

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 Федерального закона 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 "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ.
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О Персональных данных»
- Федеральный закон "О коммерческой тайне" от 29.07.2004 № 98-ФЗ
- Постановление Правительства Российской Федерации от 8 февраля 2018 г. N 127
- «Методика оценки угроз безопасности информации» (утвержден 5 февраля 2021 года ФСТЭК России)
- Приказ ФСТЭК России от 25 декабря 2017 г. N 239
- Приказ ФСТЭК России от 21 декабря 2017 г. N 235
- Приказ ФСТЭК России от 14 марта 2014 г. N 31
- Постановление Правительства Российской Федерации от 01 ноября 2012 г. N 1119
- Приказ ФСТЭК России от 18 февраля 2013 г. N 21
- 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 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 действующего законодательства РФ:

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 2-х экземплярах на бумажных носителях и в 1-м 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 документом «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» утвержденных протоколом комиссии по КИИ от 25.11.201 №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	<p>1. Обследования объектов защиты:</p> <p>обследование объекта защиты\системы и сбор исходных данных для категорирования и построения ПОИБ.</p> <p>- составление отчета</p>
Этап 2	Проектирование	<p>1. Акт установления уровня защищенности системы по требованиям защиты информации (ПДн) по постановлению правительства от 1 ноября 2012 г. N 1119</p> <p>2. Проект Акта категорирования объекта критической информационной инфраструктуры. (Постановление правительства 127 п.17 а,б,в,з)</p> <p>3. Проект Сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.</p> <p>4. Проектная документация на ПОИБ в составе:</p> <ul style="list-style-type: none"> <li>• определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;</li> <li>• определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);</li> <li>• определяются и обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта;</li> <li>• определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;</li> <li>• осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами,</li> </ul>

		<p>выполняемых функций безопасности и ограничений на эксплуатацию;</p> <ul style="list-style-type: none"> <li>• разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;</li> <li>• 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;</li> <li>• определяются меры по обеспечению безопасности при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.</li> </ul> <p>5. Рабочая (эксплуатационная) документация на ПОИБ в составе:</p> <ul style="list-style-type: none"> <li>• описание архитектуры подсистемы безопасности значимого объекта;</li> <li>• порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;</li> <li>• правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).</li> </ul> <p>6. Модель угроз информационной безопасности (в ее составе описание состава системы (сервера, ПО, АРМы, сеть, интеграция с внешними и внутренними системами)</p> <p><i>Для строительных титулов предоставляется сводно-сметный расчет</i></p>
Этап 3	Внедрение, Испытания, Опытная эксплуатация и Ввод в промышленную эксплуатацию.	<p><i>По итогам СМР + ПНР системы, до ввода в опытную эксплуатацию:</i></p> <p>1. Актуализация:</p>



		<ul style="list-style-type: none"> <li>• Акт установления уровня защищенности системы по требованиям защиты информации (ПДн) по постановлению правительства от 1 ноября 2012 г. N 1119</li> <li>• Проект Акта категорирования объекта критической информационной инфраструктуры. (Постановление правительства 127 п.17 (а-и))</li> <li>• Проект Сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.</li> <li>• Рабочей документации на ПОИБ (на основании модели угроз)</li> </ul> <p>Возможна замена ЧТЗ, в случае изменения категории значимости, класса защиты.</p> <p>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)</p> <p>3. Описание настроек средств защиты, в части встроенных в систему средств защиты. Заявка на отдел ИБ на настройку наложенных средств защиты – в соответствии с актуализированной рабочей документацией.</p> <p>4. Программа и методика испытаний ПОИБ (для предварительных испытаний и перевода в опытную эксплуатацию системы, включая сканирование на уязвимости)</p> <p>5. Акт о завершении предварительных испытаний СИБ и передачи в опытную эксплуатацию</p> <p>6. Акт о завершении опытной эксплуатации СИБ</p> <p>7. Акт о приемке СИБ в постоянную эксплуатацию</p> <p>По результатам испытаний, информационная система переезжает в защищенный сегмент (в случае необходимости)</p> <p>8. Исполнительная документация по ПОИБ, в части встроенных в систему средств защиты:</p>
--	--	---

		<ul style="list-style-type: none"> <li>a. Описание комплексов технических средств и программного обеспечения</li> <li>b. Приложение 1. Структурная схема</li> <li>c. Приложение 2. Логическая схема</li> <li>d. Приложение 3. Схема расположения технических средств на планах (при наличии)</li> <li>e. Приложение 4. Схема расположения технических средств в конструктивах (шкафах) (при наличии)</li> <li>f. Приложение 5. Таблица адресации</li> <li>g. Приложение 6. Таблицы описания настроек</li> <li>h. Приложение 7. Политика безопасности МЭ (при наличии)</li> <li>i. Приложение 8. Описание подключаемых источников</li> <li>j. Приложение 9. Таблица соединений и подключений (при наличии)</li> <li>k. Приложение 10. Схема электрическая принципиальная (при наличии)</li> <li>l. Приложение 11. Перечень актуальных угроз и комплексов защиты</li> <li>9. Руководство администратора безопасности</li> </ul>
--	--	---

***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://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.