БЕЗОПАСНОСТЬ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ

Общие рекомендации

(Версия 1.0)

Москва, 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Вышедший в середине 2017 года и вступивший в силу с 1 января 2018 года Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» еще с самого выхода в свет породил массу вопросов.

По прошествии полугода со дня вступления его в законную силу в сообществе специалистов по информационной безопасности возникло множество различных, иногда диаметрально противоположных, точек зрения относительно практики его применения.

В этой связи, Ассоциацией руководителей служб информационной безопасности была выдвинута инициатива по подготовке практического пособия, целью которого является формулировка рекомендаций (дорожной карты) для специалистов служб информационной безопасности и информационно-технического обеспечения дающих понимание того, что такое критическая информационная инфраструктура и какие шаги необходимо предпринять для обеспечения ее безопасности на уровне организации.

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

Данное пособие является первой попыткой представить в комплексе весь спектр основных вопросов касающихся указанной тематики с учетом сложностей и неоднозначностей толкования принятых нормативно-правовых актов и отсутствия практики их право применения.

В целом, алгоритм связанный с обеспечением безопасности объектов критической информационной инфраструктуры в организации можно представить в виде следующих шагов (рисунок 1).

В главах данного пособия коллектив авторов - практиков в области защиты информации, рассматривает вопросы реализации указанного алгоритма, затрагивает ряд спорных и проблемных моментов, вызывающих вопросы у руководителей служб информационной безопасности и представителей бизнес сообщества.

ГЛАВА 1. ЧТО ТАКОЕ КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА?

Основные понятия, касающиеся области обеспечения безопасности критической информационной инфраструктуры (далее по тексту - КИИ) сформулированы в статье 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее по тексту - Закон «О безопасности КИИ»). В соответствии с ней, под КИИ понимаются объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Как видно из определения критическая информационная инфраструктура Российской Федерации представляет собой совокупность всех принадлежащих российским организациям и органам государственной власти объектов КИИ и обеспечивающих их взаимодействие сетей электросвязи.

Объекты КИИ - это имеющиеся у субъектов КИИ:

- Информационные системы (ИС)[1]. Одним из наиболее распространенных видов информационных систем являются информационные системы персональных данных (ИСПДн).
- Информационно-телекоммуникационные сети (ИТКС).[2] Самыми распространенными видами информационно-телекоммуникационных систем являются корпоративные информационные сети и сеть международного обмена «Интернет».
- Автоматизированные системы управления (АСУ)[3]. Одним из наиболее распространенных видов указанных систем являются

[1] Информационная система - 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»).

[2] Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

[3] Один из видов автоматизированных систем. Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (ГОСТ 34.003-90. Межгосударственный стандарт. Информационная

автоматизированные системы управления технологическими процессами (АСУ ТП) промышленных предприятий.

Под субъектами КИИ понимаются:

1. Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели:

- функционирующие в одной из 14 сфер жизнедеятельности: 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 указанных систем или сетей: ИС, ИТКС, АСУ.

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 (государственный орган, учреждение) субъектом КИИ, необходимо оценивать сферу функционирования не принадлежащей ей ИС, АСУ или ИТКС, а сферу деятельности самой организации.

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).

ГЛАВА 2. ТИПОЛОГИЯ ОБЪЕКТОВ КИИ

Помимо отнесения того или иного хозяйствующего субъекта к критической информационной инфраструктуре, достаточно большое количество вопросов связано с типологией объектов критической информационной инфраструктуры (далее по тексту - Объект КИИ, ОКИИ).

Типология - это классификация объекта по его существенным признакам. Классификация имеет познавательное значение и предназначена для постоянного использования в науке или области практической деятельности, в целях выявления существенных сходства и различия между предметами, а также систематизации объектов по каким-либо признакам.

Прикладное (практическое) значение типологии в том, что правильное определение типа объекта КИИ позволяет сформировать перечень мер, необходимых для обеспечения его безопасности, в том числе с учетом требований специальных нормативных правовых актов:

1. По значимости, ОКИИ подразделяются на следующие виды (рисунок 1):

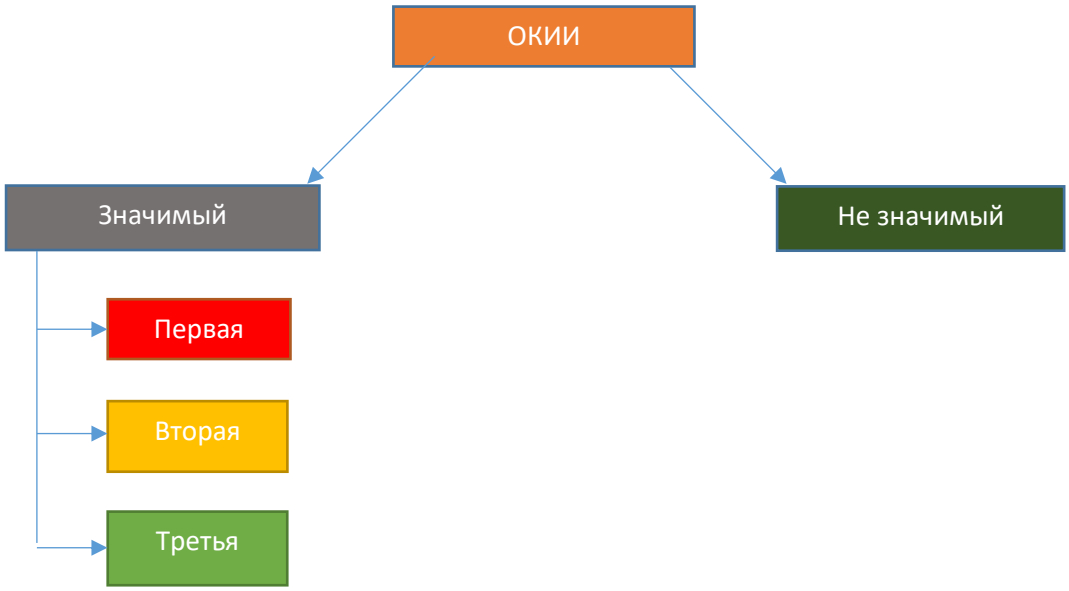

Рисунок 1. Классификация ОКИИ по значимости

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 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»): максимальный целевой уровень защищенности - первый, минимальный - третий.

От уровня защищенности значимого ОКИИ, 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, АСУ ТП и т.п.

При этом, все субъекты (как значимые, так и нет), наделяются следующими правами (ст. 9 Закона «О безопасности КИИ»):

1) получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации[4], 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;

[4] 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.

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 Федерации[5], 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,

[5] 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».

предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

С практической точки зрения, для выполнения возложенных на субъекта КИИ, не владеющего значимыми объектами, 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 (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 и 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 14 областей:

1) здравоохранение;
2) наука;
3) транспорт;
4) связь;
5) энергетика;
6) банковская сфера;
7) сфера финансовых рынков
8) топливно-энергетический комплекс;
9) атомная энергетика;
10) оборонная промышленность;
11) ракетно-космическая промышленность;
12) горнодобывающая промышленность;
13) металлургическая промышленность;
14) химическая промышленность.

С точки зрения практического применения следует учитывать два момента:

1) Для конкретной отрасли будет преобладающим конкретный вид объекта КИИ (см. таблицу 1).

Таблица 1. 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 относиться к категории значимых. Рассмотрим в качестве примера металлургическую промышленность. Как правило, на металлургических предприятиях есть АСУ (АСУ ТП), которые осуществляют управление технологическими и (или) производственными процессами, также есть информационные бухгалтерские системы по учету заработной платы и кадров. Оба класса систем функционируют в сфере металлургии и поэтому являются объектами КИИ. Однако, АСУ ТП с наибольшей вероятностью (в большинстве случаев) будут отнесены к значимым объектам, чем ИС.

2) Необходимо оценивать, с точки зрения функционирования в той или иной сфере, именно субъекта, а не объект КИИ.

При этом, важным становится вопрос о том, как определить сферу деятельности самой организации? Очевидно, что основным документом, опираясь на который можно это сделать, является выписка из Единого государственного реестра юридических лиц (ЕГРЮЛ), в которой содержатся сведения о заявленных организацией видах деятельность и наличии у нее

лицензий. Кроме того, информация о сфере функционирования организации содержится в ее Уставе (Положении). При этом, как правило, информация Устава (Положения) и ЕГРЮЛ совпадает (рисунок 2).

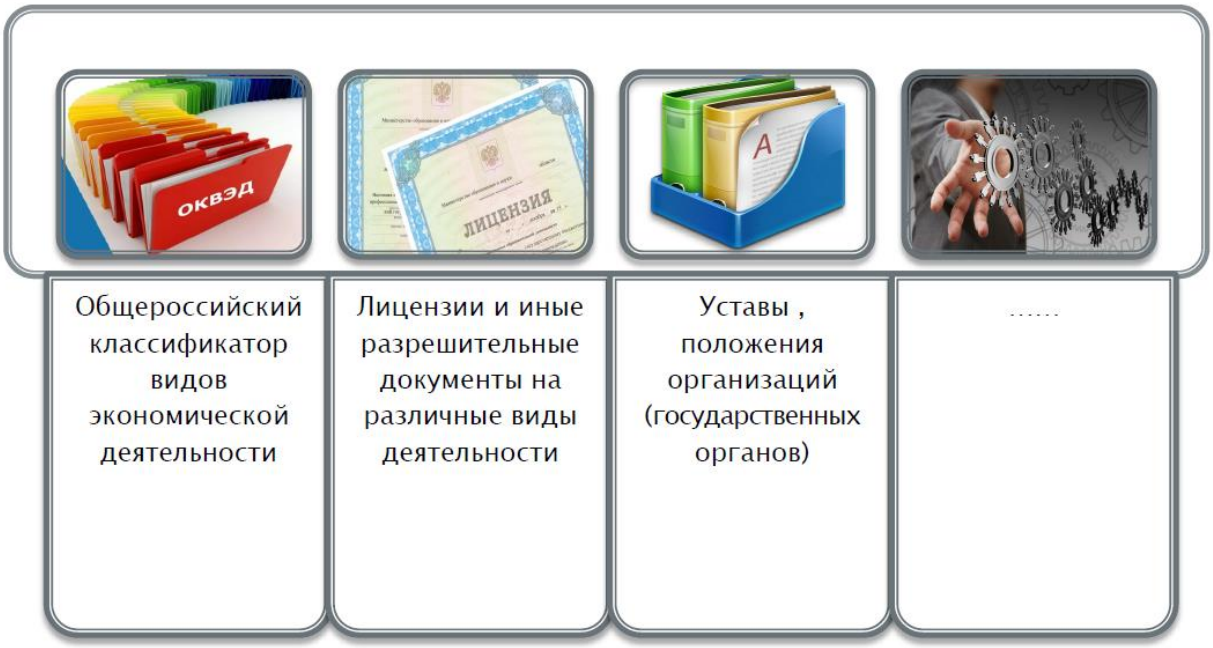

Рисунок 2. Определение является ли организация субъектом КИИ

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

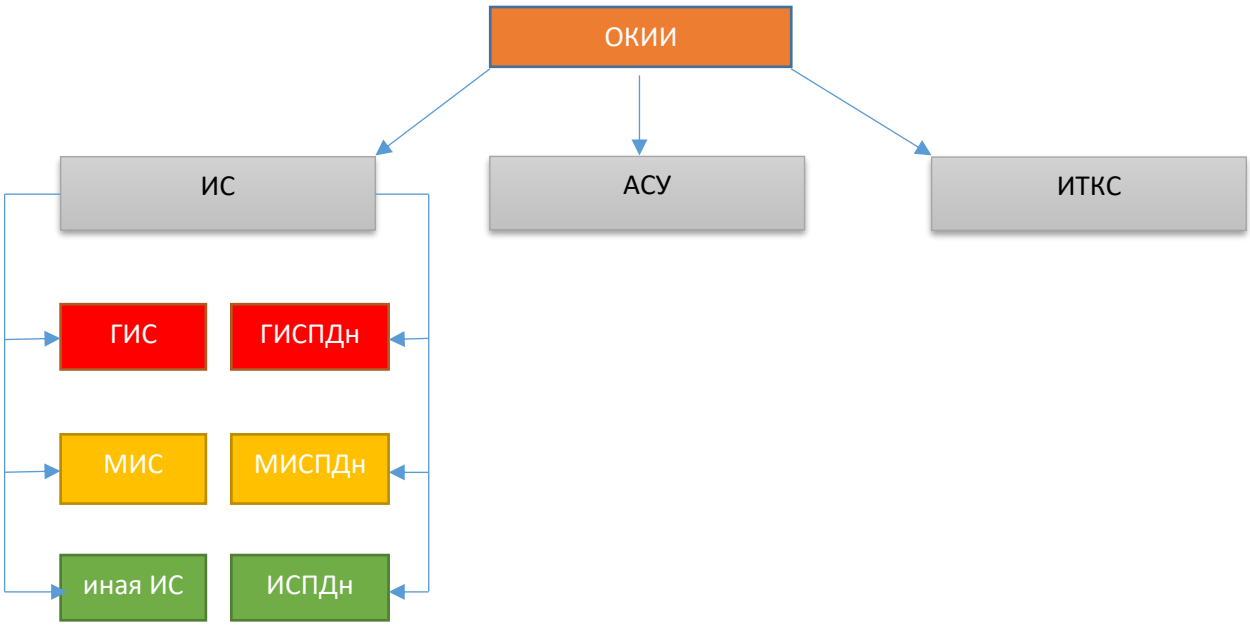

Рисунок 3. Классификация ОКИИ по виду системы

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 ОКИИ (таблица 2).

Таблица 2 Основные нормативно-правовые акты, устанавливающие меры защиты ОКИИ

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:

1. НК РФ - Налоговый кодекс Российской Федерации
2. 98-ФЗ - Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
3. 149-ФЗ - Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. 152-ФЗ - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. 395-1 - Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»
6. 1119 - Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7. 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».
8. 17 - Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

9. 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».
10. 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».
11. 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»
12. 239 - Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»
13. 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».
14. 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 таблице 2 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.

ГЛАВА 3. ПРОВЕДЕНИЕ ПРОЦЕДУРЫ КАТЕГОРИРОВАНИЯ

В соответствии с ч. 1 ст. 7 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Процедуру категорирования можно схематично представить следующим образом (рисунок 3)

Рисунок 4. 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», рассматривать ее в

данном параграфе не имеет смысла. Остановимся лишь на проблемных вопросах ее проведения:

Вопрос 1. Какие объекты подлежат категорированию?

Согласно п. 3 Правил категорирования объектов критической информационной инфраструктуры Российской Федерации (утв. постановлением Правительства Российской Федерации от 8 февраля 2018 года № 127, далее по тексту - Правила) категорированию подлежат объекты КИИ, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ. Таким образом, из буквального толкования указанной нормы следует, что категорированию подлежат все принадлежащие субъекту КИИ объекты.

При этом, некоторые эксперты, изучая процедуру категорирования объектов КИИ, нередко приходят к мнению, что категорированию подлежат только те объекты, которые обрабатывают информацию, необходимую для обеспечения критических процессов и (или) осуществление управления, контроля или мониторинга ими.

Исходя из буквального толкования п. 5 Правил следует, что процедура категорирования объектов КИИ включает:

1. Определение всех процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов КИИ.

2. Выявление критических процессов, то есть тех, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка.

3. Определение тех объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения критических процессов и (или) осуществления управления, контроля или мониторинга ими.

4. Формирование перечня объектов КИИ, подлежащих категорированию.

5. Оценка, в соответствии с перечнем показателей критериев значимости (утв. постановлением Правительства Российской Федерации от 8 февраля 2018 года № 127), возможных последствий в случае возникновения компьютерных инцидентов на объектах КИИ.

6. Присвоение каждому из объектов КИИ категории значимости, либо принятие решения о ее отсутствии.

Таким образом, согласно процедуре категорирования, в перечень объектов КИИ, подлежащих категорированию, включаются только те, которые обрабатывают информацию, необходимую для автоматизации критических процессов и (или) осуществляют их управление, контроль или мониторинг, а, следовательно, они и подлежат категорированию.

Вопрос 2. 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 толкование дефиниции «критический процесс» и не содержит методики его определения, а значит, вопрос отнесения того или иного процесса к перечню критических остается исключительно на усмотрение субъекта КИИ.

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

1. Субъект может обосновать, что критические процессы у него отсутствуют, а, следовательно, нет и значимых объектов КИИ. 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 относятся только те процессы, которые обеспечивают основные виды деятельности субъекта. Основные виды деятельности

субъекта, как правило, содержатся в его уставных документах. Такой подход, к примеру, предлагается различными экспертами на отраслевых конференциях. Если следовать его логике, субъекту необходимо проанализировать ЕГРЮЛ и выделить в нем виды деятельности, задекларированные как основные. Далее для полученного перечня основных видов деятельности следует определить, имеются ли у субъекта объекты КИИ которые их автоматизируют.

3. К критическим следует относить все процессы исходя из той логики, что нарушение вспомогательного процесса может, прямо или косвенно, привести к нарушению основного.

По мнению автора, определение критичности процесса должно базироваться на общей логике закона. Речь идет о том, что к критическим нужно относить те процессы, нарушение нормального функционирования которых может привести к последствиям, указанным в Перечне показателей критериев значимости объектов КИИ (утв. постановлением Правительства РФ от 08.02.2018 № 127), и, соответственно, выделять конкретные объекты КИИ, с помощью которых автоматизируются указанные критические процессы.

Вопрос 3. Как осуществлять присвоение категории значимости объекту КИИ: с учетом мер защиты или без них?

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.

Вопрос 4. Каковы реальные сроки проведения категорирования?

Согласно п. 15 Правил максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом КИИ перечня объектов. При этом срок подготовки данного перечня законом не определен. По заявлению представителей ФСТЭК России на различных отраслевых конференциях, субъекты КИИ уже должны были направить данный перечень в указанную федеральную службу. При этом, по мнению автора, поскольку срок законодательно не установлен, субъект КИИ 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) 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: появятся новые, либо часть будет выведена из эксплуатации. Результатом чего может стать несовпадение сведений, содержащихся в итоговых актах категорирования и направленном ранее во ФСТЭК России перечне объектов КИИ, что, по мнению автора, 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 с актами категорирования.

ГЛАВА 4. ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

Опираясь на материла предыдущих глав мы определили, что относимся (или нет) к субъектам КИИ, установили категорию значимости и наступил долгожданный момент практической реализации предусмотренных мер по обеспечению безопасности КИИ.

Из самого закона: Статья 4 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определяет принципы обеспечения безопасности критической информационной инфраструктуры:

1) законность;

2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

3) приоритет предотвращения компьютерных атак.

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» Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации

устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

Данные требования установлены приказом ФСТЭК России от 21 декабря 2017 г. № 235, в котором определены состав и требования к силам обеспечения информационной безопасности объектов КИИ, их структура и функции. Что важнее всего им вменяется «проводить анализ угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры и выявлять уязвимости в них».

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

Отдельное внимание уделено организационно-распорядительным документам по безопасности значимых объектов, которые являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта критической информационной инфраструктуры. При этом положения, определяющие порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования значимого объекта критической информационной инфраструктуры.

Приказом ФСТЭК России от 25 декабря 2017 г. № 239 утверждены требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Обеспечение безопасности значимых объектов является составной частью работ по созданию (модернизации), эксплуатации и вывода из эксплуатации значимых объектов. Меры по обеспечению безопасности значимых объектов принимаются на всех стадиях (этапах) их жизненного цикла.

Прямо по пунктам закона можно задавать алгоритм действий:

- устанавливаем требования к обеспечению безопасности значимого объекта;

- разрабатываем организационные и технические меры по обеспечению безопасности значимого объекта;

- внедряем организационные и технические меры по обеспечению безопасности значимого объекта;

Организационные и технические меры по обеспечению безопасности значимого объекта (состав подробно приведен в приложении к приказу ФСТЭК №239 от 25 декабря 217 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);
- 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).

Сравним меры приказов ФСТЭК 239, 31 и 17

Приказ ФСТЭК №239	**Приказ ФСТЭК № 31**	**Приказ ФСТЭК №17**
ИАФ	ИАФ	ИАФ
УПД	УПД	УПД
ОПС	ОПС	ОПС
ЗНИ	ЗНИ	ЗНИ
АУД	**РСБ**	**РСБ**
АВЗ	АВЗ	АВЗ
СОВ	СОВ	СОВ
ОЦЛ	**АНЗ**	**АНЗ**

ОДТ	ОЦЛ	ОЦЛ
ЗТС	ОДТ	ОДТ
ЗИС	**ЗСВ**	**ЗСВ**
ПЛН	ЗТС	ЗТС
УКФ	ЗИС	ЗИС
ОПО	ОБР	
ИНЦ	ОПО	
ДНС	**ПЛН**	
ИПО	**ДНС**	
	ИПО	
	УБИ	
	ИНЦ	
	УКФ	

Зелёным - обшее для 239, 31 и 17
Синим - общее для
239 и 31
Красным - оригинальное для 239 и 31
Черным - для 31 и 17

Углубимся в пункты, по которым наблюдаются различия:

Из приказа ФСТЭК №239	**Из приказа ФСТЭК №31 и №17 (УБИ соответствует только приказу №31)**
V. Аудит безопасности (АУД)	***V. Регистрация событий безопасности (РСБ)***
Разработка политики аудита безопасности	Разработка правил и процедур (политик) регистрации событий безопасности
Инвентаризация информационных ресурсов	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
Анализ уязвимостей и их устранение	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

Генерирование временных меток и (или) синхронизация системного времени	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
Регистрация событий безопасности	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
Контроль и анализ сетевого трафика	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
Защита информации о событиях безопасности	Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления
Мониторинг безопасности	Защита информации о событиях безопасности
Реагирование на сбои при регистрации событий безопасности	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей
Анализ действий пользователей	***VIII. Контроль (анализ) защищенности информации (АНЗ)***
Проведение внутренних аудитов	Разработка правил и процедур (политик) контроля (анализа) защищенности
Проведение внешних аудитов	Выявление, анализ уязвимостей и оперативное устранение вновь выявленных уязвимостей
XIV. Управление обновлениями программного обеспечения (ОПО)	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
Разработка политики управления обновлениями программного обеспечения	Контроль работоспособности, параметров настройки и правильности функционирования

	программного обеспечения и средств защиты информации
Поиск, получение обновлений программного обеспечения от доверенного источника	Контроль состава технических средств, программного обеспечения и средств защиты информации
Контроль целостности обновлений программного обеспечения	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей
Тестирование обновлений программного обеспечения	***XIX. Анализ угроз безопасности информации и рисков от их реализации (УБИ)***
Установка обновлений программного обеспечения	Разработка правил и процедур (политик) анализа угроз безопасности информации и рисков от их реализации
	Периодический анализ изменения угроз безопасности информации, возникающих в ходе эксплуатации автоматизированной системы управления
	Периодическая переоценка последствий от реализации угроз безопасности информации (анализ риска)

Состав меры «Аудит безопасности» (АУБ) приказа №239 - содержит в себе элементы «Регистрация событий безопасности» (РСБ), «Контроль (анализ) защищенности информации» (АНЗ), «Анализ угроз безопасности информации и рисков от их реализации» (УБИ) из приказа №31.

Если у субъекта КИИ уже в полном объеме реализованы меры приказа ФСТЭК России от 14 марта 2014 г. № 31, обеспечить соответствие приказу ФСТЭК России от 25 декабря 2017 г. № 239 будет не сложно, но важно выполнить меру «XIV. Управление обновлениями программного обеспечения» (ОПО). Интересен пункт Тестирование обновлений

программного обеспечения, т.е. не просто поддержание актуальности ПО, но и корректности обновления именно для действующей системы конкретного объекта.

Труднее придется субъектам КИИ, реализовавшим только 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).

ГЛАВА 5. ПОДКЛЮЧЕНИЕ К 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:

1) Указом Президента Российской Федерации от 15.01.2013 № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;
2) Концепцией государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - ГосСОПКА), утвержденной Президентомт Российской Федерации 12.02.2014 г. № К 1274 (http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf);
3) Методическими рекомендациями ФСБ России от 24.12.2016 № 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);

Субъект КИИ должен провести подключение объектов КИИ к ГосСОПКА.

В сфере функционирования ГосСОПКА применяются следующие основные термины и определения:

1. 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.

2. Информационные ресурсы Российской Федерации - информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.
3. Субъекты ГосСОПКА - федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности КИИ, федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования ГосСОПКА, владельцы информационных ресурсов Российской Федерации, операторы связи, а также иные организации, осуществляющие лицензируемую деятельность в области защиты информации.
4. Зона ответственности субъекта ГосСОПКА - совокупность информационных ресурсов Российской Федерации, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак.
5. Силы обнаружения, предупреждения и ликвидации последствий компьютерных атак - уполномоченные подразделения субъектов ГосСОПКА и специально выделенные сотрудники субъектов ГосСОПКА, принимающие участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
6. Средства обнаружения, предупреждения и ликвидации последствий компьютерных атак - технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры), предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

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.

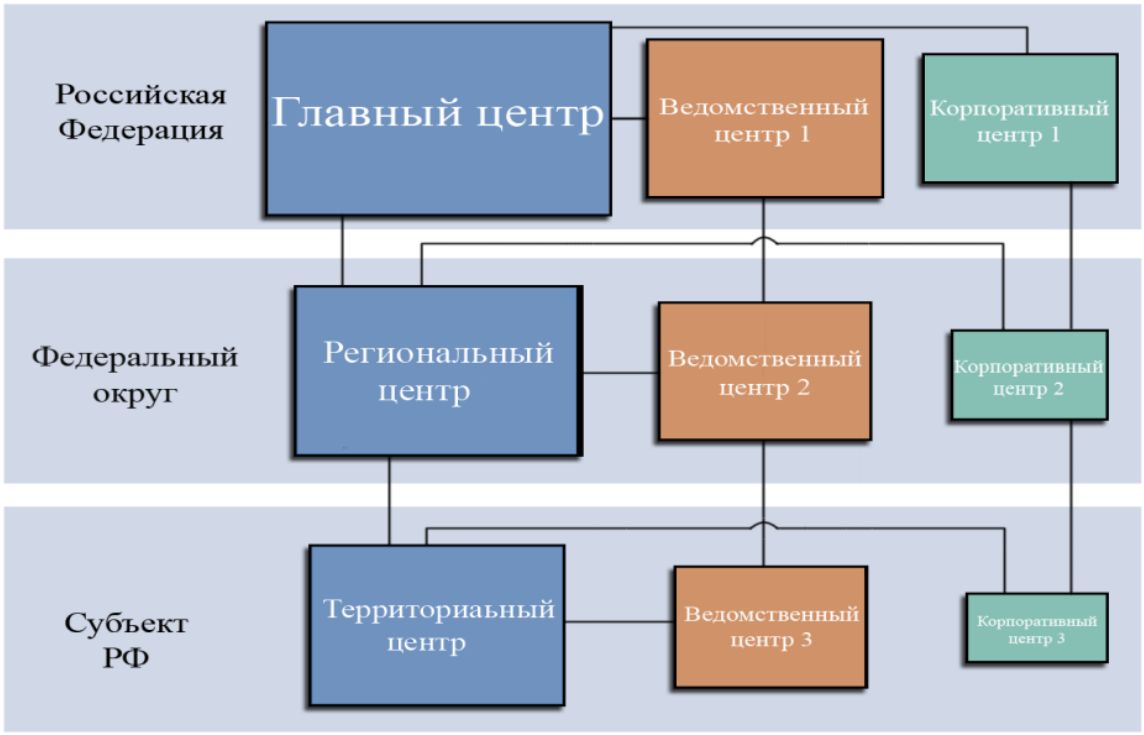

Рисунок 5. Структура ГосСОПКА

К основным задачам центров ГосСОПКА относятся:

1. Обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы.
2. Проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;
3. Проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы.

4. Сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах.
5. Осуществление взаимодействия между центрами.
6. Информирование заинтересованных лиц и субъектов ГосСОПКА по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Подключение объекта КИИ к ГосСОПКА возможно в двух вариантах:

1. Создать и подключить собственный ведомственный (корпоративный) центр (сегмент) ГосСОПКА.
2. Подключиться к ведомственному (корпоративному) центру (сегменту) ГосСОПКА (возложение части функций субъекта КИИ на внешнего контрагента).

Порядок подключения собственного ведомственного (корпоративного) центра (сегмента) к ГосСОПКА состоит из следующих этапов:

1. Заключить соглашение с ФСБ России (НКЦКИ) на создание ведомственного (корпоративного) центра (сегмента) ГосСОПКА и взаимодействие с главным центром ГосСОПКА (далее - Соглашение).
2. Выполнить организационные и технические требования к процессам, персоналу, технологиям при создании центра (сегмента) ГосСОПКА в соответствии с Методическими рекомендациями.
3. Развернуть специализированные средства взаимодействия сегмента ГосСОПКА с главным (или территориальным) центром ГосСОПКА (в приоритете для значимых объектов КИИ).

Минимальный комплект документации центра (сегмента) ГосСОПКА, необходимый для заключения Соглашения:

1. Положение о центре (сегменте) ГосСОПКА.
2. Штатное расписание центра (сегмента) ГосСОПКА.
3. Должностные инструкции специалистов центра (сегмента) ГосСОПКА.

Порядок подключения к ведомственному (корпоративному) центру (сегменту) ГосСОПКА (возложение части функций субъекта КИИ на внешнего контрагента) состоит из следующих этапов:

1. 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.
2. Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности ведомственного (корпоративного) центра ГосСОПКА.

При взаимодействии с ГосСОПКА субъектами КИИ предоставляется информация в соответствии с перечнем информации и в порядке, определяемом ФСБ России.

При этом, следует отметить, что на момент написания настоящих методических рекомендаций имеются проекты правовых актов утверждение которых необходимо отслеживать, а затем исполнить при создании, подключении и эксплуатации ведомственного (корпоративного) центра (сегмента) ГосСОПКА:

1. Проект приказа ФСБ России «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА» (http://regulation.gov.ru/projects#npa=76747).
2. Проект приказа ФСБ России «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на

компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (http://regulation.gov.ru/projects#npa=76750).

3. Проект приказа ФСБ России «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты» (http://regulation.gov.ru/projects#npa=78182).
4. Проект приказа ФСБ России «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» (http://regulation.gov.ru/projects#npa=78179).
5. Проект приказа ФСБ России «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» (http://regulation.gov.ru/projects#npa=78961).

Методические рекомендации по подключению к ГосСОПКА и созданию центров ГосСОПКА можно получить путем направления соответствующего письменного запроса в НКЦКИ.

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[6], PaaS[7], SaaS[8];
- дата-центры, предоставляющие сервис colocation[9].

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

---

[6] IaaS (Infrastructure as a Service) - инфраструктура как услуга.
[7] PaaS (Platform as a Service) - платформа как услуга
[8] SaaS (Software as a Service) - программное обеспечение как услуга
[9] Размещение оборудования в дата центре

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. Сформулировать основанные на своей, возможно пока и небольшой практике, рекомендации по реализации мероприятий по обеспечению безопасности объектов критической информационной инфраструктуры.

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

- Главы 1 и 2 - Константин Саматов
- Глава 3 - Лев Палей, Константин Саматов
- Глава 4 - Радмир Нафиков
- Глава 5 - Александр Мишурин
- Глава 6 - Николай Носов

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

Следует отметить, что 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 во второй версии данного пособия. В рамках второй версии планируется освятить следующие вопросы:

1. Проблемные вопросы при категорировании объектов КИИ. Примеры из практики проведения категорирования объектов КИИ.

2. Применение методологии Business impact analysis и Business continuity management при оценке критичности процессов и построении системы защиты объектов КИИ.

3. Практические примеры создания системы обеспечения безопасности объектов КИИ.

4. Вопросы аутсорсинга:

- что можно, что нельзя на аутсорсинг?
- как относится ФСБ (ФСТЭК) к аутсорсингу?
- какие требования к провайдеру?
- на что обратить внимание?
- какие лицензии нужны?
- что писать в договоре (SLA)?
- и многое другое.

А также, дополнить пособие чек листами для определения является ли организация субъектом КИИ.

За указанные идеи Ассоциация благодарит своего члена Андрея Прозорова.

Кроме того, Ассоциация выражает огромную благодарность работникам 2 Управления ФСТЭК России за методическую помощь в подготовке данного пособия.

ПРИЛОЖЕНИЕ. 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 тд)?

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 неприсвоение 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.