назначении ответственных за выявление компьютерных инцидентов и реагирование на них. • Утверждение функциональных обязанностей • Инструкция по реагированию на компьютерные инциденты.
Для обеспечения действий в нештатных ситуациях при эксплуатации значимого объекта (пункт 13.6)	• План мероприятий по обеспечению безопасности значимого объекта на случай возникновения нештатных ситуаций; • Журнал (Зачетная ведомость) по обучению и отработке действий персонала по обеспечению безопасности значимого объекта в случае возникновения нештатных ситуаций; • Приказ об определении альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций; • Положение (Регламент) о резервировании программных и программно-аппаратных средств, в том числе средств защиты

	информации, каналов связи на случай возникновения нештатных ситуаций; • Приказ об обеспечении восстановления значимого объекта и (или) его компонентов в случае возникновения нештатных ситуаций; • Положение (Регламент) по проведению анализа возникших нештатных ситуаций и принятию мер по недопущению их повторного возникновения.

ПРИЛОЖЕНИЕ 4. ПРИМЕРНЫЙ СОСТАВ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ПО ВЗАИМОДЕЙСТВИЮ С ГОССОПКА

Норма законодательства	Разрабатываемые документы
Федеральный закон от 26.07.2017 № 187-ФЗ	
Статья 5. 2. ….. 3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.	• Приказ о создании системы обнаружения, предупреждения и ликвидации последствий компьютерных атак и назначении ответственных. • Функциональные обязанности должностных лиц (подразделений). • Правила (Регламент) реагирования на компьютерные инциденты.
Статья 9. 2. ….. 3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.	• Акт установки. • Накладные, формуляры, документация, сертификаты. • Инструкция оператору по эксплуатации средств. • Приказ об организации хранения средств.
3. …. 3) реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры.	• Правила (Регламент) реагирования на компьютерные инциденты. • Функциональные обязанности должностных лиц (подразделений). • План ликвидации последствий компьютерных атак.
3. …. 4) обеспечивать беспрепятственный доступ должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения	Приказ об организации допуска на объекты КИИ должностных лиц федерального органа исполнительной власти.

безопасности критической информационной инфраструктуры Российской Федерации, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий, предусмотренных статьей 13 настоящего Федерального закона.	
Статья 10. 4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.	Приказ об организации взаимодействия с ГосСОПКА
Приказ ФСБ России от 24 июля 2018 г. № 367	
Приказ ФСБ России от 24 июля 2018 г. № 367	• Приказ об утверждении перечня передаваемой информации • Приказ о порядке предоставления сведений • Приказ о назначении ответственного за организацию передачи сведений
Приказ ФСБ* России от *24 июля 2018* г. *№ 368	
2. ….. Субъекты критической информационной инфраструктуры вправе самостоятельно определять круг субъектов критической информационной инфраструктуры, с которыми осуществляется такой обмен.	*При необходимости* Приказ об организации информационного обмена с субъектами КИИ
Приказ ФСБ России от 06.05.2019 № 196	
3.3. Средства ГосСОПКА должны иметь возможность модернизации российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц. 3.4. Средства ГосСОПКА должны быть обеспечены гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.	В Политике по информационной безопасности выделяются пункты, регламентирующие модернизацию, гарантийную и техническую поддержку средств защиты информации, либо разрабатывается отдельное положение (регламент).
13. Средства ликвидации последствий должны обладать следующими функциями: • учет и обработка компьютерных инцидентов; • управление процессами реагирования на компьютерные	• Правила (Регламент) реагирования на компьютерные инциденты • Журнал учета компьютерных инцидентов • Приказ об организации взаимодействия с ГосСОПКА

инциденты и ликвидации последствий компьютерных атак; • взаимодействие с НКЦКИ посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными;	
Приказ ФСБ России от 19.06.2019 № 281	
2. Для согласования установки средств субъект критической информационной инфраструктуры не позднее чем за 45 календарных дней до даты планируемой установки направляет в ФСБ России структурно-функциональную схему подключения средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления	Заявка на подключение и установку средств защиты
7. Субъект критической информационной инфраструктуры после приема в эксплуатацию средств информирует об этом Национальный координационный центр по компьютерным инцидентам в течение 5 календарных дней.	Информационное письмо
9. Субъект критической информационной инфраструктуры определяет порядок доступа к эксплуатируемым средствам и осуществления контроля за ним.	Регламент по порядку доступа к средствам защиты
Приказ ФСБ России от 19.06.2019 № 282	
Приказ ФСБ России от 19.06.2019 № 282	Правила (Регламент) реагирования на компьютерные инциденты
6. Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, … разрабатывается план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак	• Правила (Регламент) реагирования на компьютерные инциденты • Функциональные обязанности должностных лиц (подразделений) • План ликвидации последствий компьютерных атак
10. Субъект критической информационной инфраструктуры…, не реже одного раза в	План проведения тренировки.

год организует и проводит тренировки по отработке мероприятий Плана.	
11. Субъект КИИ в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак осуществляет: анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками;	Результаты анализа
13. В ходе ликвидации последствий компьютерных атак субъектом КИИ, принимаются меры по восстановлению функционирования и проверке работоспособности значимого объекта критической информационной инфраструктуры	Правила (Регламент) реагирования на компьютерные инциденты

ПРИЛОЖЕНИЕ 5. ПРИМЕР ПРИКАЗА О СОЗДАНИИ ПОСТОЯННО ДЕЙСТВУЩЕЙ КОМИССИИ ПО КАТЕГОРИРОВАНИЮ

На фирменном бланке организации

ПРИКАЗ

от «_____» _____201_ г. г. _____

О создании постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Постановлением 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» и в целях определения категорий значимости объектов КИИ

Приказываю:

1. Создать постоянно действующую комиссию по категорированию объектов КИИ (далее по тексту – Комиссии).
2. Включить в состав Комиссии по категорированию объектов КИИ:

Председатель комиссии:

(наименование должности) (И.О.Ф.)

Члены комиссии:

(наименование должности) (И.О.Ф.)

…….

(наименование должности) (И.О.Ф.)

3. Председателю Комиссии в срок до «__»_____201_ г. организовать разработку и утверждение:

- Плана работы постоянно действующей комиссии по категорированию объектов критической информационной инфраструктуры в (*наименование организации*).
- Положение о постоянно действующей комиссии по категорированию в (*наименование организации*).

4. Организовать работу комиссии в соответствии с разработанными и утвержденными согласно п. 3 локальными нормативными актами.

5. Контроль за выполнением настоящего приказа оставляю за собой.

Директор _____ _____

С приказом ознакомлены:

(наименование должности)	(И.О.Ф)
(наименование должности)	(И.О.Ф.)

ПРИЛОЖЕНИЕ 6. ПРИМЕР ПИСЬМА О НАПРАВЛЕНИИ СВЕДЕНИЙ О РЕЗУЛЬТАТАХ ПРИСВОЕНИЯ ОБЪЕКТУ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОДНОЙ ИЗ КАТЕГОРИЙ ЗНАЧИМОСТИ ЛИБО ОБ ОТСУТСТВИИ НЕОБХОДИМОСТИ ПРИСВОЕНИЯ ЕМУ ОДНОЙ ИЗ ТАКИХ КАТЕГОРИЙ

На фирменном бланке организации

ФСТЭК России
105066, г. Москва,
ул. Старая Басманная, д. 17

О направлении сведений о результатах присвоения объектам критической информационной инфраструктуры категорий значимости либо об отсутствии необходимости присвоения им таких категорий

Во исполнение требований пункта 17 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. Постановлением Правительства РФ от 8 февраля 2018 г. № 127) направляем Сведения о результатах присвоения объектам критической информационной инфраструктуры нашей организации категорий значимости либо об отсутствии необходимости присвоения им таких категорий.

В случае возникновения вопросов или необходимости получить какие-либо разъяснения с нашей стороны, просим обращаться к ФИО, телефон, адрес эл. почты.

Приложение: Сведения о результатах присвоения объектам критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения им одной из таких категорий на число цифрой (число прописью) листах в 1 (одном) экз.

Должность /И.О.Ф/