

Приложение
к приказу ПАО «Россети Ленэнерго»
от 24.04.2024 № 234



ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «РОССЕТИ ЛЕНЭНЕРГО»

ПРАВИЛА ОРГАНИЗАЦИИ

П-19.1-003-2024

Методические рекомендации и правила по выполнению требований в части категорирования объектов критической информационной инфраструктуры и выполнению требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры ПАО «Россети Ленэнерго»

Редакция 2

Санкт-Петербург
2024

I. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящих Методических рекомендациях используются термины и соответствующие им определения, введенные действующими нормативными правовыми актами Российской Федерации, а также государственными стандартами и методическими документами:

Автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления таким оборудованием и процессами;

Безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

Значимый объект критической информационной инфраструктуры – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

Комиссия по категорированию – постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры субъекта критической информационной инфраструктуры;

Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

Критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

Цифровая трансформация – оптимизация и/или изменение логики технологического процесса в результате внедрения цифровых технологий на основании анализа больших данных;

Информационные активы – любая информация о параметрах (состоянии) управляемого объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная важная (технологическая) информация),

хранящаяся на различных носителях и в различных форматах, обрабатываемая в системе и передаваемая по каналам связи.

Список сокращений

Сокращение	Определение
АСУ, АСТУ,	автоматизированные системы управления (в том числе автоматизированные рабочие места, промышленные серверы, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства) имеющее функции как локального, так и дистанционного управления, либо имеющее функционирующие интерфейсы сетевого взаимодействия, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие надежное снабжение потребителей электроэнергией, а также САЦ, ЦУС
АСУ ТП (ПС)	программно-технический комплекс средств автоматизации ПС, интегрирующий в своем составе подсистемы сбора и передачи информации о параметрах работы оборудования и устройств ПС, диагностики и мониторинга технологического оборудования, РЗА, инженерных систем, управления оборудованием и устройствами с целью реализации задач управления технологическими процессами ПС в полном объеме
АС	автоматизированная система
ГК «Россети»	группа компаний «Россети» – ПАО «Россети» и все дочерние общества ПАО «Россети»
ДО	дочерние общества ПАО «Россети»
Общество	ПАО «Россети Ленэнерго»
КИС	корпоративные информационные системы (в том числе машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности
ОКИИ	объекты критической информационной инфраструктуры – корпоративные информационные

	системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры
КИИ	ОКИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов
ЗОКИИ	значимый ОКИИ, объекту КИИ присвоена категория значимости
ИТС	корпоративные и технологические информационно-телекоммуникационные сети (в том числе телекоммуникационное оборудование, программное обеспечение, система управления, линии связи), формирующие единое информационное пространство и цифровую среду взаимодействия
ИСУ	интеллектуальные системы учета электроэнергии, системы автоматизации процессов формирования балансов и объемов услуг по передаче электрической энергии, системы планирования работ и управляемые устройства, личный кабинет потребителя
НКЦКИ	национальный координационный центр по компьютерным инцидентам Федеральной службы безопасности Российской Федерации
ИСПДн	информационная система персональных данных
СМР	строительно-монтажные работы
ТЭК	топливно-энергетический комплекс
ПНР	пуско-наладочные работы, испытания
ПС	подстанция электрическая
РЭС	район электрических сетей
ЛЭП	линия электропередачи
ПО	программное обеспечение
ТП	трансформаторная подстанция
ИС	информационные системы (в том числе машинные носители информации, автоматизированные рабочие места, серверы, средства обработки буквенно-цифровой, графической, видео- и речевой информации, микропрограммное, общесистемное, прикладное программное обеспечение), обеспечивающие устойчивость финансово-хозяйственной деятельности
ТЗ	техническое задание

II. АННОТАЦИЯ

1. ПАО «Россети Ленэнерго» (далее – Общество) является субъектом КИИ в соответствии с пунктом 8 статьи 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в сфере энергетики (электроэнергетики), а также Обществу принадлежат на праве собственности, аренды или на ином законном основании любые ИС, ИТКС и АСУ ТП, в части категорирования ОКИИ.

2. Настоящие Методические рекомендации базируются на разработанных Методических рекомендациях по определению и категорированию объектов критической информационной инфраструктуры топливно-энергетического комплекса, согласованных Минэнерго России (исх. от 31.07.2019 № ЧА-8630/15) и ФСТЭК России (исх. от 26.08.2019 № 240/25/4048), а также на утвержденной Программе информационной безопасности ПАО «Россети Ленэнерго» на 2020-2030 годы, утвержденной Советом директоров, протокол от 28.12.2020 № 43.

3. Категорирование объекта ТЭК в соответствии с Федеральным законом от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» не является основанием для непроведения процедуры категорирования в соответствии с Федеральным законом № 187-ФЗ.

4. К объектам защиты в контексте обеспечения безопасности критической информационной инфраструктуры относятся:

- корпоративные информационные системы, обеспечивающие устойчивость финансово-хозяйственной деятельности, в том числе ИСУ;
- автоматизированные системы управления, обеспечивающие надежное снабжение потребителей электроэнергией;
- корпоративные и технологические информационно-телекоммуникационные сети, формирующие единое информационное пространство и цифровую среду взаимодействия;
- сети электросвязи, используемые для организации взаимодействия объектов;
- информация конфиденциального характера, в том числе технологическая информация, представляющая коммерческую ценность в силу неизвестности третьим лицам.

5. Объекты критической информационной инфраструктуры Общества группируются по следующим категориям физических объектов электросетевого комплекса, в отношении которых требуется реализовать мероприятия по защите:

- Исполнительный аппарат, исполнительные аппараты филиалов;
- ЦОД (РЦОД);
- ЕЦУС (РЦУС), САЦ;
- РЭС филиалов, Пункт ОДУ ПС в своей зоне ответственности;

- ПС с наличием элементов SCADA верхнего уровня;
- ПС с элементами телемеханики;
- ПС без элементов телемеханики;
- все остальные отдельно размещаемые ТП, реклоузеры, УСПД, приборы учета, микропроцессорное оборудование, монтируемое на ЛЭП и опоры, смартфоны, планшеты, ноутбуки для удаленного доступа.

6. Обеспечение безопасности значимых объектов критической информационной инфраструктуры осуществляется в зависимости от установленной категории значимости ОКИИ в соответствии с требованиями, установленными Федеральным законом № 187-ФЗ, а также подзаконными актами ФСБ России и ФСТЭК России.

7. Обеспечение безопасности объектов критической информационной инфраструктуры АСТУ, ИСУ, ИТСО без установленной категории значимости осуществляется в соответствии с распоряжением ПАО «Россети» от 01.04.2016 № 140р и требованиями Единой технической политики в электросетевом комплексе.

Соответствующие требования также отражены в следующих документах:

- стандарт организации ПАО «Россети» «Каналы связи для РЗА. Технические решения для сетей 35-220 кВ» (СТО 34.01-9.2-004-2019, распоряжение ПАО «Россети» от 28.06.2019 № 284р), раздел 21;
- стандарт организации ПАО «Россети» «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ» (СТО 34.01-21-004-2019, приложение 1 к приказу ПАО «Россети» от 29.03.2019 № 64), раздел 28;
- Цифровая электрическая сеть. Требования к проектированию цифровых распределительных электрических сетей 0,4-220 кВ» (СТО 34.01-21-005-2019, приложение 2 к приказу ПАО «Россети» от 29.03.2019 № 64), раздел 9;
- Типовое задание на проектирование объектов нового строительства, расширения, реконструкции, технического перевооружения и модернизации объектов электросетевого комплекса, утверждено распоряжением ПАО «Россети» от 17.11.2017 № 628р, раздел 5.3.4.19. Решения по информационной безопасности АСУ ТП.

8. Для обеспечения безопасности объектов критической информационной инфраструктуры АСТУ без установленной категории значимости, эксплуатируемых на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды настоящие Методические рекомендации применяются с учетом Требований

к обеспечению защиты информации, утвержденных приказом ФСТЭК России от 14.03.2014 № 31.

9. Для обеспечения безопасности объектов критической информационной инфраструктуры, являющихся информационными системами персональных данных, настоящие Методические рекомендации применяются с учетом требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119, приказа ФСТЭК России от 18.02.2013 № 21.

10. Для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие Методические рекомендации применяются с учетом требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

11. В Обществе создана постоянно действующая комиссия по категорированию объектов критической информационной инфраструктуры ПАО «Россети Ленэнерго» и определены критичные процессы в рамках видов деятельности Общества.

III. Общие положения

В Обществе проводятся следующие мероприятия:

1. Включение заказчиком требований по КИИ во все ТЗ Общества по проектированию, созданию, внедрению (модернизации, строительству и т.д.) любых ИС, КИС, ИТС, АСУ ТП, АСТУ, ИТСО. Рекомендуемые требования согласно приложению 1 к настоящим Методическим рекомендациям.

2. По факту реализации требований исполнителем проводится обследование объекта защиты/системы и сбор исходных данных.

Исходными данными являются:

1) сведения об объекте/системе критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

2) процессы, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры., в рамках выполнения функций (полномочий) или

осуществления видов деятельности субъекта критической информационной инфраструктуры;

3) состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

4) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт безопасности объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта безопасности предусмотрена законодательством Российской Федерации);

5) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов;

6) угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

Результатом работ является отчет об обследовании, включающий в себя данные о назначении, функциях, условиях функционирования создаваемой (модернизируемой) ИС, КИС, ИТС, АСУ ТП, АСТУ и характере обрабатываемой информации; информация, подлежащая защите; Тип объекта (системы), какие процессы обеспечиваются или выполняются, Сведения о взаимодействии с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи; Сведения о программных и программно-аппаратных средствах (планируемых), наличие паспорта безопасности объекта топливно-энергетического комплекса, текущие и предполагаемые Архитектурная и Функциональная схемы, выводы о состоянии объекта и рекомендации.

3. Исполнитель на базе исходных данных разрабатывает Модели угроз и нарушителя безопасности информации:

3.1. Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными

системами управления, информационно-телекоммуникационными сетями (далее – архитектура значимого объекта), а также особенностей функционирования значимого объекта.

Анализ угроз безопасности информации должен включать:

- 1) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
- 2) анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
- 3) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
- 4) оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

3.2. В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085, (www.bdu.fstec.ru) ФСТЭК России, а также источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

3.3. По результатам анализа угроз безопасности информации могут быть разработаны рекомендации по корректировке архитектуры значимого объекта и организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

3.4. Модель угроз и нарушителя безопасности информации должна содержать:

- 1) наименование объекта;
- 2) описание объекта защиты;
- 3) состав основных технических средств объекта защиты:
 - серверы (серверы системы SCADA, архивные, сервер единого времени, сервер телемеханики и другие);
 - АРМ пользователей (операторов, машинистов, инженеров);
 - телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, преобразователи интерфейсов, мультиплексоры);
 - каналы связи;
 - управляющие устройства (ПЛК, устройства связи с объектами и др.);
 - исполнительные устройства (электротехническое оборудование, датчики, счетчики, КИП и ЗРА, устройства РЗА, измерительные преобразователи).

- программное обеспечение (микропрограммы, системное и прикладное ПО), а также информационные активы АСУ;
- 4) краткое описание архитектуры значимого объекта и схема;
- 5) классификацию нарушителей;
- 6) список уязвимостей объекта защиты;
- уязвимости системного и прикладного ПО;
- уязвимости аппаратного обеспечения;
- уязвимости протоколов сетевого взаимодействия;
- уязвимости, вызванные недостатками организации обеспечения ИБ систем АСУ при эксплуатации и обслуживании систем АСУ;
- 7) состав характеристики источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта;
- 8) последствия нарушения свойств безопасности информации;
- 9) вывод с определением соответствующих мер защиты.

3.5. Описание каждой угрозы безопасности информации должно включать:

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

3.6. Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

3.7. Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085, такие как:

- Методика оценки угроз безопасности информации, утвержденная ФСТЭК России 05.02.2021;
- Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18.05.2007;
- Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 18.05.2007;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная ФСТЭК России, 15.02.2008;

– ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19.08.2015 № 1180-ст;

– ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19.08.2015 № 1181-ст.

4. Исполнитель определяет критичные бизнес процессы, которые обеспечиваются проектируемым объектом КИИ (из определенного в Обществе перечня процессов, приложение 2 к настоящим Методическим рекомендациям).

5. Исполнителем производится разработка проекта документа «Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» (приложение 3 к настоящим Методическим рекомендациям).

6. Исполнителем производится формирование проекта АКТа категорирования объектов критической информационной инфраструктуры (приложение 4 к настоящим Методическим рекомендациям).

7. Комиссией по категорированию объектов критической информационной инфраструктуры проводится рассмотрение исходных данных, отчета об обследовании, схем, сведений, Акта другой необходимой информации и принимается решение о присвоении каждому из ОКИИ одной из категории значимости либо об отсутствии необходимости присвоения им категорий значимости.

7.1. Определение категорий значимости объектов критической информационной инфраструктуры (далее – категория значимости) осуществляется на основании показателей критериев значимости объектов критической информационной инфраструктуры и их значений, предусмотренных перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденным Постановлением Правительства Российской Федерации 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» (далее – перечень показателей критериев значимости, показатели критериев значимости).

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

7.3. Категорирование включает в себя:

1) определение процессов, указанных в пункте 7.2 настоящих Методических рекомендаций, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

2) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов 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 (далее - критические процессы);

3) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

4) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

5) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

6) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

7.4. В случае если ни один из показателей критериев значимости неприменим для объекта критической информационной инфраструктуры или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.

7.5. Формирование организационно-технических требований, выбор, контроль и приемка внедряемых решений, включая средства и методы защиты, осуществляется рабочими группами, сформированными в соответствии с ОРД ГК «Россети», в том числе на основе результатов

категорирования ОКИИ, выполненных комиссиями по категорированию ПАО «Россети Ленэнерго».

7.6. В отношении создаваемого объекта критической информационной инфраструктуры, в том числе в рамках создания объекта капитального строительства, категория значимости определяется при формировании заказчиком, техническим заказчиком или застройщиком требований к объекту критической информационной инфраструктуры с учетом имеющихся исходных данных о критических процессах субъекта критической информационной инфраструктуры.

7.7. Для создаваемого объекта критической информационной инфраструктуры, указанного в пункте 7.6 настоящих Методических рекомендаций, категория значимости может быть уточнена в ходе его проектирования.

7.8. Для объектов, принадлежащих одному субъекту критической информационной инфраструктуры, но используемых для целей контроля и управления технологическим и (или) производственным оборудованием, принадлежащим другому субъекту критической информационной инфраструктуры, категорирование осуществляется на основе исходных данных, представляемых субъектом критической информационной инфраструктуры, которому принадлежит технологическое и (или) производственное оборудование.

7.9. Субъект критической информационной инфраструктуры не реже чем один раз в 5 лет, а также в случае изменения показателей критериев значимости объектов критической информационной инфраструктуры или их значений осуществляет пересмотр установленных категорий значимости или решений об отсутствии необходимости присвоения указанным объектам таких категорий в соответствии с настоящими Методическими рекомендациями. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в федеральный орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

8. Разработка и проектирование системы защиты (на стадии ПД и РД), установление требований к обеспечению безопасности значимого объекта и разработка организационных и технических мер по обеспечению безопасности значимого объекта.

8.1. При проектировании значимых объектов критической информационной инфраструктуры необходимо учесть и разработать все необходимые меры, требуемые в соответствии с предварительной категорией объекта (согласно действующей редакции приказа ФСТЭК от 25.12.2017 № 239), преимущественно использовать собственные и действующие системы информационной безопасности Общества, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак

и реагирования на компьютерные инциденты для обеспечения безопасности объектов критической информационной инфраструктуры.

8.2. Требования к обеспечению безопасности включаются в техническое задание на создание значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, которые должны содержать:

- 1) цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;
- 2) категорию значимости значимого объекта;
- 3) перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;
- 4) перечень типов объектов защиты значимого объекта;
- 5) требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта;
- 6) стадии (этапы работ) создания подсистемы безопасности значимого объекта;
- 7) требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
- 8) требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);
- 9) требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями;
- 10) требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта.

8.3. В случае если значимый объект создается в рамках объекта капитального строительства, требования к обеспечению безопасности значимого объекта задаются проектировщиком\застройщиком и оформляются в виде приложения к заданию на проектирование (реконструкцию/ модернизацию) объекта капитального строительства.

8.4. При определении требований к обеспечению безопасности значимого объекта учитываются положения организационно-распорядительных документов по обеспечению безопасности значимых объектов, разрабатываемых Обществом в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ (далее – организационно-распорядительные документы по безопасности значимых объектов).

8.5. При проектировании подсистемы безопасности значимого объекта:

- 1) определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;
- 2) определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);
- 3) определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта;
- 4) определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;
- 5) осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
- 6) разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
- 7) определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;
- 8) определяются меры по обеспечению безопасности при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

8.6. В случае если в ходе проектирования подсистемы безопасности значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения.

8.7. Результаты проектирования подсистемы безопасности значимого объекта отражаются в проектной документации на значимый объект (подсистему безопасности значимого объекта), разрабатываемой в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта.

8.8. В процессе проектирования значимого объекта его категория значимости может быть уточнена. (исполнителем выполняются действия в соответствии с пунктами 3, 4 и 5)

8.9. В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды. Тестирование должно быть направлено на:

- обеспечение работоспособности и совместимости выбранных средств защиты информации с программными и аппаратными средствами значимого объекта;
- практическую отработку выполнения средствами защиты информации функций безопасности, а также выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в соответствии с пунктами 12.1 – 12.9 настоящих Методических рекомендаций;
- исключение влияния подсистемы безопасности на функционирование значимого объекта.

8.10. Макетирование подсистемы безопасности значимого объекта и ее тестирование может проводиться с использованием средств и методов моделирования, а также с использованием технологий виртуализации.

8.11. При проектировании подсистем безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями, настоящие Требования применяются с учетом Требований к проектированию сетей электросвязи, утвержденных приказом Минкомсвязи России от 09.03.2017 № 101, а также иных нормативных правовых актов федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи.

8.12. Разработка рабочей (эксплуатационной) документации на значимый объект осуществляется в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта на основе проектной документации.

8.13. Рабочая (эксплуатационная) документация на значимый объект должна содержать:

- 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).

8.14. Состав и формы рабочей (эксплуатационной) документации определяются в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта.

В зависимости от категории значимости, требуемого уровня защищенности и актуальных угроз безопасности информации в системе безопасности объектов критической информационной инфраструктуры должны быть реализованы следующие организационные и технические меры:

- 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), включая комплексные решения для защиты от атак нулевого дня (TDS);
- 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).

8.15. Технические меры по обеспечению информационной безопасности реализуются посредством преимущественного использования программного обеспечения и СУБД из реестра Российского программного обеспечения, а также программных и программно-аппаратных средств – средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение):

- средства защиты информации от несанкционированного доступа к АРМ, Ноутбукам, Серверам (включая DLP, а также встроенные в общесистемное, прикладное программное обеспечение функции защиты информации от НСД);
- средства защиты информации от несанкционированного доступа к информации, обрабатываемой на смартфонах, планшетах;
- межсетевые экраны уровня сети, уровня логических границ сети;
- межсетевые экраны уровня промышленной сети;
- средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети;
- межсетевые экраны уровня веб-сервера;

- средства однонаправленной передачи данных (Дата-диод);
- средствами обнаружения (предотвращения) вторжений (компьютерных атак) уровня узла;
- средства антивирусной защиты общего назначения;
- средства антивирусной защиты АРМ производственного персонала, промышленных серверов;
- средства антивирусной защиты уровня сети, веб-сервера;
- средства (системы) контроля (анализа) защищенности;
- средства мониторинга и корреляции событий безопасности;
- средства управления инцидентами;
- средства предупреждения компьютерных атак;
- средства защиты каналов передачи данных;
- средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа, двухфакторной аутентификации;
- средства резервного копирования, в том числе средства создания и хранения резервных копий;
- средства управления ключевой информацией.

8.16. Базовый (минимальный) набор технических мер включает:

- средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение);
- межсетевые экраны уровня сети;
- средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети;
- средства антивирусной защиты потовых и веб-серверов, файловых хранилищ и рабочих станций;
- средства защиты каналов передачи данных;
- средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа, двухфакторной аутентификации;
- средства резервного копирования.

Если объект/система не имеет категорию значимости по ОКИИ, то:

- для АС (систем АСТУ и связи, а также систем, обеспечивающих технологические процессы) применяются требования Приказа ФСТЭК от 14.03.2014 № 31 «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». Также обеспечение безопасности объектов критической информационной инфраструктуры АСТУ, ИСУ, ИТСО без установленной категории значимости осуществляется в соответствии с распоряжением

ПАО «Россети» от 01.04.2016 № 140р и требованиями Единой технической политики в электросетевом комплексе;

- для ИС (Информационных систем и ИТ-инфраструктуры, обеспечивающих корпоративные процессы) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»; Приказ ФСТЭК от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;

- ГОСТ 34.602-2020 «Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (введен в действие Приказом Росстандарта от 19.11.2021 № 1522-ст);

- ГОСТ 34.201-2020 «Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» (введен в действие Приказом Росстандарта от 19.11.2021 № 1521-ст);

- ГОСТ Р 59793-2021 «Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» (утв. и введен в действие Приказом Росстандарта от 25.10.2021 № 1285-ст);

- РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс Стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».

При проектировании преимущественно использовать действующие системы информационной безопасности Общества.

8.17. В случае если значимый объект является государственной информационной системой, в иных случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры, оценка значимого объекта и его подсистемы безопасности проводится в форме аттестации значимого объекта в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными Приказом ФСТЭК России от 11.02.2013 № 17.

9. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

9.1. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта организуется субъектом критической информационной инфраструктуры в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, стандартами организаций и включает:

- 1) установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств;
- 2) разработку организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта;
- 3) внедрение организационных мер по обеспечению безопасности значимого объекта;
- 4) предварительные испытания значимого объекта и его подсистемы безопасности;
- 5) опытную эксплуатацию значимого объекта и его подсистемы безопасности;
- 6) анализ уязвимостей значимого объекта и принятие мер по их устранению;
- 7) приемочные испытания значимого объекта и его подсистемы безопасности.

По решению субъекта критической информационной инфраструктуры к разработке и внедрению организационных и технических мер по обеспечению безопасности значимого объекта может привлекаться лицо, эксплуатирующее (планирующее эксплуатировать) значимый объект.

9.2. Установка и настройка средств защиты информации должна проводиться в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, а также в соответствии с эксплуатационной документацией на отдельные средства защиты информации.

При установке и настройке средств защиты информации должно быть обеспечено выполнение ограничений на эксплуатацию этих средств защиты информации, в случае их наличия в эксплуатационной документации.

9.3. Разрабатываемые организационно-распорядительные документы по безопасности значимого объекта должны определять правила и процедуры реализации отдельных организационных и (или) технических мер (политик безопасности), разработанных и внедренных в рамках подсистемы безопасности значимого объекта.

Организационно-распорядительные документы по безопасности значимого объекта должны в том числе устанавливать правила 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.

Состав и формы организационно-распорядительных документов по безопасности значимых объектов определяются Обществом с учетом особенностей его деятельности.

9.4. При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляются:

- 1) организация контроля физического доступа к программно-аппаратным средствам значимого объекта и его линиям связи;
- 2) реализация правил разграничения доступа, регламентирующих 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;
- 3) проверка полноты и детальности описания в организационно-распорядительных документах по безопасности значимых объектов действий пользователей и администраторов значимого объекта по реализации организационных мер;
- 4) определение администратора безопасности значимого объекта;
- 5) отработка действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.

9.5. Предварительные испытания значимого объекта и его подсистемы безопасности должны проводиться в соответствии с программой и методиками предварительных испытаний и включать проверку работоспособности подсистемы безопасности значимого объекта и отдельных средств защиты информации, оценку выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в соответствии с пунктами 12.1 – 12.9 настоящих Методических рекомендаций, оценку влияния подсистемы безопасности на функционирование значимого объекта при проектных режимах его работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации значимого объекта и его подсистемы безопасности.

9.6. Опытная эксплуатация значимого объекта и его подсистемы безопасности должна проводиться в соответствии с программой и методиками опытной эксплуатации и включать проверку функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер, а также знаний и умений пользователей и администраторов, необходимых для эксплуатации значимого объекта и его подсистемы безопасности. По результатам опытной эксплуатации принимается решение о возможности (или невозможности) проведения приемочных испытаний значимого объекта и его подсистемы безопасности.

9.7. В ходе приемочных испытаний значимого объекта и его подсистемы безопасности должен быть проведен комплекс организационных

и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности настоящим Требованиям, а также требованиям технического задания на создание значимого объекта и (или) технического задания (частного технического задания) на создание подсистемы безопасности значимого объекта.

9.8. В качестве исходных данных при приемочных испытаниях используются модель угроз безопасности информации, результаты (акт) категорирования, техническое задание на создание (модернизацию) значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, проектная и рабочая (эксплуатационная) документация на значимый объект, организационно-распорядительные документы по безопасности значимых объектов, результаты анализа уязвимостей значимого объекта, материалы предварительных испытаний и опытной эксплуатации, а также иные документы, разрабатываемые в соответствии с настоящими Методическими рекомендациями и требованиями стандартов организации.

9.9. Приемочные испытания значимого объекта и его подсистемы безопасности проводятся в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний значимого объекта и его подсистемы безопасности с выводом о ее соответствии установленным требованиям включаются в акт приемки значимого объекта в эксплуатацию.

9.10. Ввод в эксплуатацию значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии значимого объекта установленным требованиям по обеспечению безопасности.

10. Обеспечение безопасности объекта\системы в ходе его эксплуатации

10.1. Обеспечение безопасности в ходе эксплуатации значимого объекта осуществляется в соответствии с эксплуатационной документацией и организационно-распорядительными документами по безопасности значимого объекта и должно включать реализацию следующих мероприятий:

- 1) планирование мероприятий по обеспечению безопасности значимого объекта;
- 2) анализ угроз безопасности информации в значимом объекте и последствий от их реализации;
- 3) управление (администрирование) подсистемой безопасности значимого объекта;
- 4) управление конфигурацией значимого объекта и его подсистемой безопасности;
- 5) реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;

6) обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта;

7) информирование и обучение персонала значимого объекта;

8) контроль за обеспечением безопасности значимого объекта.

10.2. В ходе планирования мероприятий по обеспечению безопасности значимого объекта осуществляются:

1) определение лиц, ответственных за планирование и контроль мероприятий по обеспечению безопасности значимого объекта;

2) разработка, утверждение и актуализация плана мероприятий по обеспечению безопасности значимого объекта;

3) определения порядка контроля выполнения мероприятий по обеспечению безопасности значимого объекта, предусмотренных утвержденным планом.

10.3. Планирование мероприятий по обеспечению безопасности значимого объекта должно осуществляться в рамках процесса планирования, внедренного в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ.

10.4. В ходе анализа угроз безопасности информации в значимом объекте и возможных последствий их реализации осуществляются:

1) анализ уязвимостей значимого объекта, возникающих в ходе его эксплуатации;

2) анализ изменения угроз безопасности информации в значимом объекте, возникающих в ходе его эксплуатации;

3) оценка возможных последствий реализации угроз безопасности информации в значимом объекте.

10.5. Периодичность проведения указанных работ определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов с учетом категории значимости объекта и особенностей его функционирования.

10.6. В ходе управления (администрирования) подсистемой безопасности значимого объекта осуществляются:

1) определение лиц, ответственных за управление (администрирование) подсистемой безопасности значимого объекта;

2) управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в значимом объекте;

3) управление средствами защиты информации значимого объекта;

4) управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта;

5) централизованное управление подсистемой безопасности значимого объекта (при необходимости);

6) мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее – события безопасности);

7) сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по безопасности значимого объекта.

10.7. В ходе управления конфигурацией значимого объекта и его подсистемы безопасности для целей обеспечения его безопасности осуществляются:

1) определение лиц, которым разрешены действия по внесению изменений в конфигурацию значимого объекта и его подсистемы безопасности, и их полномочий;

2) определение компонентов значимого объекта и его подсистемы безопасности, подлежащих изменению в рамках управления конфигурации (идентификация объектов управления конфигурации): программно-аппаратные, программные средства, включая средства защиты информации, и их настройки, и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

3) управление изменениями значимого объекта и его подсистемы безопасности: разработка параметров настройки, обеспечивающих безопасность значимого объекта, анализ потенциального воздействия планируемых изменений на обеспечение безопасности значимого объекта, санкционирование внесения изменений в значимый объект и его подсистему безопасности, документирование действий по внесению изменений в значимый объект и сохранение данных об изменениях конфигурации;

4) контроль действий по внесению изменений в значимый объект и его подсистему безопасности.

10.8. Реализованные процессы управления изменениями значимого объекта и его подсистемы безопасности должны охватывать процессы гарантийного и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, значимого объекта.

10.9. Реагирование на компьютерные инциденты осуществляется в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона № 187-ФЗ.

10.10. Для реагирования на компьютерные инциденты определяются работники, ответственные за выявление компьютерных инцидентов и реагирование на них, и определяются их функции.

10.11. Для обеспечения действий в нештатных ситуациях при эксплуатации значимого объекта осуществляются:

1) планирование мероприятий по обеспечению безопасности значимого объекта на случай возникновения нештатных ситуаций;

2) обучение и отработка действий персонала по обеспечению безопасности значимого объекта в случае возникновения нештатных ситуаций;

3) создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций;

4) резервирование программных и программно-аппаратных средств, в том числе средств защиты информации, каналов связи на случай возникновения нештатных ситуаций;

5) обеспечение возможности восстановления значимого объекта и (или) его компонентов в случае возникновения нештатных ситуаций;

6) определение порядка анализа возникших нештатных ситуаций и принятия мер по недопущению их повторного возникновения.

10.12. В ходе информирования и обучения персонала значимого объекта осуществляются:

1) информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации значимого объекта;

2) доведение до персонала требований по обеспечению безопасности значимых объектов, а также положений организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся;

3) обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;

4) контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности критической информационной инфраструктуры.

10.13. Периодичность проведения указанных мероприятий устанавливается субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимого объекта с учетом категории значимости и особенностей функционирования значимого объекта.

10.14. В ходе контроля за обеспечением безопасности значимого объекта осуществляются:

1) контроль (анализ) защищенности значимого объекта с учетом особенностей его функционирования;

2) анализ и оценка функционирования значимого объекта и его подсистемы безопасности, включая анализ и устранение уязвимостей и иных недостатков в функционировании подсистемы безопасности значимого объекта;

3) документирование процедур и результатов контроля за обеспечением безопасности значимого объекта;

4) принятие решения по результатам контроля за обеспечением безопасности значимого объекта о необходимости доработки (модернизации) его подсистемы безопасности.

11. Обеспечение безопасности значимого объекта при выводе его из эксплуатации

11.1. Обеспечение безопасности значимого объекта при выводе его из эксплуатации или после принятия решения об окончании обработки информации осуществляется субъектом критической информационной инфраструктуры в соответствии с эксплуатационной документацией на значимый объект и организационно-распорядительными документами по безопасности значимого объекта.

11.2. Обеспечение безопасности значимого объекта при выводе его из эксплуатации должно предусматривать:

- 1) архивирование информации, содержащейся в значимом объекте;
- 2) уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации;
- 3) уничтожение или архивирование данных об архитектуре и конфигурации значимого объекта;
- 4) архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта.

11.3. Архивирование информации, содержащейся в значимом объекте, должно осуществляться в случае ее дальнейшего использования в деятельности субъекта критической информационной инфраструктуры.

11.4. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации осуществляется в случае обработки значимым объектом информации ограниченного доступа или в случае принятия такого решения субъектом критической информационной инфраструктуры.

11.5. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю значимого объекта или в иные организации для ремонта, технического обслуживания или дальнейшего уничтожения.

11.6. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, производится или физическое уничтожение самих машинных носителей информации или уничтожение содержащейся на машинных носителях информации.

11.7. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации подлежит документированию в соответствии с организационно-распорядительными документами по безопасности значимого объекта.

11.8. При выводе значимого объекта из эксплуатации должен быть осуществлен сброс настроек программных и программно-аппаратных средств,

в том числе средств защиты информации, удалена информация о субъектах доступа и объектах доступа, удалены учетные записи пользователей, а также идентификационная и аутентификационная информация субъектов доступа.

11.9. При выводе значимого объекта из эксплуатации вся эксплуатационная документация на значимый объект и его подсистему безопасности, эксплуатационная документация на отдельные средства защиты информации подлежит архивному хранению.

11.10. Сроки хранения документации определяются субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимого объекта.

11.11. По решению субъекта критической информационной инфраструктуры эксплуатационная документация на значимый объект и его подсистему безопасности, а также организационно-распорядительные документы по безопасности значимого объекта (инструкции, руководства) могут быть уничтожены. В этом случае факт уничтожения подлежит документированию субъектом критической информационной инфраструктуры с указанием наименования, состава документов, способов и даты их уничтожения.

12. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов.

12.1. Технические меры по обеспечению безопасности в значимом объекте реализуются посредством использования программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов – средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение), а также обеспечения безопасности программного обеспечения и программно-аппаратных средств, применяемых в значимых объектах.

При этом в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов (при их наличии).

12.2. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры

самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

12.3. В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации средств защиты информации:

1) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;

2) в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;

3) в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 категории значимости применяются сертифицированные средства защиты информации, соответствующие 4 или более высокому уровню доверия. В значимых объектах 2 категории значимости применяются сертифицированные средства защиты информации, соответствующие 5 или более высокому уровню доверия. В значимых объектах 3 категории значимости применяются сертифицированные средства защиты информации, соответствующие 6 или более высокому уровню доверия.

Классы защиты и уровни доверия определяются в соответствии с нормативными правовыми актами ФСТЭК России, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 № 1085.

При использовании в значимом объекте средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Методических рекомендаций.

12.4. При проектировании вновь создаваемых или модернизируемых значимых объектов 1 категории значимости в качестве граничных маршрутизаторов, имеющих доступ к информационно-телекоммуникационной сети «Интернет», выбираются маршрутизаторы, сертифицированные на соответствие требованиям по безопасности информации (в части реализованных в них функций безопасности).

В случае отсутствия технической возможности применения в значимых объектах 1 категории значимости граничных маршрутизаторов, сертифицированных на соответствие требованиям по безопасности информации, функции безопасности граничных маршрутизаторов подлежат оценке на соответствие требованиям по безопасности в рамках приемки или испытаний значимых объектов.

Обоснование отсутствия технической возможности приводится в проектной документации на значимые объекты (подсистемы безопасности значимых объектов), разрабатываемой в соответствии с техническим заданием на создание значимых объектов и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимых объектов.

12.5. Средства защиты информации, оценка соответствия которых проводится в форме испытаний или приемки, должны соответствовать требованиям к функциям безопасности, установленным в соответствии с подпунктом «8» пункта 8.2 настоящих Методических рекомендаций.

Не встроенные в общесистемное и прикладное программное обеспечение средства защиты информации, оценка соответствия которых проводится в форме испытаний или приемки, дополнительно к указанным требованиям должны соответствовать 6 или более высокому уровню доверия.

Испытания (приемка) средств защиты информации на соответствие требованиям к уровню доверия и требованиям к функциям безопасности проводятся на этапе предварительных испытаний в соответствии с пунктом 8.9 настоящих Методических рекомендаций.

Испытания (приемка) проводятся отдельно или в составе значимого объекта. Программа и методики испытаний (приемки) утверждаются субъектом критической информационной инфраструктуры в случае самостоятельного проведения испытаний. В случае проведения испытаний иным лицом, программа и методики испытаний (приемки) утверждаются этим лицом по согласованию с субъектом критической информационной инфраструктуры.

По результатам испытаний (приемки) средства защиты информации оформляется протокол испытаний, в котором указываются:

- дата и место проведения испытаний (приемки);
- описание испытываемого средства защиты информации;
- описание проведенных испытаний;
- результаты испытаний по каждому испытываемому параметру (характеристике);
- выводы о соответствии (несоответствии) средства защиты информации требованиям по безопасности информации.

Протокол испытаний утверждается субъектом критической информационной инфраструктуры в случае самостоятельного проведения испытаний. В ином случае протокол испытаний утверждается лицом,

проводившим испытания, и представляется субъекту критической информационной инфраструктуры на этапе приемочных испытаний для принятия решения о возможности применения средства защиты информации в значимом объекте.

Испытания (приемка), предусмотренные настоящим пунктом, проводятся в отношении средств защиты информации, планируемых к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимых объектов.

12.6. Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) значимого объекта и обеспечивающее выполнение его функций по назначению (далее – программное обеспечение), должно соответствовать следующим требованиям по безопасности:

12.6.1. Требования по безопасной разработке программного обеспечения:

- наличие руководства по безопасной разработке программного обеспечения;
- проведение анализа угроз безопасности информации программного обеспечения;
- наличие описания структуры программного обеспечения на уровне подсистем и результатов сопоставления функций программного обеспечения и интерфейсов, описанных в функциональной спецификации, с его подсистемами (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

12.6.2. Требования к испытаниям по выявлению уязвимостей в программном обеспечении:

- проведение статического анализа исходного кода программы;
- проведение фаззинг-тестирования программы, направленного на выявление в ней уязвимостей;
- проведение динамического анализа кода программы (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

12.6.3. Требования к поддержке безопасности программного обеспечения:

- наличие процедур отслеживания и исправления обнаруженных ошибок и уязвимостей программного обеспечения;
- определение способов и сроков доведения разработчиком (производителем) программного обеспечения до его пользователей информации об уязвимостях программного обеспечения, о компенсирующих мерах по защите информации или ограничениях по применению программного обеспечения, способов получения пользователями

программного обеспечения его обновлений, проверки их целостности и подлинности;

- наличие процедур информирования субъекта критической информационной инфраструктуры об окончании производства и (или) поддержки программного обеспечения (для программного обеспечения, планируемого к применению в значимых объектах 1 категории значимости).

12.7. Выполнение требований по безопасности, указанных в подпунктах 12.6.1 – 12.6.3 пункта 12.6 настоящих Методических рекомендаций, оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции или ремонту) значимого объекта и (или) обеспечению его безопасности, на этапе проектирования значимого объекта на основе результатов анализа материалов и документов, представляемых разработчиком (производителем) программного обеспечения в соответствии с техническим заданием (частным техническим заданием), разрабатываемым в соответствии с пунктом 8.2 настоящих Методических рекомендаций.

Результаты оценки включаются в проектную документацию на значимый объект (подсистему безопасности значимого объекта) и представляются субъекту критической информационной инфраструктуры.

12.8. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны эксплуатироваться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией.

12.9. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны быть обеспечены гарантийной и (или) технической поддержкой.

При выборе программных и программно-аппаратных средств, в том числе средств защиты информации, необходимо учитывать наличие ограничений на возможность их применения субъектом критической информационной инфраструктуры на любом из принадлежащих ему значимых объектов критической информационной инфраструктуры со стороны разработчиков (производителей) или иных лиц.

В значимом объекте не допускаются:

- наличие удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, а также работниками его дочерних и зависимых обществ;

- наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры, его дочерних и зависимых обществ;

- передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны субъекта критической информационной инфраструктуры.

В случае технической невозможности исключения удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, в значимом объекте принимаются организационные и технические меры по обеспечению безопасности такого доступа, предусматривающие:

- определение лиц и устройств, которым разрешен удаленный доступ к программным и программно-аппаратным средствам значимого объекта, предоставление им минимальных полномочий при доступе к этим средствам;
- контроль доступа к программным и программно-аппаратным средствам значимого объекта;
- защиту информации и данных при их передаче по каналам связи при удаленном доступе к программным и программно-аппаратным средствам значимого объекта;
- мониторинг и регистрацию действий лиц, которым разрешен удаленный доступ к программным и программно-аппаратным средствам значимого объекта, а также инициируемых ими процессов, анализ этих действий в целях выявления фактов правонарушений;
- обеспечение невозможности отказа лиц от выполненных действий при осуществлении удаленного доступа к программным и программно-аппаратным средствам значимого объекта.

Дополнительные рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры в приложении 5 к настоящим Методическим рекомендациям.

В значимом объекте могут приниматься дополнительные организационные и технические меры по обеспечению безопасности удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, направленные на блокирование (нейтрализацию) угроз безопасности информации, приведенных в модели угроз безопасности информации, разрабатываемой в соответствии с пунктом 11.1 настоящих Методических рекомендаций.

Входящие в состав значимого объекта 1 и 2 категорий значимости программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях субъекта

критической информационной инфраструктуры (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации).

13. Порядок согласования подключения значимого объекта критической информационной инфраструктуры Общества к сети связи общего пользования.

13.1. Настоящие Методические рекомендации устанавливают процедуру согласования Обществом с ФСТЭК России подключения значимого значимый объекта к сети связи общего пользования, осуществляемого в соответствии с пунктом 3 Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденных Постановлением Правительства Российской Федерации от 08.06.2019 № 743.

13.2. Согласование подключения создаваемого значимого объекта осуществляется до ввода его в действие на этапе, определяемом субъектом критической информационной инфраструктуры. Согласование подключения действующего значимого объекта осуществляется до заключения договора с оператором связи, предусмотренного пунктом 6 Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, утвержденных Постановлением Правительства Российской Федерации от 08.06.2019 № 743.

13.3. В случае если значимый объект на момент его включения в реестр значимых объектов критической информационной инфраструктуры Российской Федерации (далее – реестр значимых объектов критической информационной инфраструктуры) подключен к сети связи общего пользования, согласование ФСТЭК России в соответствии с настоящими Методическими рекомендациями не требуется.

13.4. Для согласования подключения значимого объекта к сети связи общего пользования субъект критической информационной инфраструктуры представляет посредством почтового отправления или непосредственно в ФСТЭК России следующие сведения:

1) полное и сокращенное (при наличии) наименование субъекта критической информационной инфраструктуры, его адрес в пределах места нахождения, идентификационный номер налогоплательщика;

2) наименование значимого объекта, в отношении которого планируется подключение к сети связи общего пользования, его регистрационный номер в реестре значимых объектов критической информационной инфраструктуры;

3) цель подключения значимого объекта к сети связи общего пользования (оказание услуг, управление, контроль за технологическим,

производственным оборудованием (исполнительными устройствами), доступ к информационным ресурсам, передача информации (данных), обеспечение информационного взаимодействия между сегментами значимого объекта либо с другим значимым объектом и иными системами (сетями), иная цель);

4) планируемый тип подключения значимого объекта к сети связи общего пользования (проводной, беспроводной), наименования протоколов сетевого взаимодействия, используемых для целей подключения;

5) наименование, модель программно-аппаратных и (или) программных средств обеспечения безопасности значимого объекта, применяемых при его подключении к сети связи общего пользования (далее – средства), с указанием версий программного обеспечения средств;

6) номера сертификатов соответствия, имеющихся на средствах, и даты их выдачи (для средств, прошедших оценку соответствия в форме обязательной сертификации);

7) реквизиты протоколов испытаний, содержащих результаты оценки соответствия средств (для средств, прошедших оценку соответствия в форме испытаний, приемки).

Образец сведений о значимом объекте критической информационной инфраструктуры Российской Федерации, в отношении которого планируется подключение к сети связи общего пользования, приведен в приложении 6 к настоящим Методическим рекомендациям.

13.5. К сведениям прилагаются следующие документы:

1) копия модели угроз безопасности информации значимого объекта, разработанной в соответствии с пунктом 11 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных приказом ФСТЭК России от 25.12.2017 № 239 (с изменениями, внесенными приказами ФСТЭК России от 09.08.2018 № 138 и от 26.03.2019 № 60), и утвержденной руководителем субъекта критической информационной инфраструктуры или уполномоченным им лицом;

2) копии протоколов испытаний, содержащих результаты оценки соответствия средств (для средств, прошедших оценку соответствия в форме испытаний, приемки);

3) схема организации связи (в случае предоставления оператором связи субъекту критической информационной инфраструктуры цифровых каналов связи).

13.6. Сведения оформляются на русском языке (допускается указывать на иностранном языке фирменные наименования средств), подписываются руководителем субъекта критической информационной инфраструктуры или уполномоченным им лицом. Сведения с сопроводительным письмом направляются в ФСТЭК России на бумажном носителе с приложением электронной копии сведений в формате файлов электронных таблиц (.ods). Документы, указанные в абзацах одиннадцатом – тринадцатом пункта 4

настоящих Методических рекомендаций, представляются на бумажном носителе.

13.7. ФСТЭК России на основе представленных субъектом критической информационной инфраструктуры сведений и документов оценивает достаточность применяемых при подключении значимого объекта к сети связи общего пользования средств в соответствии с Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом ФСТЭК России от 21.12.2017 № 235 (с изменениями, внесенными приказом ФСТЭК России от 27.03.2019 № 64), и Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25.12.2017 № 239.

13.8. В случае если представленные субъектом критической информационной инфраструктуры сведения недостаточны для принятия решения о согласовании либо об отказе в согласовании подключения значимого объекта к сети связи общего пользования, ФСТЭК России запрашивает дополнительные сведения по безопасности значимого объекта в целях уточнения состава актуальных для значимого объекта угроз безопасности информации и применяемых в нем средств защиты информации.

13.9. Субъект критической информационной инфраструктуры представляет запрошенные сведения посредством почтового отправления или непосредственно в ФСТЭК России.

13.10. Основаниями для отказа в согласовании подключения значимого объекта к сети связи общего пользования являются:

- представление субъектом критической информационной инфраструктуры в ФСТЭК России неполного объема сведений и документов, указанных в пункте 13.4 настоящих Методических рекомендаций, или непредставление дополнительных сведений;

- несоответствие наименований, моделей, используемых версий программного обеспечения средств наименованиям, моделям, версиям программного обеспечения средств, указанным в сертификатах соответствия (для средств, прошедших оценку соответствия в форме обязательной сертификации);

- несоответствие наименований, моделей, используемых версий программного обеспечения средств наименованиям, моделям, версиям программного обеспечения средств, указанным в протоколах испытаний, содержащих результаты оценки соответствия средств (для средств, прошедших оценку соответствия в форме испытаний, приемки);

- несоответствие средств Требованиям к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденным приказом ФСТЭК России от 21.12.2017

№ 235, или Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России от 25.12.2017 № 239.

Требования информационной безопасности

Требования информационной безопасности включаются обязательно во все технические задания, частные технические задания и задания на проектирование объектов нового строительства, расширения, реконструкции, технического перевооружения и модернизации объектов электросетевого комплекса, в части создания, внедрения (модернизации, строительстве и т.д.) любых ИС, АС, ИТКС, АСУ ТП, АСТУ, ИТСО, сетей связи:

«Согласно Федеральному закону от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» провести предварительное категорирование объектов критической информационной инфраструктуры проектируемого объекта. Результаты предварительного категорирования согласовать с Заказчиком.»

1.1 Перечень нормативных и методических документов

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
- Постановление Правительства Российской Федерации 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».
- Методика оценки угроз безопасности информации (утверждена 05.02.2021 ФСТЭК России).
- Приказ ФСТЭК России от 25.12.2017 № 239.
- Приказ ФСТЭК России от 21.12.2017 № 235.
- Приказ ФСТЭК России от 14.03.2014 № 31.
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК России от 18.02.2013 № 21.
- ГОСТ Р 59793-2021 «Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов

на автоматизированные системы. Автоматизированные системы. Стадии создания» (утвержден и введен в действие Приказом Росстандарта от 25.10.2021 № 1285-ст).

– ГОСТ 34.601-90 Информационная технология. Автоматизированные системы. Стадии создания.

– ГОСТ 2.105-95 Общие требования к текстовым документам.

– ГОСТ 34.602-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

– ГОСТ 34.201-2020 Информационная технология. Виды, комплектность и обозначение документов при создании автоматизированных систем.

– ГОСТ 19.101-77. Виды программ и программных документов.

– ГОСТ Р 59792-2021 Виды испытаний автоматизированных систем.

– ГОСТ Р ИСО/МЭК 14764-2002. Информационная технология. Сопровождение программных средств.

– ГОСТ Р 59795-2021 Требования к содержанию документов.

– ГОСТ 28195 89 Оценка качества программных средств. Общие положения.

1.2 Требования к информационной безопасности

1.2.1 Требования к организации процесса проектирования, в части информационной безопасности

В рамках реализации каждого из этапов технического проектирования настоящего Технического задания Исполнитель должен провести предварительное категорирование, а также учесть требования к проектированию создаваемой Системы и ее компонентов для целей последующей защиты согласно действующему законодательству Российской Федерации:

1. в случае выявления критериев отнесения Системы или ее частей к объектам критической информационной инфраструктуры;

2. в случае выявления критериев отнесения Системы или ее частей к информационным системам персональных данных;

3. в случае выявления критериев отнесения Системы или ее частей к информационным системам обработки коммерческую или служебную тайны.

Результаты предварительного категорирования необходимо согласовать с Заказчиком.

1.2.2 Требования по обеспечению информационной безопасности при создании ИС, АСУ, ИТС

Организационные и технические меры по обеспечению информационной безопасности должны обеспечивать:

1. предотвращение неправомерного доступа к обрабатываемой информации, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
2. недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование системы и обеспечивающих (управляемых, контролируемых) им процессов;
3. восстановление функционирования системы, в том числе за счет создания и хранения резервных копий необходимой для этого информации;

Разработка документации на создание подсистемы безопасности Системы должно включать:

1. проектирование подсистемы безопасности Системы;
2. разработку рабочей (эксплуатационной) документации на Систему (в части обеспечения его безопасности).
3. анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);

Проектирование подсистемы безопасности Системы осуществляется с учетом модели угроз безопасности информации, категории значимости Системы, уровня защищенности ПДн:

1. определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;
2. определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);
3. определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности объекта;
4. определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности объекта;
5. осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;
6. разрабатывается архитектура подсистемы безопасности объекта, включающая состав, места установки, взаимосвязи средств защиты информации;
7. определяются требования к параметрам настройки программных

и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей объекта;

8. определяются меры по обеспечению безопасности при взаимодействии объекта с иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями, а также сетями электросвязи.

Результаты проектирования подсистемы безопасности объекта отражаются в проектной документации на объект (подсистему безопасности объекта).

Раздел проектной документации «Требования к обеспечению информационной безопасности» должен содержать:

1. цель и задачи обеспечения безопасности Системы или подсистемы безопасности Системы;
2. категорию значимости Системы, уровень защищенности ПДн;
3. перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать подсистема безопасности Системы;
4. перечень типов объектов защиты Системы;
5. требования к организационным и техническим мерам, применяемым для обеспечения безопасности Системы;
6. стадии (этапы работ) создания подсистемы безопасности Системы;
7. требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
8. требования к защите средств и систем, обеспечивающих функционирование Системы (обеспечивающей инфраструктуре);
9. требования к информационному взаимодействию Системы с иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями, а также сетями электросвязи;
10. требования к составу и содержанию документации, разрабатываемой в ходе создания объекта.

Разработка рабочей (эксплуатационной) документации на Систему осуществляется на основе проектной документации.

Рабочая (эксплуатационная) документация на ПОИБ должна содержать:

1. описание архитектуры подсистемы безопасности Системы;
2. порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;

3. правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

Анализ угроз безопасности информации должен включать:

1. выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
2. анализ возможных уязвимостей Системы и его программных, программно-аппаратных средств;
3. определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
4. оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов Системы, взаимодействия с иными информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, сетями электросвязи, а также особенностями функционирования объекта.

Модель угроз безопасности информации должна содержать:

- описание систем и сетей и их характеристики как объектов защиты,
- класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных, назначение,
- задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим;
- основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети;
- состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;
- описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации));
- описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами

и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;

- информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту информации между обладателем информации, оператором и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии).

К модели угроз безопасности информации должны прилагаться схемы и рисунки, иллюстрирующие состав и архитектуру систем и сетей, интерфейсы взаимодействия компонентов системы и сети, группы пользователей, а также другие поясняющие материалы (или указывать ссылки на проектные документы с данной информацией);

- возможные негативные последствия от реализации (возникновения) угроз безопасности информации;
- возможные объекты воздействия угроз безопасности информации;
- источники угроз безопасности информации;
- способы реализации (возникновения) угроз безопасности информации;
- актуальные угрозы безопасности информации.

Описание каждой угрозы безопасности информации должно включать:

1. источник угрозы безопасности информации;
2. уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;
3. возможные способы (сценарии) реализации угрозы безопасности информации;
4. возможные последствия от реализации (возникновения) угрозы безопасности информации.
5. Сопоставление актуальных угроз с проектируемыми компенсирующими мерами и средствами защиты.

Внедрение организационных и технических мер по обеспечению безопасности Системы организуется субъектом электроэнергетики в соответствии с проектной и рабочей (эксплуатационной) документацией на ПОИБ, стандартами организаций и включает:

1. установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств;
2. разработку организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности Системы;
3. внедрение организационных мер по обеспечению безопасности

Системы;

4. предварительные испытания Системы и его подсистемы безопасности;
5. анализ уязвимостей Системы и принятие мер по их устранению;
6. опытную эксплуатацию Системы и его подсистемы безопасности;
7. приемочные испытания Системы и его подсистемы безопасности.

Предварительные испытания Системы и его подсистемы безопасности должны проводиться в соответствии с программой и методикой испытаний и включать проверку работоспособности подсистемы безопасности Системы и отдельных средств защиты информации, оценку выполнения требований по безопасности, предъявляемых к программным и программно-аппаратным средствам, в том числе средствам защиты информации, оценку влияния подсистемы безопасности на функционирование Системы при проектных режимах его работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации Системы и его подсистемы безопасности.

Анализ уязвимостей Системы проводится средствами комплексной системы информационной безопасности.

Применение способов и средств выявления уязвимостей осуществляется субъектом электроэнергетики с учетом особенностей функционирования Системы.

Допускается проведение анализа уязвимостей на макете (в тестовой зоне) Системы или макетах отдельных сегментов Системы.

По результатам анализа уязвимостей должно быть подтверждено, что в Системе отсутствуют уязвимости, как минимум содержащиеся в банке данных угроз безопасности информации ФСТЭК России или выявленные уязвимости не приводят к возникновению угроз безопасности информации в отношении Системы.

Опытная эксплуатация Системы и его подсистемы безопасности должна проводиться в соответствии с программой и методиками опытной эксплуатации и включать проверку функционирования подсистемы безопасности Системы, в том числе реализованных организационных и технических мер, а также знаний и умений пользователей и администраторов, необходимых для эксплуатации Системы и его подсистемы безопасности. По результатам опытной эксплуатации принимается решение о возможности (или невозможности) проведения приемочных испытаний Системы и его подсистемы безопасности и необходимости переноса Системы в защищенный сегмент.

В ходе приемочных испытаний Системы и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие Системы и его подсистемы безопасности настоящим Требованиям, а также требованиям технического задания на создание Системы и (или) технического

задания (частного технического задания) на создание подсистемы безопасности Системы.

Результаты приемочных испытаний Системы и его подсистемы безопасности с выводом о ее соответствии установленным требованиям включаются в акт приемки Системы в эксплуатацию.

Ввод в эксплуатацию Системы и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии Системы установленным требованиям по обеспечению безопасности.

В составе Руководства администратора безопасности предусмотреть разработку:

1. Описание обеспечения информационной безопасности Системы в ходе его эксплуатации;
2. Описание действий персонала по восстановлению информации и штатного функционирования Системы в случае возникновения нештатных ситуаций в результате которых нарушено и (или) прекращено функционирование объектов информационной инфраструктуры;
3. Описание обеспечения информационной безопасности Системы при выводе его из эксплуатации.

1.2.3 Общие требования

Документы, являющиеся результатом работ, предоставляются Исполнителем Заказчику в двух экземплярах на бумажных носителях и в одном экземпляре на электронном носителе. Документы предоставляются в редактируемых форматах файлов (doc(x), xls(x), odp, ods, odt) на USB-носителе. При выполнении работ в части информационной безопасности руководствоваться Методическими рекомендациями и правилами по выполнению требований в части категорирования объектов критической информационной инфраструктуры и выполнению требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры ПАО «Россети Ленэнерго», утвержденными протоколом комиссии по КИИ № ЛЭ/01-07/333.

В Раздел состав и содержание работ должны быть добавлены работы из приложенной таблицы в каждом этапе создания системы:

Этап работы	Наименование этапа разработки основной системы	Состав и результаты работы
Этап 1	Обследование объектов	1. Обследования объектов защиты: обследование объекта защиты\системы и сбор исходных данных для категорирования и построения ПОИБ.

		- составление отчета
Этап 2	Проектирование	1. Акт установления уровня защищенности системы по требованиям защиты информации (ПДн) по Постановлению Правительства от 01.11.2012 № 1119 2. Проект Акта категорирования объекта критической информационной инфраструктуры. (Постановление Правительства № 127 п.17 а, б, в, з) 3. Проект Сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. 4. Проектная документация на ПОИБ в составе: • определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа; • определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная); • определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта; • определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта; • осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию; • разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации; • определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз

		безопасности информации и устранение уязвимостей значимого объекта; • определяются меры по обеспечению безопасности при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями. 5. Рабочая (эксплуатационная) документация на ПОИБ в составе: • 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). 6. Модель угроз информационной безопасности (в ее составе описание состава системы (сервера, ПО, АРМы, сеть, интеграция с внешними и внутренними системами) <i>Для строительных титулов предоставляется сводно-сметный расчет</i>
Этап 3	Внедрение, Испытания, Опытная эксплуатация и Ввод в промышленную эксплуатацию.	<i>По итогам СМР + ПНР системы, до ввода в опытную эксплуатацию:</i> 1. Актуализация: • Акт установления уровня защищенности системы по требованиям защиты информации (ПДн) по Постановлению правительства от 01.11.2012 № 1119 • Проект Акта категорирования объекта критической информационной инфраструктуры. (Постановление Правительства № 127 п. 17 (а-и)) • Проект Сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. • Рабочей документации на ПОИБ (на основании модели угроз)

	Возможна замена ЧТЗ, в случае изменения категории значимости, класса защиты. 2. Актуализированная модель угроз информационной безопасности (в ее составе описание состава системы (сервера, ПО, АРМы, сеть, интеграция с внешними и внутренними системами) + таблица межсетевого экранирования, резервирование) 3. Описание настроек средств защиты, в части встроенных в систему средств защиты. Заявка на департамент ИБ на настройку наложенных средств защиты – в соответствии с актуализированной рабочей документацией. 4. Программа и методика испытаний ПОИБ (для предварительных испытаний и перевода в опытную эксплуатацию системы, включая сканирование на уязвимости) 5. Акт о завершении предварительных испытаний СИБ и передачи в опытную эксплуатацию 6. Акт о завершении опытной эксплуатации СИБ 7. Акт о приемке СИБ в постоянную эксплуатацию По результатам испытаний, информационная система переезжает в защищенный сегмент (в случае необходимости) 8. Исполнительная документация по ПОИБ, в части встроенных в систему средств защиты: a. Описание комплексов технических средств и программного обеспечения b. Приложение 1. Структурная схема c. Приложение 2. Логическая схема d. Приложение 3. Схема расположения технических средств на планах (при наличии) e. Приложение 4. Схема расположения технических средств в конструктивах (шкафах) (при наличии) f. Приложение 5. Таблица адресации g. Приложение 6. Таблицы описания настроек h. Приложение 7. Политика безопасности МЭ (при наличии)
--	---

		i. Приложение 8. Описание подключаемых источников j. Приложение 9. Таблица соединений и подключений (при наличии) k. Приложение 10. Схема электрическая принципиальная (при наличии) l. Приложение 11. Перечень актуальных угроз и комплексов защиты 9. Руководство администратора безопасности
--	--	---

Дополнительно требование для ПО:

Входящие в состав Системы программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях Субъекта (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации).

Все передаваемое программное обеспечение (ПО) и СУБД не должны иметь общеизвестных уязвимостей, опубликованных в сети «Интернет». Проверка осуществляется на сайте [бдУ - Уязвимости \(fstec.ru\)](http://бдУ - Уязвимости (fstec.ru)) в банке данных угроз безопасности информации ФСТЭК России.

В ПО и СУБД не должно быть функций, позволяющих удаленно подключаться напрямую к ПО или СУБД для обновления или управления со стороны лиц, не являющихся работниками ПАО «Россети», а также работниками его дочерних и зависимых Обществ.

В ПО и СУБД не должно быть функций, позволяющих автоматически передавать информацию, в том числе технологическую информации, Правообладателю (разработчикам) ПО или СУБД, а также иным третьим лицам.

Все передаваемое программное обеспечение (ПО) и СУБД не должно иметь ограничений со стороны Правообладателя (разработчиков) или иных лиц на применение ПО на всей территории Российской Федерации.

Эксплуатационно-техническое обслуживание, техническая поддержка ПО, в том числе СУБД, должна оказываться Правообладателем (разработчиком) или представителем Правообладателя, зарегистрированным на территории Российской Федерации.

Приложение 2
к Методическим рекомендациям

Перечень критичности бизнес-процессов ПАО «Россети Ленэнерго»

(приложение размещено на вкладке «Контент» в СЭД)

Приложение 3
к Методическим рекомендациям

Рекомендуемый образец
Утв. приказом ФСТЭК России
от 22 декабря 2017 г. № 236
(в ред. от 21 марта 2019 г.)

**Сведения о результатах присвоения объекту критической
информационной инфраструктуры одной из категорий значимости
либо об отсутствии необходимости присвоения ему
одной из таких категорий**

Ограничительная пометка
или гриф секретности
(при необходимости)

В Федеральную службу по техническому и экспортному контролю

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	<i>Заполняется в соответствии с наименованием, указанным в проектных и эксплуатационных документах и на основании балансовой ведомости субъекта КИИ.</i>
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	<i>Необходимо указать адреса размещения всех компонентов объекта КИИ, в том числе адреса обособленных подразделений, филиалов, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства))</i>
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона	<i>Указывается одна или несколько из перечня сфер деятельности, в соответствии с пунктом 8 статьи 2</i>

	от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	<i>Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в которой функционирует объект КИИ (Энергетика)</i>
1.4.	Назначение объекта	<i>Назначение объекта КИИ указывается в соответствии с рабочей, проектной, эксплуатационной или иной документацией на объект КИИ, а также в соответствии с локальными нормативно-правовыми актами о создании и (или) вводе объекта КИИ в эксплуатацию</i>
1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	<i>Указывается тип объекта КИИ - ИС, ИТКС или АСУ ТП особое внимание должно уделяться АСУ ТП.</i>
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	<i>Тип архитектуры определяется в соответствии с рабочей, проектной или эксплуатационной документацией на объект КИИ, фактическим составом технических средств и их взаимосвязью. Для примера, архитектура объекта КИИ может быть следующих типов: одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления и др.</i>

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	<i>Указывается полное и краткое наименование субъекта КИИ в соответствии с уставными документами</i>
2.2.	Адрес местонахождения субъекта	<i>Указывается адрес местонахождения субъекта КИИ. Адрес местонахождения определяется в соответствии с уставными документами и ЕГРЮЛ субъекта КИИ</i>

2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	<i>Указывается полное наименование должности руководителя субъекта КИИ в соответствии с уставными документами и его фамилия, имя и отчество (при наличии)</i>
2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта	<i>Если функции обеспечения безопасности значимых объектов КИИ возложены на соответствующее должностное лицо из числа работников субъекта КИИ, указывается должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов КИИ.</i> <i>Если функции обеспечения безопасности значимых объектов КИИ в субъекта КИИ ни на кого из работников не возложены, то указывается полное наименование должности руководителя субъекта КИИ в соответствии с уставными документами и его фамилия, имя и отчество (при наличии).</i>
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	<i>Если ответственность за обеспечение безопасности значимых объектов КИИ возложена на структурное подразделение организации, указывается полное наименование (в соответствии с утвержденной организационно-штатной структурой) структурного подразделения, а также полное наименование (в соответствии с утвержденной организационно-штатной структурой) должности руководителя этого структурного подразделения, его фамилию, имя и отчество (при наличии), номер телефона и адрес электронной почты (при наличии).</i> <i>Если ответственность за обеспечение безопасности значимых объектов КИИ возложена на штатного специалиста, указывается полное наименование (в соответствии с утвержденной организационно-штатной структурой)</i>

		<i>должности этого штатного специалиста, его фамилию, имя и отчество (при наличии), а также его номер телефона и адрес электронной почты (при наличии)</i>
2.6.	ИНН субъекта и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	<i>Указывается ИНН субъекта КИИ и КПП филиалов, представительств, в которых размещаются компоненты объекта КИИ</i>

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	<i>Если рассматриваемый объект КИИ взаимодействует с сетями электросвязи - указывается категория сети электросвязи.</i> <i>В соответствии с Федеральным законом от 07 июля 2003 г. № 126-ФЗ «О связи» сети электросвязи могут делиться на следующие категории:</i> - <i>сеть связи общего пользования;</i> - <i>выделенная сеть связи;</i> - <i>технологическая сеть связи, а также технологическая сеть связи, присоединенная к сети связи общего пользования;</i> - <i>сеть связи специального назначения</i> <i>Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение</i>
3.2.	Наименование оператора связи и (или) провайдера хостинга	<i>Если рассматриваемый объект КИИ взаимодействует с сетями связи, для каждой из них необходимо указать наименование оператора связи (в соответствии с договором об оказании услуг связи), предоставляющего доступ к данной сети электросвязи. Если</i>

		<i>рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение.</i> <i>Примечание - если технологические сети связи - это сети связи предприятия, используемые для обеспечения производственной деятельности, управления технологическими процессами в производстве, для них в качестве оператора указывается наименование субъекта КИИ.</i> <i>В случае, если компоненты объекта КИИ размещаются на площадках провайдеров хостингов, указывается наименование провайдера хостинга.</i> <i>В случае, если для размещения компонентов объекта КИИ не используются сторонние хостинги, дается соответствующее пояснение</i>
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	<i>Если рассматриваемый объект КИИ взаимодействует с сетями электросвязи, необходимо указать цель такого взаимодействия. Цель взаимодействия указывается в соответствии с рабочей, проектной и (или) эксплуатационной документацией на данный объект КИИ. Для примера, могут быть указаны следующие цели взаимодействия: передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), или любая иная цель.</i> <i>Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение</i>

3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	<i>Если рассматриваемый объект КИИ взаимодействует с сетями электросвязи, необходимо указать способ взаимодействия (проводной и (или) беспроводной), используемые технологии доступа к сети электросвязи, а также протоколы, по которым осуществляется взаимодействие. Данный пункт заполняется на основании рабочей, проектной и/или эксплуатационной документации на данный объект КИИ, а также на основании договора об оказании услуг связи.</i> <i>Если рассматриваемый объект КИИ не взаимодействует с вышеперечисленными сетями электросвязи, дается соответствующее пояснение</i>
------	--	---

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	<i>указывается наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект КИИ. Если рассматриваемый объект КИИ эксплуатируется только субъектом КИИ, то указывается наименование полное и краткое наименование организации.</i>
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	<i>указывается адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект КИИ. Если какие-либо компоненты рассматриваемого объекта КИИ эксплуатируются сторонним юридическим лицом, также указывается полное наименование (в соответствии с уставными документами, ЕГРЮЛ) этого юридического лица</i>

4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные устройства), иные элементы (компоненты)	указывается элемент (компонент) объекта, который эксплуатируется указанным юридическим лицом или индивидуальным предпринимателем. Если рассматриваемый объект КИИ эксплуатируется только организацией, указывается адрес местонахождения организации.
4.4.	ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта	указывается ИНН лица, эксплуатирующего объект и КПП его обособленных подразделений (филиалов, представительств), в которых размещаются сегменты распределенного объекта. Если какие-либо компоненты рассматриваемого объекта КИИ эксплуатируются сторонним юридическим лицом, также указывается адрес местонахождения (в соответствии с уставными документами, ЕГРЮЛ) этого юридического лица

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	Указываются наименования всех программно-аппаратных средств в составе объекта КИИ (без разбиения на какие-либо группы и указания мест размещения), с указанием их количества. Заполняются на основании сведений из балансовой ведомости субъекта КИИ
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии))	Указываются наименования и версии клиентских, серверных операционных систем, средств виртуализации (при наличии), входящих в состав рассматриваемого объекта КИИ общим перечнем (без разбиения на какие-либо группы и указания мест размещения) заполняются на основании сведений из балансовой ведомости субъекта КИИ
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ,	Указываются наименования и версии прикладных программ, обеспечивающих выполнение функций объекта КИИ по его назначению, за исключением

	входящих в состав дистрибутивов операционных систем)	<i>прикладных программ, входящих в состав дистрибутивов операционных систем, общим перечнем (без разбиения на какие-либо группы и указания мест размещения) заполняются на основании сведений из балансовой ведомости субъекта КИИ</i>
5.4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	<i>Если на рассматриваемом объекте КИИ применяются средства защиты информации, указываются наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о не проведении такой оценки.</i> <i>Если в качестве средств защиты информации используются встроенные в системное и/или прикладное программное обеспечение средства, указываются функции безопасности программного обеспечения (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции).</i> <i>Если на объекте КИИ не используются средства защиты информации и их функции не реализованы встроенными средствами системного и (или) прикладного программного обеспечения, дается соответствующее пояснение</i>

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности	<i>Заполняется на основании сведений из Моделей угроз и нарушителей безопасности информации объекта КИИ (в случае наличия).</i> <i>Во всех случаях указывается тип нарушителя: внешний или внутренний.</i>
------	--	--

	нарушителем реализовать угрозы безопасности информации	<i>В случае наличия объективных факторов, свидетельствующих о возможности исключения тех или иных положений из описания, по решению Комиссии то описание может быть скорректировано</i>
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	<i>Заполняется на основании сведений из Моделей угроз и нарушителей безопасности информации объекта КИИ (в случае наличия).</i> <i>Указываются группы угроз, актуальных для объекта КИИ исходя из его структурно-функциональных характеристик, используемых типов технических средств и технологий.</i> <i>В соответствии с критериями, установленными в указанном документе, выбираются группы угроз и конкретные угрозы безопасности с их идентификаторами Банка данных угроз безопасности информации ФСТЭК России, которые указываются при заполнении данного поля</i>

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	<i>Заполняется на основании сведений из Моделей угроз и нарушителей безопасности информации объекта КИИ</i>
------	---	---

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из

категорий значимости, а также сведения о результатах оценки показателей критериев значимости

8.1.	Категория значимости, которая присвоена объекту либо информация о не присвоении объекту ни одной из таких категорий	<i>Указывается категория в соответствии с результатами категорирования, отраженными в утвержденном Акте соответствующего объекта КИИ</i>
8.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	<i>Заполняется на основании сведений, полученных при выполнении оценки возможного масштаба последствий.</i> <i>Указывается по всем показателям критериев значимости, определенным в Правилах.</i> <i>По неприменимым показателям критериев значимости - указывается факт неприменимости</i>
8.3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	<i>Заполняется на основании сведений, полученных при выполнении оценки возможного масштаба последствий.</i> <i>Указывается по всем показателям критериев значимости, определенным в Правилах.</i> <i>По неприменимым показателям критериев значимости - указывается текстовое обоснование неприменимости</i>

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	<i>Меры указываются вне зависимости от того, присвоена ли объекту КИИ категория значимости или нет.</i>
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по	<i>Меры указываются вне зависимости от того, присвоена ли объекту КИИ категория значимости или нет.</i> <i>Технические меры рекомендуется группировать в соответствии с приказом ФСТЭК России № 239,</i>

	обеспечению безопасности значимых объектов	<i>описывая, что конкретно технически реализовано в рамках той или иной группы мер.</i>
--	--	---

(наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица)

(подпись)

(инициалы, фамилия)

М. П.
(при наличии печати)

« ____ » _____ 20 ____ г.

Приложение 4
к Методическим рекомендациям

АКТ
категорирования объектов критической информационной
инфраструктуры ПАО «Россети Ленэнерго»
№ ____

На основании _____ комиссия в составе:

Председатель комиссии:

(Должность, ФИО)

Члены комиссии:

(Должность, ФИО)

провела в Исполнительный аппарат категорирование объектов критической информационной инфраструктуры следующих автоматизированных систем:

№	Наименование объекта критической информационной инфраструктуры
1.	Система 1
2.	Система 2
3.	Система 3
4.	
5.	

1. Объект критической информационной инфраструктуры Система 1:

1.1. Сведения об объекте критической информационной инфраструктуры

1.1.1.	Наименование объекта (наименование информационной системы, автоматизированной системы управления или информационно-телекоммуникационной сети)	Заполняется в соответствии с наименованием, указанным в проектных и эксплуатационных документах и на основании балансовой ведомости субъекта КИИ.
--------	---	---

1.1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, (филиалов, представительств) субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта	<i>Необходимо указать адреса размещения всех компонентов объекта КИИ, в том числе адреса обособленных подразделений, филиалов, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства))</i>
1.1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»	<i>Указывается одна или несколько из перечня сфер деятельности, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в которой функционирует объект КИИ (Энергетика)</i>
1.1.4.	Назначение объекта	<i>Назначение объекта КИИ указывается в соответствии с рабочей, проектной, эксплуатационной или иной документацией на объект КИИ, а также в соответствии с локальными нормативно-правовыми актами о создании и (или) вводе объекта КИИ в эксплуатацию Пример: Система информационного моделирования электроэнергетических сетей для расчета установившихся режимов, токов короткого замыкания, потерь электрической энергии, технико-экономических показателей с отображением результатов на однолинейных схемах</i>
1.1.5.	Тип объекта (информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть)	<i>Указывается тип объекта КИИ - ИС, ИТКС или АСУ ТП особое внимание должно уделяться АСУ ТП.</i>
1.1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система	<i>Тип архитектуры определяется в соответствии с рабочей, проектной или эксплуатационной документацией на объект КИИ,</i>

	диспетчерского управления и контроля, распределенная система управления, иная архитектура)	<i>фактическим составом технических средств и их взаимосвязью. Для примера, архитектура объекта КИИ может быть следующих типов: одноранговая сеть, клиент-серверная система, технология «тонкий клиент», сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления и др.</i>
--	--	--

1.2. Сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

1.2.1.	Категория значимости, которая присвоена объекту, либо информация о неприсвоении объекту ни одной из таких категорий	Присваивается\Не присваивается
1.2.2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Социальная значимость: 1. Причинение ущерба жизни и здоровью людей (человек): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 2.а) Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемые на территории, на которой возможно нарушение обеспечения жизнедеятельности населения: <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 2.б) Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, оцениваемые по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек): <u>Применимо\Неприменимо</u>

		<u>Обоснование:</u> 3.а) Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств, оцениваемые на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг: <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 3.б) Прекращение или нарушение функционирования объектов транспортной инфраструктуры, транспортных средств, в том числе высокоавтоматизированных транспортных средств, оцениваемые по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 4. Прекращение или нарушение функционирования сети связи, оцениваемые по количеству абонентов, для которых могут быть недоступны услуги связи (тыс. человек): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 5.а) Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 5.б) Отсутствие доступа к государственной услуге, оцениваемое во времени с момента приема запроса о предоставлении государственной услуги органом, предоставляющим государственную услугу, или подведомственной государственному органу организацией, участвующей в предоставлении государственной услуги в течение которого государственная услуга не может быть оказана (в процентах от времени предоставления услуги,
--	--	--

		предусмотренного административным регламентом): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> Политическая значимость: 6. Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 7. Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации: <u>Применимо\Неприменимо</u> <u>Обоснование:</u> Экономическая значимость: 8. Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, государственной компанией, организацией оборонно-промышленного комплекса, стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов от годового объема доходов, усредненного за прошедший пятилетний период): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 9. Возникновение ущерба бюджету Российской Федерации, оцениваемого в снижении выплат (отчислений) в бюджет, осуществляемых субъектом критической информационной инфраструктуры (процентов
--	--	--

		прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 10. Прекращение или нарушение проведения клиентами операций по осуществлению перевода денежных средств, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, кредитной организацией, выполняющей функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитной организацией, значимой на рынке платежных услуг, оператором услуг платежной инфраструктуры, оказывающим услуги платежной инфраструктуры в рамках системно значимых платежных систем, оцениваемые среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов – на основе прогнозных значений): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 10.1. Прекращение или нарушение проведения операций по исполнению обязательств, осуществляемых субъектом критической информационной инфраструктуры, являющимся центральным контрагентом, среднедневной размер обязательств которого по передаче денежных средств в валюте Российской Федерации по итогам клиринга за последние 12 месяцев (трлн. рублей): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 10.2. Прекращение или нарушение проведения учетно-расчетных операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся центральным депозитарием и регистратором финансовых транзакций, среднедневное количество ценных бумаг (ISIN) российских эмитентов, которые учитывались на счетах в центральном депозитарии (оцениваемые за последние 12 месяцев в тыс. штук): <u>Применимо\Неприменимо</u>
--	--	---

		<u>Обоснование:</u> 10.3. Прекращение или нарушение проведения операций по выплатам, передаче или размещению денежных средств, осуществляемых субъектом критической информационной инфраструктуры, являющимся негосударственным пенсионным фондом, которые оцениваются суммой пенсионных накоплений и пенсионных резервов негосударственного пенсионного фонда (млрд. рублей): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 10.4. Прекращение или нарушение проведения операций по выплатам, перестрахованию, инвестициям, осуществляемых субъектом критической информационной инфраструктуры, являющимся страховой организацией, оцениваемые объемом активов (млрд. рублей): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 10.5. Прекращение или нарушение выполнения функций по переводу денежных средств, осуществляемых субъектом критической информационной инфраструктуры, являющимся оператором услуг информационного обмена (некредитной организацией), который оценивается количеством заключенных договоров с кредитными организациями: <u>Применимо\Неприменимо</u> <u>Обоснование:</u> Экологическая значимость: 11.а) Вредные воздействия на окружающую среду, оцениваемые на территории, на которой окружающая среда может подвергнуться вредным воздействиям: <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 11.б) Вредные воздействия на окружающую среду, оцениваемые по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек): <u>Применимо\Неприменимо</u>
--	--	--

		<u>Обоснование:</u> Значимость для обеспечения обороны страны, безопасности государства и правопорядка: 12. Прекращение или нарушение функционирования (невыполнение установленных показателей) пункта управления (ситуационного центра), оцениваемые в уровне (значимости) пункта управления или ситуационного центра: <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 13.a) Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 13.б) Снижение показателей государственного оборонного заказа, выполняемого (обеспечиваемого) субъектом критической информационной инфраструктуры, оцениваемое в увеличении времени изготовления единицы продукции с заданным объемом (процентов установленного времени на изготовлении единицы продукции): <u>Применимо\Неприменимо</u> <u>Обоснование:</u> 14. Прекращение или нарушение функционирования (невыполнение установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемые в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов): <u>Применимо\Неприменимо</u> <u>Обоснование:</u>
--	--	---

Члены комиссии:

(подпись)

(подпись)

(подпись)

(подпись)

(подпись)

(подпись)

(подпись)

(подпись)

Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры

Для обеспечения дистанционного режима исполнения должностных обязанностей может потребоваться удаленный доступ работников к объектам критической информационной инфраструктуры, что создает дополнительные угрозы безопасности информации, связанные с несанкционированным доступом и воздействием на такие объекты.

В дистанционном режиме не допускается предоставлять удаленный доступ для управления (в том числе путём передачи управляющих команд и (или) сигналов, изменения параметров управляемых процессов и осуществления иных управляющих воздействий) режимами функционирования промышленного (технологического) оборудования (устройств) автоматизированных систем управления производственными (технологическими) процессами, являющихся значимыми объектами критической информационной инфраструктуры.

В целях минимизации рисков возникновения дополнительных угроз безопасности информации в объектах критической информационной инфраструктуры при осуществлении удаленного доступа работников рекомендуется принятие следующих мер:

1. Проведение инструктажа работников субъектов критической информационной инфраструктуры, осуществляющих удаленный доступ к объектам критической информационной инфраструктуры, о правилах безопасного удаленного взаимодействия с такими объектами.

2. Определение перечня средств вычислительной техники, в том числе портативных мобильных средств вычислительной техники (ноутбуков, планшетных компьютеров, мобильных устройств), которые будут предоставлены работникам для удаленной работы (далее – удаленное СБТ). Для удаленного доступа не рекомендуется использование личных средств вычислительной техники, в том числе портативных мобильных средств вычислительной техники.

3. Определение перечня информации и информационных ресурсов (программ, томов, каталогов, файлов), расположенных на серверах объектов критической информационной инфраструктуры, к которым будет предоставляться удаленный доступ.

4. Назначение минимально необходимых прав и привилегий пользователям при удаленной работе.

5. Идентификация удаленных СБТ по физическим адресам (MAC-адресам) на серверах объектов критической информационной

инфраструктуры, к которым будет предоставляться удаленный доступ, предоставление им доступа к информационным ресурсам объектов критической информационной инфраструктуры методом «белого списка».

6. Исключение возможности эксплуатации удаленных СВТ посторонними лицами.

7. Выделение в отдельный домен работников, управление которым должно осуществляться с серверов субъекта критической информационной инфраструктуры, и присвоение каждому удаленному СВТ сетевого (доменного) имени.

8. Обеспечение двухфакторной аутентификации работников удаленных СВТ, при этом один из факторов обеспечивается устройством, отделенным от объекта критической информационной инфраструктуры, к которому осуществляется доступ.

9. Организация защищенного доступа с удаленного СВТ к серверам объектов критической информационной инфраструктуры с применением средств криптографической защиты информации (VPN-клиент).

10. Применение на удаленных СВТ средств антивирусной защиты информации, обеспечение актуальности баз данных признаков вредоносных компьютерных программ (вирусов) на удаленных СВТ путем их ежедневного обновления.

11. Исключение возможности установки работником программного обеспечения на удаленное СВТ, кроме программного обеспечения, установка и эксплуатация которого определена служебной необходимостью, реализуемое штатными средствами операционной системы удаленного СВТ или средствами защиты информации от несанкционированного доступа.

12. Обеспечение мониторинга безопасности объектов критической информационной инфраструктуры, в том числе ведения журналов регистрации действий работников, удаленных СВТ и их анализа.

13. Блокирование сеанса удаленного доступа пользователя при неактивности более установленного субъектом критической информационной инфраструктуры времени.

14. Обеспечение возможности оперативного реагирования и принятия мер защиты информации при возникновении компьютерных инцидентов.

Кроме того, субъектам критической информационной инфраструктуры рекомендуется руководствоваться рекомендациями Национального координационного центра по компьютерным инцидентам и центров мониторинга информационной безопасности, имеющих соответствующие лицензии ФСТЭК России, по вопросам компьютерных атак, в том числе размещенными на веб-ресурсе www.safe-surf.ru.

Приложение 6
к Методическим рекомендациям

Приложение
к Порядку согласования субъектом
критической информационной инфраструктуры
Российской Федерации с Федеральной службой
по техническому и экспортному контролю
подключения значимого объекта критической
информационной инфраструктуры Российской
Федерации к сети связи общего пользования,
утвержденному приказом ФСТЭК России
от 28 мая 2020 г. № 75

Рекомендуемый образец

**Сведения
о значимом объекте критической информационной инфраструктуры
Российской Федерации, в отношении которого планируется
подключение к сети связи общего пользования**

Наименование субъекта критической информационной инфраструктуры

указывается полное и сокращенное (при наличии) наименование

Адрес в пределах места нахождения субъекта критической информационной
инфраструктуры _____

Идентификационный номер налогоплательщика _____

Адрес для переписки _____

1.	Наименование значимого объекта, планируемого к подключению к сети связи общего пользования; регистрационный номер в реестре значимых объектов критической информационной инфраструктуры	
2.	Цель подключения значимого объекта к сети связи общего пользования	
3.	Тип подключения значимого объекта к сети связи общего пользования (проводной, беспроводной); наименование протоколов сетевого взаимодействия, используемых для целей подключения	

4.	Наименование, модель средств обеспечения безопасности значимого объекта, применяемых при его подключении к сети связи общего пользования; версии программного обеспечения средств	
5.	Номера сертификатов соответствия и даты их выдачи (для средств, прошедших оценку соответствия в форме обязательной сертификации)	
6.	Реквизиты протоколов испытаний, содержащих результаты оценки соответствия средств (для средств, прошедших оценку соответствия в форме испытаний, приемки)	

Приложение:

1. Копия модели угроз безопасности информации значимого объекта.
2. Копии протоколов испытаний, содержащих результаты оценки соответствия средств (для средств, прошедших оценку соответствия в форме испытаний, приемки).
3. Схема организации связи (в случае предоставления оператором связи субъекту критической информационной инфраструктуры цифровых каналов связи).

Руководитель субъекта критической
информационной инфраструктуры
(уполномоченное им лицо)

_____ (подпись)

_____ (расшифровка подписи)