ООО «СПЕЦИНЖСТРОЙ»

ОГРН 1167847487444, ИНН 7806258664, КПП 770301001, тел.: +7 (499) 113-08-80, e-mail: info@specingstroy.ru 123001, г. Москва, вн.тер.г. муниципальный округ Пресненский, ул. Садовая-Кудринская, д. 25, помещ. 2/4

Заказчик ПАО "Россети Московский регион"

«Строительство ПС 220/20 кВ Мельниково»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 5 Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения

Подраздел 5.5 Сети связи

Информационная безопасность

Шифр: 6350-25-ИОС5.3

Москва 2025 г.

ООО «СПЕЦИНЖСТРОЙ»

ОГРН 1167847487444, ИНН 7806258664, КПП 770301001, тел.: +7 (499) 113-08-80, e-mail: info@specingstroy.ru 123001, г. Москва, вн.тер.г. муниципальный округ Пресненский, ул. Садовая-Кудринская, д. 25, помещ. 2/4

Заказчик ПАО "Россети Московский регион"

«Строительство ПС 220/20 кВ Мельниково»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 5 Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения

Подраздел 5.5 Сети связи

Информационная безопасность

Шифр: 6350-25-ИОС5.3

Том 5.5.3

Генеральный директор: **А.Н. Черняев**

Главный инженер проекта: **С.С. Мельников**

Регистрационный номер НОПРИЗ: **ПИ-161380**

Москва 2025 г.

Согласовано

Взам. инв. №

Подп. и дата

Инв. № подл.

Формат А4

ООО «СП-Инновация» 190020, г. Санкт-Петербург, Бумажная ул., д. 16, корп. 1, лит. А, пом. 33Н, оф. 303А. Тел.: +7 (812) 676-53-24
107140, Москва, Верхняя Красносельская ул., д. 2/1, стр.1.
Тел.: +7 (495) 987-10-27 E-mail: info@sp-innovation.ru

Выписка из реестра СРО: СРО-П-029-25092009

Заказчик: ООО «СПЕЦИНЖСТРОЙ»

«Строительство ПС 220/20 кВ Мельниково»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 5 Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения

Подраздел 5.5 Сети связи

Информационная безопасность

6350-25-ИОС5.3

Том 5.5.3

2025

ООО «СП-Инновация» 190020, г. Санкт-Петербург, Бумажная ул., д. 16, корп. 1, лит. А, пом. 33Н, оф. 303А. Тел.: +7 (812) 676-53-24
107140, Москва, Верхняя Красносельская ул., д. 2/1, стр.1.
Тел.: +7 (495) 987-10-27 E-mail: info@sp-innovation.ru

Выписка из реестра СРО: СРО-П-029-25092009

Заказчик: ООО «СПЕЦИНЖСТРОЙ»

«Строительство ПС 220/20 кВ Мельниково»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Раздел 5 Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения

Подраздел 5.5 Сети связи

Информационная безопасность

6350-25-ИОС5.3

Том 5.5.3

Генеральный директор А.С. Клименко

Главный инженер проекта Р.А. Морев

Регистрационный номер НОПРИЗ: П-159282

2025

Взам. инв.№

Подп. и дата

Инв. № подл.

Общество с ограниченной ответственностью

ИНТЕЛЛЕКТУАЛЬНЫЕ СЕТИ И СИСТЕМЫ

Строительство ПС 220/20 кВ Мельниково

Проектная документация

Раздел 5 Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения

Подраздел 5.5 Сети связи

Информационная безопасность

6350-25-ИОС5.3

Том 5.5.3

Изм.	№ док.	Подп.	Дата

Москва 2025 г.

Общество с ограниченной ответственностью

ИНТЕЛЛЕКТУАЛЬНЫЕ СЕТИ И СИСТЕМЫ

Строительство ПС 220/20 кВ Мельниково

Проектная документация

Раздел 5 Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения

Подраздел 5.5 Сети связи

Информационная безопасность

6350-25-ИОС5.3

Том 5.5.3

Генеральный директор В.Н. Зайцев

Главный инженер проекта Ю.В. Булаев

Москва 2025 г.

Обозначение	Наименование	Примечание
	Текстовая часть:	
6350-25-ИОС5.3-С	Содержание тома	на 1 листе
6350-25-ИОС5.3-СПр	Справка главного инженера проекта	на 1 листе
6350-25-ИОС5.3-СП	Состав проектной документации	на 1 листе
6350-25-ИОС5.3-ПЗ	Пояснительная записка	на 47 листах
6350-25-ИОС5.3-СО	Спецификация оборудования, изделий и материалов	на 4 листах
6350-25-ИОС5.3-ВР.1	Ведомость объёмов монтажных работ	на 1 листе
6350-25-ИОС5.3-ВР.2	Ведомость объёмов пусконаладочных работ	на 1 листе
	Графическая часть:	
6350-25-ИОС5.3-ГЧ.1	Структурная схема системы обеспечения информационной безопасности	на 1 листе
	Прилагаемые документы:	
Приложение 1	Модель нарушителя и модель угроз информационной безопасности	На 45 листах
Приложение 2	Руководящие указания по риск-ориентированному управлению объектами ИТТ активами	на 11 листах
Приложение 3	Программа информирования и обучения персонала объекта информационной инфраструктуры	на 7 листах
Приложение 4	Расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры,	на 5 листах
Приложение 5	План мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций	на 10 листах
Приложение 6	Руководящие указания по конфигурации параметров программных и программно-аппаратных средств	на 10 листах
Приложение 7	Лицензии и сертификаты	на 11 листах
Приложение 8	Задание на проектирование	на 72 листах
	Всего в томе:	**228 листов**

Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№ докум.	Подпись	Дата
Разраб.		Соловьев			08.25
Пров.		Булаев			08.25
Н. Контр.		Николаев			08.25
ГИП		Булаев			08.25

6350-25-ИОС5.3-С

Содержание тома

Стадия	Лист	Листов
П	-	1

ООО «Интеллектуальные сети и системы»

Справка главного инженера проекта

Проектная документация разработана в соответствии с требованиями Федерального закона от 30.12.2009 № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»; постановлением Правительства РФ от 28 мая 2021 г. № 815 «Об утверждении перечня национальных стандартов и сводов правил (частей таких стандартов и сводов правил), в результате применения которых на обязательной основе обеспечивается соблюдение требований Федерального закона «Технический регламент о безопасности зданий и сооружений», и о признании утратившим силу постановления Правительства Российской Федерации от 4 июля 2020 г. № 985» (ред. от 20.05.2022); действующими строительными, технологическими и санитарными нормами и правилами; техническими регламентами, в том числе устанавливающими требования по обеспечению безопасной эксплуатации зданий, строений, сооружений и безопасного использования прилегающих к ним территорий, с соблюдением задания на проектирование и технических условий.

Главный инженер проекта Ю.В. Булаев

Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм.	Кол.уч.	Лист	№ докум.	Подпись	Дата	6350-25-ИОС5.3-СПр		
Разраб.		Соловьев			08.25	Справка главного инженера проекта	Стадия	Лист	Листов
Пров.		Булаев			08.25		П	-	1
							ООО «Интеллектуальные сети и системы»		
Н. Контр.		Николаев			08.25				
ГИП		Булаев			08.25				

Состав проектной документации

Состав проектной документации приведен в 6350-25-СП «Состав проектной документации».

Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№ докум.	Подпись	Дата	6350-25-ИОС5.3-СП		
Разраб.		Соловьев			08.25	Состав проектной документации	Стадия	Лист	Листов
Пров.		Булаев			08.25		П	1	1
							ООО «Интеллектуальные сети и системы»		
Н. Контр.		Николаев			08.25				
ГИП		Булаев			08.25				

Строительство ПС 220/20 кВ Мельниково

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

ПС 220/20 кВ Мельниково

Информационная безопасность

Проектная документация

Пояснительная записка

Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№ докум.	Подпись	Дата	6350-25-ИОС5.3-ПЗ		
Разраб.		Соловьев			08.25	Пояснительная записка	Стадия	Лист	Листов
Пров.		Булаев			08.25		П	1	47
							ООО «Интеллектуальные сети и системы»		
Н. Контр.		Николаев			08.25				
ГИП		Булаев			08.25				

Содержание

1. Общие сведения ... 4
1.1. Наименование объекта защиты ... 4
1.2. Состав объекта защиты ... 4
1.3. Наименование системы ... 4
1.4. Назначение системы обеспечения информационной безопасности ... 4
1.5. Основание разработки ... 4
2. Требования к системе обеспечения информационной безопасности ... 7
2.1. Основные требования к проектируемому объекту ... 7
2.1.1. Состав представляемых на рассмотрение материалов проектирования ... 7
2.1.2. Требования к предоставляемым материалам в части подсистемы Информационной безопасности ... 7
2.2. Требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации ... 8
2.2.1. Общие требования. ... 8
2.2.2. Требования к системному программному обеспечению АРМ, серверов, программируемых контроллеров, терминалов РЗА ... 8
2.2.3. Межсетевой экран ... 11
2.2.4. Коммутатор ... 11
2.2.5. Средства криптографической защиты ... 11
2.3. Требования к защите средств и систем, обеспечивающих функционирование объекта информационной инфраструктуры ... 12
2.3.1. Общие организационные требования ... 12
2.3.2. Организация контролируемой зоны и защита технических средств ... 12
2.3.3. Защита компонентов ... 12
2.3.4. Идентификация и аутентификация ... 13
2.3.5. Управление доступом ... 13
2.3.6. Управление конфигурацией ... 15
2.3.7. Анализ защищенности и аудит безопасности ... 15
2.3.8. Управление обновлениями ПО ... 16
2.3.9. Защита машинных носителей ... 16
2.3.10. Обеспечение доступности ... 17
2.3.11. Обеспечение целостности ... 17
2.3.12. Повышение осведомленности ... 18
2.4. Требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями ... 18
2.4.1. Требования к информационному взаимодействию со смежными системами ... 18
2.4.2. Требования к информационному взаимодействию с системами управления верхнего уровня ... 18
3. Обеспечение информационной безопасности ... 20
3.1. Классификация и категорирование объекта ... 20
3.2. Определение угроз безопасности информации ... 20
3.3. Определение состава и базового набора мер защиты информации ... 20
3.4. Адаптация базового набора мер защиты информации ... 21
3.5. Уточнение и дополнение базового набора мер защиты информации ... 22
3.6. Итоговый набор мер и подсистемы обеспечения информационной безопасности ... 23
4. Описание решений по организационным и техническим мерам обеспечения информационной безопасности ... 30
4.1. Общие сведения по обеспечению информационной безопасности ... 30
4.2. Организационные меры ... 32
4.3. Общие требования к информационной безопасности технологического сегмента ... 33
4.4. Структура системы обеспечения информационной безопасности ... 34
5. Система обеспечения информационной безопасности ... 35
5.1. Подсистема защиты каналов связи и межсетевого экранирования ... 35
5.1.1. Описание ... 35
5.1.2. Реализация ... 36
5.2. Подсистемы идентификации и аутентификации. Подсистема управления доступом. Подсистема регистрации событий безопасности. Подсистема обеспечения целостности ... 37
5.2.1. Идентификация и аутентификация ... 37

5.2.2. Управление доступом ... 37
5.2.3. Регистрация событий безопасности ... 37
5.2.4. Обеспечение целостности ... 37
5.2.5. Реализация ... 37
5.3. Подсистема обнаружения вторжений ... 38
5.3.1. Описание ... 38
5.3.2. Реализация ... 39
5.4. Подсистема резервного копирования и восстановления информации, централизованного обновления ПО ... 39
5.4.1. Описание ... 39
5.4.2. Реализация ... 39
5.5. Централизованное управление и мониторинг ... 40
6. Проверка информационной безопасности системы ... 41
6.1. Проверка конфигурации оборудования ... 41
6.2. Проверка интерфейсов и сетевых настроек ... 41
6.3. Настройка удаленного доступа ... 41
6.4. Проверка сервисов операционной системы ... 41
6.5. Конфигурация сетевого оборудования ... 41
6.6. Конфигурация серверов диспетчерских пунктов ... 41
6.7. Общие мероприятия ... 41
7. Мероприятия по подготовке к вводу в эксплуатацию ... 43
7.1. Подготовка объекта ... 43
7.2. Подготовка помещений ... 43
7.3. Ввод в эксплуатацию ... 43
7.4. Предварительные испытания ... 44
7.5. Опытная эксплуатация ... 44
7.6. Приемочные испытания ... 44
8. Сведения о соответствии применяемого оборудования и программного обеспечения требованиям ФЗ ... 45
9. Перечень принятых сокращений ... 46

1. Общие сведения

1.1. Наименование объекта защиты

Объект защиты — автоматизированные системы (далее — АС) ПС 220/20 кВ Мельниково (далее — ПС).

Цель проведения работ — разработка системы обеспечения информационной безопасности (далее — СОИБ) АС ПС.

Заказчик — публичное акционерное общество «Россети Московский Регион» (далее — Общество).

1.2. Состав объекта защиты

В рамках настоящего проекта в качестве состава объекта защиты рассматривается компоненты АС, обрабатывающие данные, циркулирующие между ПС и ЦУС.

1.3. Наименование системы

Полное наименование: Система обеспечения информационной безопасности автоматизированных систем управления и комплексов телемеханики ПС 220/20 кВ Мельниково.

Краткое наименование: СОИБ.

1.4. Назначение системы обеспечения информационной безопасности

Защита информации реализуется путем применения совокупности организационных и технических мер, направленных на нейтрализацию угроз безопасности информации (далее — УБИ), реализация которых может привести к нарушению штатного режима функционирования энергообъектов и реализуемых ими процессов.

СОИБ предназначена для обеспечения защиты информации, не являющейся государственной тайной, обрабатываемой в соответствии с действующим законодательством Российской Федерации, руководящими и нормативными документами по защите информации.

Организационные и технические меры защиты информации, реализуемые в рамках создания СОИБ, должны быть направлены на исключение:

- неправомерного доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);
- неправомерного уничтожения или модификации информации (обеспечения целостности информации);
- неправомерной блокировки информации (обеспечения доступности информации).

В частности, СОИБ должна обеспечивать:

- снижение рисков отказа или внештатного функционирования подсистем и компонентов объекта защиты;
- предупреждение и выявление инцидентов информационной безопасности (далее — ИБ), связанных с использованием уязвимостей базовых элементов объекта защиты;
- нейтрализации актуальных УБИ объекта защиты;
- соответствие требованиям законодательства Российской Федерации в части обеспечения ИБ.

СОИБ реализуется с учетом поддержания объекта защиты в штатном режиме, при котором обеспечивается выполнение целевых функций в условиях воздействия УБИ, а также на снижение рисков незаконного вмешательства в процессы функционирования объекта защиты.

Состав СОИБ

1.5. Основание разработки

Основанием для разработки проектной документации по титулу «Строительство ПС 220/20 кВ Мельниково» являются следующие документы:

- Инвестиционная программа ПАО «Россети Московский регион», утвержденная приказом МЭ РФ от 22.12.2023г. №31а «Об утверждении изменений, вносимых в инвестиционную программу ПАО «Россети

Московский регион» на 2023 — 2027 годы, утвержденную приказом Минэнерго России от 24.11.2022г. №30а», а также текущий проект ее корректировки.;

- Задание на проектирование ПАО «Россети Московский регион» №153-13/ГД/02/ВН-1454 от 19.08.2024г.;
- Технические условия на технологическое присоединение к электрическим сетям ПАО «Россети Московский регион» энергопринимающих устройств ОАО «РЖД» № И-24-00-223309/125 к договору о технологическом присоединении от 15.06.2023г. № ИА-23-302-15007 (624621).

Настоящий проект выполнен в соответствии с требованиями нормативных, отраслевых и руководящих документов по обеспечению ИБ.

Источниками разработки настоящего тома стали следующие документы.

1 Федеральное законодательство:

- Федеральный закон Российской Федерации от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон от 21.07.2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

2 Указы президента РФ:

- Указ Президента РФ от 22.05.2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации»;
- Указ Президента РФ от 06.031997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

3 Постановления правительства:

- Постановление Правительства Российской Федерации от 08.02.2018 г № 127-ПП «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».

4 Приказы регуляторов.

4.1 ФСТЭК:

- Приказ ФСТЭК России от 02.06.2020 г. №76 «Об утверждении Требований по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»;
- Приказ ФСТЭК России от 14.03.2014 г. № 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»;
- Приказ ФСТЭК России от 21.12.2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

4.2 ФСБ:

- Приказ ФСБ РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

4.3 Министерство энергетики:

- Приказ Министерства энергетики РФ от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования».

5 Государственные стандарты:

- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
- ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».
- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».
- ГОСТ 53113.1-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».
- ГОСТ 53113.2-2008 «Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов».

6 Методические документы:

- Методика оценки угроз безопасности информации (утв. ФСТЭК 05.02.2021 г.);
- Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 02 июня 2020 г. № 76.

7 Информационные сообщения:

- Информационное сообщение ФСТЭК России от 29 марта 2019 г. № 240/24/1525 О требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

8 Распоряжения ПАО «Россети»:

- Распоряжение ПАО «Россети» от 01.04.2016 № 140 «Об утверждении минимальных требований к информационной безопасности АСТУ» (в редакции распоряжения ПАО «Россети» от 27.04.2016 № 178р и распоряжения ПАО «Россети» от 08.02.2019 г. № 70р).

9 Внутренняя документация:

- Задание на проектирование по титулу: «Строительство ПС 220/20 кВ Мельниково» (далее – ЗнП).

2. Требования к системе обеспечения информационной безопасности

2.1. Основные требования к проектируемому объекту

2.1.1. Состав представляемых на рассмотрение материалов проектирования

В рамках разработки проектной документации (далее — ПД) согласно ЗнП должны быть проведены следующие мероприятия:

- анализ УБИ и разработка модели УБИ или ее уточнение (при ее наличии);
- определение категории значимости объекта информационной инфраструктуры;
- предоставление решений по организационным и техническим мерам обеспечения ИБ объектов информационной инфраструктуры;
- определение требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
- требования к защите средств и систем, обеспечивающих функционирование объекта информационной инфраструктуры (обеспечивающей инфраструктуре);
- требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

Указанные требования реализуются в рамках настоящего тома, Модель УБИ представлена в Приложении 2 к настоящему тому.

Модель УБИ может быть уточнена на стадии РД, в случае появления новых сведений о проектируемой системе и внесения изменений в текущий и/или смежные тома.

2.1.2. Требования к предоставляемым материалам в части подсистемы Информационной безопасности

В рамках ПД согласно ЗнП должны быть разработаны следующие документы:

- руководящие указания по установке и настройке средств защиты информации, настройке программных и программно-аппаратных средств безопасности объектов информационной инфраструктуры;
- руководящие указания по риск-ориентированному управлению объектами информационной инфраструктуры (ИТТ активами), организации в рамках процесса эксплуатации установки критических обновлений программного обеспечения для объектов;
- руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры, в том числе по обеспечению безопасного удаленного мониторинга объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сеть субъекта электроэнергетики;
- программа информирования и обучения персонала объекта информационной инфраструктуры;
- расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности, управление средствами защиты информации, управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта, мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности, сопровождением функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документах по безопасности значимого объекта;
- план мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций;

- акт категорирования объекта критической информационной инфраструктуры (разрабатывается по итогам согласования окончательного состава объекта защиты на стадии РД).

Настоящие требования реализуются в рамках приложений к настоящему тому.

2.2. Требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации

2.2.1. Общие требования.

В качестве средств защиты информации в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение (далее — ПО) и (или) программно-аппаратные средства значимых объектов критической информационной инфраструктуры (при их наличии).

Средства защиты информации (в том числе встроенные) должны применяться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на средства защиты информации.

Применяемые средства защиты информации (в том числе встроенные) должны быть обеспечены гарантийной, технической поддержкой со стороны разработчиков (производителей).

При выборе средств защиты информации (в том числе встроенных) должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на любом из принадлежащих субъекту критической информационной инфраструктуры значимых объектов критической информационной инфраструктуры.

2.2.2. Требования к системному программному обеспечению АРМ, серверов, программируемых контроллеров, терминалов РЗА.

2.2.2.1. Функции идентификации и аутентификации

Операционная система компонент (АРМ, серверов, программируемых контроллеров, терминалов РЗА) должна реализовывать функцию идентификации и аутентификации пользователей.

Функциональные возможности безопасности ОС должны требовать, чтобы каждый уполномоченный субъект доступа (пользователь, администратор) был успешно идентифицирован и аутентифицирован.

ОС компонент объекта защиты также должна:

- иметь возможность идентификации субъекта доступа путем предъявления физического устройства идентификации;
- предоставлять администратору возможность управлять идентификаторами (создавать, изменять, удалять, блокировать);
- предоставлять администратору возможность управлять средствами идентификации.

2.2.2.2. Функции управления доступом

Используемые ОС должны реализовывать возможность:

- администратору управлять учетными записями;
- задания политики ролевого управления доступом для установленного множества операций, выполняемых субъектами доступа по отношению к объектам доступа;

Используемые ОС должны поддерживать следующие роли пользователей ОС:

- администратор;
- пользователь.

ОС должны блокировать учетную запись пользователя ОС при превышении установленного администратором числа неуспешных попыток аутентификации, а также предоставлять администратору возможность устанавливать пороговое значение количества неуспешных попыток аутентификации.

Функциональные возможности безопасности ОС должны запрещать любые действия до идентификации и аутентифицикации.

ОС должны блокировать сеанс после превышения установленного интервала времени бездействия пользователя ОС с осуществлением следующих действий:

- очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;
- блокирование любых действий по доступу к данным пользователя (устройствам) отображения, кроме необходимых для разблокирования сеанса;
- ОС должна требовать, чтобы до разблокирования сеанса произошла повторная аутентификация пользователя.

ОС должны предоставлять возможность для администратора управлять параметрами и атрибутами безопасности, управлять выполнением функций безопасности ОС.

ОС должны предоставлять возможность отдельно осуществлять ограничение максимального числа одновременных (параллельных) интерактивных сеансов, предоставляемых уполномоченным привилегированным субъектам доступа и уполномоченным непривилегированным субъектам доступа.

2.2.2.3. Функции регистрация событий безопасности

ОС должны обеспечивать генерирование надежных меток времени.

ОС должны генерировать записи аудита для следующих событий:

- запуск и завершение выполнения функций аудита;
- создание новых учетных записей и изменение прав доступа учетных записей;
- неуспешные операции (ошибки аутентификации, недостаточные права доступа при выполнении операций, недоступность интерфейсов ОС);
- срабатывание функций безопасности, направленных на противодействие компьютерным атакам (автоматическое блокирование учетных записей, автоматическое завершение сессий, поступление некорректных исходных данных на внешние интерфейсы ОС).
- превышение количества неудачных попыток аутентификации;
- выгрузка (чтение) журнала безопасности;
- превышение времени действия пароля;
- изменение параметра «время блокировки при достижении максимального числа попыток неудачной аутентификации»;
- изменение параметра «максимальное число попыток аутентификации»;
- изменение параметра «требование использования сложных паролей, содержащих символы в двух регистрах и цифры»;
- изменение параметра «минимальная длина пароля»;
- изменение параметра «срок действия пароля»;
- попытка изменения параметров безопасности;

ОС терминалов РЗА (при наличии), помимо событий, указанных выше, должна генерировать записи аудита для следующих событий:

- начало работы ПО;
- дата и время последней активности ПО;
- выгрузка «белого списка» адресов IP/MAC;
- добавление/удаление/модификация учетной записи пользователя;
- изменение текущей даты/времени;
- изменение настроек синхронизации времени;
- изменение часового пояса АСУТП;
- открытие/завершение сессии связи;
- изменение настроек порта RS-485;

- изменение настроек порта Ethernet;
- доступ к функциям тестирования;
- запуск аппаратного тестирования;
- переход в режим тестирования светодиодов;
- удаление записей регистратора событий;
- удаление осциллограммы;
- удаление всех осциллограмм;
- ручной пуск осциллографа;
- выгрузка/загрузка файлов функций РЗА;
- применение конфигурации/логики терминала;
- обновление ПО;
- команда ДУ (дистанционного управления);
- команда ФК (функциональной кнопки лицевой панели);
- установка/сброс контрольного выхода;
- выполнение команды ИЧМ;
- активация/создание/удаление/редактирование групп уставок;
- включение/выключение возможности изменения уставок через Ethernet;
- включение/выключение сервисного режима;
- настройки – разрешения – Упр.ФК/КА;
- сброс статистики.

В ОС должна быть реализована защита хранимых записей регистрации событий безопасности ОС (аудита) от несанкционированного удаления и предотвращения модификации записей аудита.

ОС должна предоставлять администратору возможность:

- включения и исключения событий в совокупность событий, подвергающихся аудиту;
- просмотра всей информации аудита в понятном для него виде;
- возможность выборочного просмотра данных регистрации (аудита) событий безопасности ОС (поиск, сортировка, упорядочение данных аудита).

ОС должна выполнять выбранные администратором действия, направленные на сохранение данных журнала регистрации событий безопасности ОС и обеспечивающие непрерывность процесса аудита, если журнал регистрации событий безопасности ОС превысит определенный администратором размер.

ОС должна иметь возможность полнотекстовой регистрации привилегированных команд (команд, управляющих системными функциями).

ОС компонент объекта защиты должна иметь возможность передавать данные аудита для внешнего хранения.

2.2.2.4. Функции контроля целостности и ограничения программной среды

ОС должна предоставлять возможность:

- контроля целостности компонентов ПО, разрешенного для запуска, и реагирование на попытки запуска компонентов ПО, целостность которых была нарушена;
- возможность установки ПО (компонентов ПО) только администраторами;
- автоматического запуска прикладного ПО при старте, а также возможность исключения непосредственного взаимодействия пользователей прикладного ПО с ОС.
- контроль запуска компонентов ПО и реагирование на попытки запуска компонентов ПО, произведенные в нарушение установленных правил запуска компонентов ПО.

2.2.2.5. Функции обеспечения доступности

Функциональные возможности ОС должны обеспечивать восстановление объектов ОС из резервных копий, созданных с использованием ОС.

2.2.3. Межсетевой экран

Межсетевой экран (далее – МЭ) должен осуществлять контроль и фильтрацию проходящих через него пакетов в соответствии с заданными правилами.

МЭ может иметь программное или программно-техническое исполнение и должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (IEC, Modbus).

МЭ должен реализовывать следующие функции:

- контроль и фильтрация в соответствии с заданными правилами проходящих через межсетевой экран информационных потоков;
- идентификация и аутентификация субъектов доступа;
- регистрация и учет событий безопасности, подлежащих регистрации и учету, а также оповещение о критичных видах событий безопасности;
- обеспечение сохранения штатного режима функционирования и (или) корректное восстановление штатного режима функционирования МЭ при сбоях и ошибках (в том числе в условиях кратковременных перебоев электропитания, компьютерных атак, направленных на отказ в обслуживании);
- осуществление тестирования межсетевого экрана, а также проверка целостности ПО и конфигурации (параметров) МЭ;
- осуществление управления настройками МЭ в соответствии с заданными ролями администраторов;
- Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы;
- Защита от угроз отказа в обслуживании (DOS, DDOS-атак).

2.2.4. Коммутатор

Коммутатор должен позволять сегментировать сеть на логические сегменты — уровни/шины, определяемые по функциональному назначению с целью построения многоуровневой (эшелонированной) системы защиты.

Коммутатор должен поддерживать механизмы QoS (IEEE 802.1p) и VLAN (IEEE 802.1Q).

Коммутатор должен позволять осуществлять контроль подключения устройств по MAC-адресам.

Коммутатор должен поддерживать защищенный протокол передачи данных SSH.

Коммутатор должен обеспечивать выполнение следующих функций:

- непрерывность связи между устройствами ЛВС для возможности передачи трафика иному сетевому сегменту;
- построение единственного маршрута передачи данных по ЛВС без петель коммутации, приводящих к широковещательным штормам на данном участке ЛВС;
- установку приоритетов в доступе к ресурсам сети определенным видам трафика.

Коммутатор должен обеспечивать надежную передачу данных между источником и приемником с заданными параметрами (время доставки, приоритезация и др.).

Коммутатор должен поддерживать протокол синхронизации времени PTP (поддержка режимов master, slave, transparent clock) для станционной шины — программно, для шины процесса — аппаратно.

2.2.5. Средства криптографической защиты

Средство криптографической защиты (далее – СКЗИ) должно защищать информацию при ее передаче по каналам связи.

СКЗИ должно иметь действующий сертификат ФСБ, подтверждающий соответствие требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 1) и класса КС2 (для исполнения 2) и возможность использования для криптографической защиты (шифрование IP-трафика) информации, не содержащей сведений, составляющих государственную тайну.

2.3. Требования к защите средств и систем, обеспечивающих функционирование объекта информационной инфраструктуры

2.3.1. Общие организационные требования

Принимаемые меры по обеспечению безопасности не должны оказывать отрицательного влияния на функционирование объекта защиты, обмен технологической информацией, функций дистанционного управления из удаленных центров управления и из диспетчерских центров.

В целях реализации требований информационной безопасности за каждым из объектов должно быть назначено ответственное лицо за обеспечение информационной безопасности объекта (далее «ответственный за ИБ») из числа работников, в чьи функциональные обязанности входят вопросы обеспечения информационной безопасности.

Ответственный за ИБ должен осуществлять следующие функции:

- проводить анализ угроз безопасности информации в отношении объекта и выявлять уязвимости в них;
- обеспечивать реализацию требований по обеспечению безопасности объекта;
- осуществлять реагирование на компьютерные инциденты;
- готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности объекта.

Подразделения, эксплуатирующие РАС, должны обеспечивать безопасность эксплуатируемых ими объектов в соответствии с установленными в организационно-распорядительных документах Общества требованиями по безопасности объектов.

2.3.2. Организация контролируемой зоны и защита технических средств

Должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются компоненты объекта защиты и СрЗИ.

Должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования объекта защиты, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования объекта защиты и в помещения и сооружения, в которых они установлены.

Контроль и управление физическим доступом должны предусматривать:

- определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования объекта защиты, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

Должна осуществляться защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

2.3.3. Защита компонентов

Должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

Защита информации должна обеспечиваться путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации.

Должны обеспечиваться доверенные маршруты передачи данных между администратором (пользователем) и

средствами защиты информации (функциями безопасности средств защиты информации). Доверенный канал между пользователем и средствами защиты информации должен обеспечиваться при удаленном и локальном доступе в систему.

Должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

Должно осуществляться разбиение системы на сегменты (сегментирование системы). Сегментирование системы (при наличии технической возможности) должно проводиться с целью построения многоуровневой (эшелонированной) системы защиты.

Должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании системы.

Должна осуществляться защита периметра (физических и (или) логических границ) системы при ее взаимодействии с иными системами и сетями, предусматривающая управление (контроль) входящими в систему и исходящими из системы информационными потоками на физической и (или) логической границе объектов.

Должна быть исключена возможность использования внешних устройств беспроводной связи на серверах и АРМ.

Подключение внешних устройств хранения данных по умолчанию должно быть запрещено, подключение должно быть вызвано потребностью технологического бизнес-процесса и только на ограниченное время.

Должны быть включены пароли на доступ к встроенному ПО (BIOS, UEFI, сервисы управления) компонент.

Неиспользуемый функционал и интерфейсы связи должны быть отключены.

2.3.4. Идентификация и аутентификация

Должна обеспечиваться однозначная аутентификация пользователей на основе механизма пароля, а также соответствующего характеристикам, установленным локально-нормативными документами Общества.

На ПС до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться однозначная идентификация и аутентификация устройств (технических средств). Идентификация устройств обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства.

Должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств:

- определение должностного лица (администратора), ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;
- присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного периода времени;
- блокирование идентификатора пользователя после установленного времени неиспользования.

Хранение парольной информации на серверах и АРМ в открытом виде запрещено. Должен производиться контроль за хранением и передачей парольной информации. В случае выявления инцидентов или компрометации парольной информации должны быть инициированы проверки целостности скомпрометированных узлов и незамедлительная замена парольной информации для всех учетных записей, а также ревизия учетных записей.

2.3.5. Управление доступом

Должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; временная и (или) иные типы записей);
- объединение учетных записей в группы (при необходимости);

- верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой Обществом;
- порядок заведения и контроля использования временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в системе;
- предоставление пользователям прав доступа к объектам доступа системы, основываясь на задачах, решаемых пользователями в системе и взаимодействующими с ней системами.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования системы.

Использование гостевых (анонимных) учетных записей пользователей должно быть запрещено.

Должны быть реализованы установленные методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

Правила разграничения доступа должны быть реализованы на основе установленных и задокументированных списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, параметрам настройки средств защиты информации.

Должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование системы, в соответствии с их должностными обязанностями (функциями), документирование в организационно-распорядительных документах по защите информации полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

Должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) оператора и полномочиями (ролью) по администрированию системы.

Должно быть обеспечено назначение прав и привилегий пользователям и администраторам, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

Должно быть установлено ограничение количества неуспешных попыток входа в систему (доступа к системе) за установленный период времени, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в систему за установленный период времени.

Должно обеспечиваться ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя.

Защита удаленного доступа должна обеспечиваться при всех видах доступа и должна включать:

- установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа;
- ограничение на использование удаленного доступа в соответствии с задачами (функциями) системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с политикой доступа;
- предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа систем.

2.3.6. Управление конфигурацией

Должны быть реализованы следующие функции по управлению установкой (инсталляцией) ПО:

- определение ПО (состава и конфигурации), подлежащих установке в системе после загрузки ОС;
- контроль за установкой ПО (состав компонентов, параметры установки, конфигурация);
- определение и применение параметров настройки ПО, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей системы, приводящих к возникновению угроз безопасности информации.

Должна быть обеспечена установка (инсталляция) только разрешенного к использованию в системе ПО.

Установка (инсталляция) в системе ПО должна осуществляться только администратором.

Должен обеспечиваться периодический контроль установленного (инсталлированного) в системе ПО на предмет соответствия его перечню ПО, разрешенному к установке.

Должен проводиться контроль работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации.

При контроле работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации осуществляется:

- контроль работоспособности (неотключения) ПО и СрЗИ;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) ПО и СрЗИ;
- контроль соответствия настроек ПО и СрЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации;
- восстановление работоспособности (правильности функционирования) и параметров настройки ПО и СрЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

Должен проводиться контроль состава технических средств, ПО и СрЗИ.

При контроле состава технических средств, ПО и СрЗИ осуществляется:

- контроль соответствия состава технических средств, ПО и СрЗИ приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ТМ и РЗА, и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава ТМ и РЗА несанкционированно установленных (удаленных) технических средств, ПО и СрЗИ.

2.3.7. Анализ защищенности и аудит безопасности

Должны осуществляться выявление (поиск), анализ и устранение уязвимостей.

При выявлении (поиске), анализе и устранении уязвимостей должны проводиться:

- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;
- устранение выявленных уязвимостей, в том числе путем установки обновлений ПО СрЗИ, общесистемного ПО, прикладного ПО или микро-ПО технических средств;
- информирование должностных лиц Общества (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В качестве источников информации об уязвимостях должны использоваться опубликованные данные

разработчиков средств защиты информации, общесистемного, прикладного ПО, технических средств, а также другие базы данных уязвимостей.

Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации ТМ и РЗА. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной Обществом.

Должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения информации о событиях безопасности.

Должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации, и с установленной периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности ТМ и РЗА.

В системе должна обеспечиваться защита информации о событиях безопасности. Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

2.3.8. Управление обновлениями ПО

Должен осуществляться контроль установки обновлений ПО, включая ПО средств защиты информации (далее — СрЗИ).

При контроле установки обновлений должны осуществляться проверки соответствия версий общесистемного, прикладного и специального ПО, включая По СрЗИ, установленного и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

Контроль установки обновлений должен проводиться с периодичностью, установленной регламентными документами Общества и фиксироваться в соответствующих журналах.

2.3.9. Защита машинных носителей

Должен быть обеспечен учет машинных носителей информации, используемых в ТМ и РЗА для хранения и обработки информации. Учету подлежат: съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства); портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки); машинные носители информации, встроенные в корпус компонент ТМ и РЗА.

Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации и иные номера.

Должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым на ПС:

- определение должностных лиц, имеющих физический доступ к машинным носителям информации;
- предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функции).

Должен осуществляться контроль использования интерфейсов ввода (вывода), предусматривающий:

- определение интерфейсов компонент ТМ и РЗА, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в системе;
- определение категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода);
- принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода);
- контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут

применяться:

- опечатывание интерфейсов ввода (вывода);
- использование механических запирающих устройств;
- удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);
- применение средств защиты информации.

В ТМ и РЗА должен обеспечиваться контроль подключения машинных носителей информации, предусматривающий:

- определение типов носителей информации, подключение которых к системе разрешено;
- определение категорий пользователей, которым предоставлены полномочия по подключению носителей к системе;
- запрет подключения носителей информации, подключение которых к системе не разрешено.

Должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления информации защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

2.3.10. Обеспечение доступности

Должно обеспечиваться резервирование конфигураций и баз данных компонент ТМ и РЗА.

Объект защиты должен иметь актуальную и доступную проектную и эксплуатационную документацию.

Должна быть предусмотрена возможность восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций.

Для обеспечения возможности восстановления ПО должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.

Возможность восстановления ПО, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

- восстановление ПО, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) ПО;
- восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации;
- возврат системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей системы, позволяющих решать задачи по обработке информации.

Должно обеспечиваться резервирование каналов передачи информации.

2.3.11. Обеспечение целостности

Должен осуществляться контроль целостности ПО, включая программное обеспечение средств защиты информации.

Контроль целостности ПО, включая ПО СрЗИ, должен предусматривать:

- контроль целостности ПО СрЗИ, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы системы
- контроль применения средств разработки и отладки программ в составе ПО системы.

Должны быть реализованы следующие функции по управлению запуском компонентов ПО:

- определение перечня (списка) ПО, запускаемых автоматически при загрузке ОС система компонент (АРМ, серверов, программируемых контроллеров, терминалов РЗА);

- разрешение запуска компонентов ПО, включенных в перечень (список) ПО, запускаемого автоматически при загрузке ОС.

2.3.12. Повышение осведомленности

До работников должны быть доведены положения организационно-распорядительных документов по безопасности объектов в части, их касающейся.

Не реже одного раза в год должны проводиться организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности объектов и о возможных угрозах безопасности информации.

Администраторы ИБ должны пройти обучение способам администрирования ПО. В составе программы обучения должны входить мероприятия по получению знаний и навыков реализации требований информационной безопасности, действующих в Российской Федерации.

Представители организаций, привлекаемых Обществом для эксплуатации, обеспечения функционирования объектов и (или) для обеспечения их безопасности, должны быть ознакомлены с организационно-распорядительными документами по безопасности объектов.

2.4. Требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями

2.4.1. Требования к информационному взаимодействию со смежными системами

Информационный обмен с устройствами смежных информационно-технологических систем и АСУ ТП должен осуществляться в цифровом виде с использованием протоколов передачи данных: МЭК 60870-5-103; МЭК 60870-5-101; МЭК 61850; МЭК 60870-5-104; SPA-Bus.

Устройства смежных систем должны подключаться к станционной шине ПТК ПС по резервированным каналам передачи данных Ethernet. В качестве основного протокола интеграции должен применяться МЭК 61850-8-1 (MMS).

Применение интерфейсов, отличных от Ethernet, и дополнительных устройств (шлюзов) для интеграции смежных систем нежелательно и требует отдельного обоснования.

Смежные подсистемы, не входящие в зону обслуживания АСУ, имеющие в составе сегменты ЛВС с возможностью подключения в них внешнего оборудования, должны подключаться к ПТК с помощью сетевых экранов (маршрутизаторов), предотвращающих проникновение в ЛВС ПТК АСУ ТП со стороны этих подсистем, сетевые экраны не резервируются.

2.4.2. Требования к информационному взаимодействию с системами управления верхнего уровня

Информационный обмен с системами управления верхнего уровня (ДЦ Московского РДУ, ДП ЦУС) должен осуществляться с использованием стандартного протокола МЭК-60870-5-104.

Должна осуществляться защита периметра (физических и (или) логических границ) системы при ее взаимодействии с иными системами и сетями, предусматривающая:

- управление (контроль) входящими в систему и исходящими из системы информационными потоками на физической и (или) логической границе объектов;
- обеспечение взаимодействия системы и (или) ее сегментов с иными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

Должно осуществляться управление информационными потоками при передаче информации между сегментами, включая:

- фильтрацию информационных потоков в соответствии с правилами управления потоками;
- разрешение передачи информации в системе только по установленному маршруту;

– изменение (перенаправление) маршрута передачи информации только в установленных в случаях.

Управление информационными потоками должно обеспечивать разрешенный (установленный) маршрут прохождения информации между устройствами, сегментами в рамках системы, а также между системами на основе правил управления информационными потоками, включающих контроль конфигурации системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

Управление информационными потоками должно блокировать передачу защищаемой информации по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из системы и (или) входящие в систему.

Для организации защищённого доступа к ЛВС АСУ ТП необходимо использовать технологию виртуальных частных сетей Virtual Private Network (VPN).

Управление взаимодействием с внешними информационными системами должно включать:

– предоставление доступа к ТМ и РЗА только авторизованным (уполномоченным) пользователям в соответствии с политикой управления доступом;
– определение типов прикладного ПО системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних систем;
– определение системных учетных записей, используемых в рамках данного взаимодействия;
– определение порядка предоставления доступа к ТМ и РЗА авторизованными (уполномоченным) пользователями из внешних систем.

Каждый объект должен быть изолирован от других автоматизированных систем на уровне сетевого взаимодействия. Взаимодействие должно быть обеспечено методами, исключающими возможность его использования в деструктивных целях для обоих автоматизированных систем.

Сбор информации о событиях информационной безопасности в централизованную систему сбора информации о событиях информационной безопасности должен осуществляться самостоятельной инициацией соединения (по примеру протокола Syslog). Методы в виде опроса сервисов, баз данных систем должны быть исключены (при наличии технической возможности без нанесения ущерба технологическому процессу).

Прямой сетевой доступ к базам данных должен быть исключен (при наличии технической возможности без нанесения ущерба технологическому процессу).

3. Обеспечение информационной безопасности

3.1. Классификация и категорирование объекта

В настоящее время объекту категория значимости не присвоена, класс защищенности не определен.

Необходима реализация мер защиты информации в соответствии с ФЗ № 187 и его подзаконными актами, а также в соответствии с Требованиями, установленными Приказом ФСТЭК № 31 в отношении автоматизированных систем не ниже 3 класса защищенности.

В случае, если проектируемый объект не признан ЗОКИИ, и ему не присвоена одна из категорий значимости, согласно Постановления Правительства от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования...», то меры по обеспечению защиты информации формируются исходя из требований технического задания / задания на проектирование, а также из положений пунктов «Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах...» (Приказ ФСТЭК России №31 в ред. приказов ФСТЭК России № 49 и № 138).

В случае, если проектируемый объект признан ЗОКИИ, и ему присвоена одна из категорий значимости, исходя из положений ПП №127, проектирование осуществляется с учетом категории значимости объекта КИИ согласно Требованиям, установленным Приказом ФСТЭК № 239 с учетом утвержденной модели угроз безопасности информации. Минимальная категория значимости объекта КИИ– 3 (третья).

Предварительно, для объекта рассматриваются 3 категория значимости и 3 класс защищенности.

3.2. Определение угроз безопасности информации

В соответствии с пунктом 11 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных Приказом ФСТЭК России от 29 декабря 2017 г. №239, а также в соответствии с пунктом 13 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, утвержденных Приказом ФСТЭК России от 14 марта 2017 г. №31.

Проектирование СОИБ осуществляется с учетом Модели УБИ.

Моделирование угроз проведено с учетом методологических документов ФСТЭК России, указанных в части «1.4 Основание разработки».

Результаты моделирования угроз приведены в Приложении 1 настоящему проекту.

3.3. Определение состава и базового набора мер защиты информации

С учетом требований к 3 классу защищенности проектируемого объекта, в соответствии с п.19 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, установленных Приказом ФСТЭК №31, определен следующий базовый набор мер защиты информации: ИАФ.0, ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7, УПД.0, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, УПД.14, ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.7, ЗНИ.8, АУД.0, АУД.1, АУД.2, АУД.3, АУД.4, АУД.6, АУД.7, АУД.8, АУД.10, АВЗ.0, АВЗ.1, АВЗ.2, АВЗ.4, ОЦЛ.0, ОЦЛ.1, ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8, ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5, ЗИС.0, ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.21, ЗИС.32, ЗИС.34, ЗИС.38, ЗИС.39, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, УКФ.0, УКФ.2, УКФ.3, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4, ПЛН.0, ПЛН.1, ПЛН.2, ДНС.0, ДНС.1, ДНС.2, ДНС.5, ДНС.6, ИПО.0, ИПО.1, ИПО.2, ИПО.4.

С учетом требований к 3 категории значимости проектируемого объекта, в соответствии с п.23 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденных Приказом №239, определен следующий базовый набор мер защиты информации: ИАФ.0, ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7, УПД.0, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, УПД.14, ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.7, ЗНИ.8, АУД.0, АУД.1, АУД.2, АУД.3, АУД.4, АУД.6, АУД.7, АУД.8, АУД.10, АВЗ.0, АВЗ.1, АВЗ.2, АВЗ.4, ОЦЛ.0, ОЦЛ.1, ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8, ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5, ЗИС.0, ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.21, ЗИС.32, ЗИС.34, ЗИС.35, ЗИС.38, ЗИС.39, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5,

ИНЦ.6, УКФ.0, УКФ.2, УКФ.3, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4, ПЛН.0, ПЛН.1, ПЛН.2, ДНС.0, ДНС.1, ДНС.2, ДНС.5, ИПО.0, ИПО.1, ИПО.2, ИПО.4.

Меры защиты для 3 класса защищенности и 3 категории значимости идентичны, за исключением мер ДНС.6, ЗИС.6, ЗИС.35, ИНЦ.6. Для обеспечения соответствия требованиям, установленным 31 и 239 Приказами ФСТЭК, необходимо совместить указанные меры в СОИБ.

Таким образом, базовый набор мер защиты включает в себя следующие меры: ИАФ.0, ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.7, УПД.0, УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.10, УПД.11, УПД.13, УПД.14, ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.7, ЗНИ.8, АУД.0, АУД.1, АУД.2, АУД.3, АУД.4, АУД.6, АУД.7, АУД.8, АУД.10, АВЗ.0, АВЗ.1, АВЗ.2, АВЗ.4, ОЦЛ.0, ОЦЛ.1, ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8, ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗТС.5, ЗИС.0, ЗИС.1, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.21, ЗИС.32, ЗИС.34, ЗИС.35, ЗИС.38, ЗИС.39, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, ИНЦ.6, УКФ.0, УКФ.2, УКФ.3, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4, ПЛН.0, ПЛН.1, ПЛН.2, ДНС.0, ДНС.1, ДНС.2, ДНС.5, ДНС.6, ИПО.0, ИПО.1, ИПО.2, ИПО.4.

При выборе мер защиты информации для их реализации в автоматизированной системе управления предусмотрено исключение из базового набора мер защиты информации мер, непосредственно связанных с технологиями, не используемыми в данной системе или на данном уровне.

3.4. Адаптация базового набора мер защиты информации

В соответствии с п.23 Приказа ФСТЭК России от 25.12.2017 № 239 при выборе мер по обеспечению безопасности значимого объекта предусмотрено исключение из базового набора мер по обеспечению безопасности, мер, непосредственно связанных с информационными технологиями (далее — ИТ), не используемыми в значимом объекте или характеристиками, не свойственными значимому объекту.

С учетом сведений о структурно-функциональных характеристиках объекта защиты, применяемых технологиях и особенностях функционирования, при адаптации представленных базовых наборов были исключены следующие меры:

- ЗИС.32 Защита беспроводных технологий (технологии типа 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и т.д. не применяются, защита каналов передачи данных, включая GPRS, реализуется в рамках ЗИС.19);
- ЗИС.38 Защита информации при использовании мобильных устройств (мобильные устройства не используются (отсутствуют) в составе объекта защиты);
- ЗИС.39 Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (технология виртуализации не применяется).

Применение средств антивирусной защиты (далее — САВЗ) в технических средствах АС на ARM-процессорах влечет создание дополнительных временных задержек на анализ трафика и его сравнения с базой антивирусных сигнатур, что может оказать негативное влияние на штатный режим их функционирования.

В соответствии с пунктом 26 Приказа ФСТЭК №239, при отсутствии возможности реализации отдельных мер по обеспечению безопасности и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на функционирование значимого объекта в проектных режимах, должны быть разработаны и внедрены компенсирующие меры, обеспечивающие блокирование (нейтрализацию) УБИ с необходимым уровнем защищенности значимого объекта.

Обеспечение необходимого уровня защищенности автоматизированной системы управления (далее — АСУ) и адекватного блокирования (нейтрализацию) угроз заражения вредоносным программным обеспечением (далее — ВПО) по основным и резервным каналам связи технологических сегментов с вышестоящими уровнями операторского (диспетчерского) управления объектами электросети реализуется за счет реализации защищенного средствами криптографической защиты информации (далее- СКЗИ) канала связи между ПС и вышестоящим уровнем операторского (диспетчерского) управления объектами электросети.

Обеспечение необходимого уровня защищенности АСУ и адекватного блокирования (нейтрализацию) угроз заражения ВПО через санкционированное подключение к сети технологических сегментов переносных АРМ и устройств (при наладке, конфигурации, диагностике и т.п.) реализуется за счет наличия на переносных АРМ САВЗ или применением организационных мер, предусматривающих предварительную проверку всех подключаемых к сети технологических сегментов носителей информации на отдельных АРМ с установленным САВЗ с актуальными обновлениями.

3.5. Уточнение и дополнение базового набора мер защиты информации

Для нейтрализации актуальных угроз, приведенных в модели угроз, необходимо применение мер, указанных в таблице 1.

Таблица 1 – Меры защиты при нейтрализации угроз

№	Идентификатор угрозы	Наименование угрозы	Меры защиты, нейтрализующие угрозу
1.	УБИ.006	Угроза внедрения кода или данных	ИАФ.3, УПД.2, УПД.4, УПД.5, УПД.13, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8, АУД.2, АВЗ.1, АВЗ.2, АВЗ.4
2.	УБИ.022	Угроза избыточного выделения оперативной памяти	УПД.2, УПД.4, УПД.5, АУД.2,
3.	УБИ.025	Угроза изменения системных и глобальных переменных	УПД.2, УПД.4, УПД.5, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8, АУД.2, АВЗ.1, АВЗ.2, АВЗ.4
4.	УБИ.069	Угроза неправомерных действий в каналах связи	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, УПД.13,
5.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации	ИАФ.7, УПД.2, УПД.4, УПД.5, АУД.2, АВЗ.1, АВЗ.2, АВЗ.4
6.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации	ИАФ.3, ИАФ.4, ИАФ.7, УПД.2, УПД.4, УПД.5, АУД.2, АВЗ.1, АВЗ.2, АВЗ.4
7.	УБИ.089	Угроза несанкционированного редактирования реестра	УПД.2, УПД.4, УПД.5, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8, АУД.2,
8.	УБИ.091	Угроза несанкционированного удаления защищаемой информации	УПД.2, ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АУД.2, АВЗ.1, АВЗ.2, АВЗ.4
9.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8, АУД.2
10.	УБИ.099	Угроза обнаружения хостов	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8, АУД.2,
11.	УБИ.103	Угроза определения типов объектов защиты	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АУД.2
12.	УБИ.104	Угроза определения топологии вычислительной сети	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8,
13.	УБИ.109	Угроза перебора всех настроек и параметров приложения	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35
14.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УПД.2, ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, УПД.4, УПД.5
15.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, УПД.13
16.	УБИ.132	Угроза получения предварительной информации об объекте защиты	ИАФ.1, ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8, АУД.2
17.	УБИ.139	Угроза преодоления физической защиты	ЗТС.2, ЗТС.3
18.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»	ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, АВЗ.1, АВЗ.2, АВЗ.4
19.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	ЗТС.2, ЗТС.3
20.	УБИ.169	Угроза наличия механизмов разработчика	АУД.2
21.	УБИ.170	Угроза неправомерного шифрования информации	УПД.5, УПД.6, АУД.2
22.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	ОДТ.5, ОДТ.6
23.	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	УПД.2, ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, УПД.4, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8,
24.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации	УПД.2, УПД.4
25.	УБИ.212	Угроза перехвата управления ИС	ИАФ.1 – ИАФ-6; УПД.1 – УПД.4, , ЗИС.2, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.35, УПД.4, УПД.13, АУД.1, АУД.2, АУД.4, АУД.7, АУД.8

Идентификаторы указанных мер защиты в таблице 1, соответствуют обозначениям и номерам мер, установленных Приказом ФСТЭК № 239 и приказом ФСТЭК № 31.

3.6. Итоговый набор мер и подсистемы обеспечения информационной безопасности

Адаптированный набор организационных и технических мер обеспечения ИБ, включая общее описание выполнения требований, представлен в таблице 2. В соответствии с требованием задания на проектирование о наличии в составе подсистем ИБ подсистемы анализа сетевого трафика в итоговый адаптированный набор мер обеспечения ИБ добавлены меры АУД.5, контроль и анализ сетевого трафика и СОВ.1 Обнаружение и предотвращение компьютерных атак

Таблица 2 – Адаптированный набор мер ИБ

Мера	Требования к функционированию	Реализация требований (способ реализации: О – организационные меры; Т – технические меры)
Подсистема идентификации и аутентификации (ИАФ)		
ИАФ.0	Регламентация правил и процедур идентификации и аутентификации	Наличие и выполнение утвержденных локально-нормативных актов Общества, регламентирующих правила и процедуры идентификации и аутентификации (О)
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	Реализуется на уровне подсистемы идентификации и аутентификации технологической операционной системы «TOPAZ LINUX» (далее – ТОС). Аутентификация пользователей осуществляется по паролям (Т)
ИАФ.2	Идентификация и аутентификация устройств	Реализуется настройками ТОС путем идентификации и контроля подключаемых устройств и возможности блокирования подключения не доверенных устройств. (Т)
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Реализуется на уровне подсистемы идентификации и аутентификации ТОС. При передаче аутентификационной информации по каналам связи, защита организуется путем встроенных алгоритмов криптографической защиты информации системного и прикладного программного обеспечения (далее – ПО), а также защитой каналов связи, описанной мерой ЗИС.19. (Т)
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	
ИАФ.5	Идентификация и аутентификация внешних пользователей	
ИАФ.7	Защита аутентификационной информации при передаче	
Подсистема управления доступом (УПД)		
УПД.0	Регламентация правил и процедур управления доступом	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры соответствующих подсистем ИБ (О)
УПД.1	Управление учетными записями пользователей	В рамках организационных мер реализуется через: – управление учетными записями на протяжении всего жизненного цикла учетной записи пользователя (создание, изменение, блокирование, удаление) в соответствии с требованиями локальных нормативных актов; – реализация модели управления доступом в соответствии с требованиями локальных нормативных актов; – разделение полномочий (ролей) пользователей и администраторов, обеспечивающих функционирование соответствующих компонент в соответствии с их должностными обязанностями (функциями) в соответствии с требованиями локальных нормативных актов; – назначение прав и привилегий, минимально необходимых для выполнения пользователями своих должностных обязанностей. В рамках технических мер реализуется на уровне подсистемы идентификации и аутентификации ТОС
УПД.2	Реализация модели управления доступом	
УПД.4	Разделение полномочий (ролей) пользователей	
УПД.5	Назначение минимально необходимых прав и привилегий	
УПД.6	Ограничение неуспешных попыток доступа в ИС	Реализуется на уровне подсистемы идентификации и аутентификации ТОС, СКЗИ, сетевого оборудования, САВЗ. (Т)
УПД.10	Блокирование сеанса доступа пользователя при неактивности	
УПД.11	Управление действиями пользователей до идентификации и аутентификации	
УПД.13	Реализация защищенного удаленного доступа	Реализация защищенного удаленного доступа (Т)

Мера	Требования к функционированию	Реализация требований (способ реализации: О – организационные меры; Т – технические меры)
УПД.14	Контроль доступа из внешних ИС	осуществляется настройкой межсетевого экранирования (далее – МСЭ) и защитой каналов связи. (Т)
Подсистема защиты машинных носителей информации (ЗНИ)		
ЗНИ.0	Регламентация правил и процедур защиты машинных носителей информации (далее – МНИ)	Наличие и выполнение утвержденных локально-нормативных актов Общества, регламентирующих правила и процедуры защиты МНИ (О)
ЗНИ.1	Учет МНИ	
ЗНИ.2	Управление доступом к МНИ	
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на МНИ	Реализация требований достигается путем ограничения доступа (в том числе физического) к портам ввода-вывода компонентов сети (О)
ЗНИ.7	Контроль подключения съемных МНИ	
ЗНИ.8	Уничтожение (стирание) информации на МНИ	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры защиты МНИ (О)
Подсистема аудита безопасности (АУД)		
АУД.0	Регламентация правил и процедур аудита безопасности	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры аудита безопасности (О)
АУД.1	Инвентаризация информационных ресурсов	
АУД.2	Анализ уязвимостей и их устранение	Анализ уязвимостей и их устранение реализуется в соответствии с процессами аудита безопасности, регламентированных локально-нормативными актами с применением технических средств анализа уязвимостей (сканеров безопасности) с учетом недопустимости негативного влияния на функционирование значимого объекта (Т,О)
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	Генерирование временных меток и (или) синхронизация системного времени реализуется функциями сетевого оборудования. (Т)
АУД.4	Регистрация событий безопасности	Регистрация событий осуществляется локально, функциями журналирования событий безопасности ТОС и прикладного ПО. Возможна настройка локального хранения журнала событий для отправки по протоколу syslog в систему типа SIEM (при наличии) (Т)
АУД.5	Контроль и анализ сетевого трафика	Реализуется в виде решения с централизованным управлением (Т)
АУД.6	Защита информации о событиях безопасности	Защита информации о событиях безопасности реализуется локально, функциями управления доступом к журналам событий безопасности ТОС, СКЗИ, сетевого оборудования, (Т)
АУД.7	Мониторинг безопасности	Реализуется функционалом ТОС, СКЗИ, сетевого оборудования, который предоставляет администратору возможность просмотра информации о событиях безопасности (Т)
АУД.8	Реагирование на сбои при регистрации событий безопасности	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры аудита безопасности. При наличии системы типа SIEM, в нее отправляются данные с устройств соответствующих уровней. (Т)
АУД.10	Проведение внутренних аудитов	
Антивирусная защита (АВЗ)		
АВЗ.0	Разработка политики антивирусной защиты	Документальное обеспечение: Политика ИБ КИИ; Регламент АВЗ ЗОКИИ (О)
АВЗ.1	Реализация антивирусной защиты	САВЗ установлены и настроены на АРМ и серверах (Т).
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	САВЗ осуществляют обновление базы данных признаков вредоносных компьютерных программ (вирусов). (Т)
Подсистема обеспечения целостности (ОЦЛ)		
ОЦЛ.0	Регламентация правил и процедур обеспечения целостности	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры обеспечения целостности (О)
ОЦЛ.1	Контроль целостности ПО	Реализуется функцией ТОС, СКЗИ, сетевого оборудования. Операция проверки целостности хранимых данных может осуществляться по запросу администратора либо в заданный администратором с использованием

Мера	Требования к функционированию	Реализация требований (способ реализации: О – организационные меры; Т – технические меры)
		системного планировщика момент времени. (Т)
Подсистема обеспечения доступности (ОДТ)		
ОДТ.0	Регламентация правил и процедур обеспечения доступности	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры резервного копирования конфигураций (или файлов настройки) (О)
ОДТ.4	Резервное копирование информации	
ОДТ.5	Обеспечение возможности восстановления информации	
ОДТ.6	Обеспечение возможности восстановления ПО при нештатных ситуациях	
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	
Подсистема защиты технических средств и систем (ЗТС)		
ЗТС.0	Регламентация правил и процедур защиты технических средств и систем	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры соответствующих подсистем ИБ (О)
ЗТС.2	Организация контролируемой зоны	
ЗТС.3	Управление физическим доступом	
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (О)
ЗТС.5	Защита от внешних воздействий	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры соответствующих подсистем ИБ (О)
Подсистема защиты информационной (автоматизированной) системы и ее компонентов (ЗИС)		
ЗИС.0	Регламентация правил и процедур защиты ИС и ее компонентов	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры соответствующих подсистем ИБ (О)
ЗИС.1	Разделение функций по управлению (администрированию) ИС с иными функциями	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями (О)
ЗИС.2	Защита периметра ИС	Реализуется установкой и настройкой подсистемы МСЭ, осуществляющей фильтрацию сетевого трафика (Т)
ЗИС.3	Эшелонированная защита ИС	
ЗИС.5	Организация демилитаризованной зоны	
ЗИС.6	Управление сетевыми потоками	
ЗИС.8	Сокрытие архитектуры и конфигурации ИС	
ЗИС.19	Защита информации при ее передаче по каналам связи	
ЗИС.20	Обеспечение доверенных канала, маршрута	
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	Реализуется путем ограничения сетевого взаимодействия перечнем необходимых IP-адресов и портов, а также настройкой периферийных устройств (Т)
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	Реализуется установкой и настройкой подсистемы МСЭ, осуществляющей фильтрацию сетевого трафика (Т)
ЗИС.35	Управление сетевыми соединениями	
Подсистема реагирования на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Регламентация правил и процедур реагирования на компьютерные инциденты	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры организации выявления компьютерных инцидентов, информирования о них, анализа и устранения последствий, а также принятия мер по предотвращению их повторного возникновения. (О)
ИНЦ.1	Выявление компьютерных инцидентов	
ИНЦ.2	Информирование о компьютерных инцидентах	
ИНЦ.3	Анализ компьютерных инцидентов	
ИНЦ.4	Устранение последствий компьютерных инцидентов	
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	Хранение информации о компьютерных инцидентах осуществляется локально, функциями журналирования событий безопасности ТОС, СКЗИ, сетевого оборудования (Т)
Подсистема управления конфигурацией (УКФ)		
УКФ.0	Регламентация правил и процедур управления конфигурацией ИС	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры управления конфигурацией (О)
УКФ.2	Управление изменениями	
УКФ.3	Установка (инсталляция) только разрешенного к использованию ПО	
Подсистема управления обновлениями ПО (ОПО)		

Мера	Требования к функционированию	Реализация требований (способ реализации: О – организационные меры; Т – технические меры)
ОПО.0	Регламентация правил и процедур управления обновлениями ПО	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры обновления ПО (О)
ОПО.3	Тестирование обновлений ПО	
Подсистема планирования мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры планирования мероприятий по обеспечению защиты информации (О)
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	
Подсистема обеспечения действий в нештатных ситуациях (ДНС)		
ДНС.0	Регламентация правил и процедур обеспечения действий в нештатных ситуациях	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры обеспечения действий в нештатных ситуациях (О)
ДНС.1	Разработка плана действий в нештатных ситуациях	
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	Организация процесса обучения и отработки действий персонала в нештатных ситуациях (О)
ДНС.5	Обеспечение возможности восстановления ИС в случае возникновения нештатных ситуаций	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры обеспечения действий в нештатных ситуациях (О)
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	Организация анализа возникших нештатных ситуаций и принятию мер по недопущению их повторного возникновения, в соответствии с требованиями локально-нормативных актов, регламентирующих правила и процедуры обеспечения действий в нештатных ситуациях (О)
Подсистема информирования и обучения персонала (ИПО)		
ИПО.0	Регламентация правил и процедур информирования и обучения персонала	Наличие и выполнение утвержденных локально-нормативных актов, регламентирующих правила и процедуры информирования и обучения персонала (О)
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	
ИПО.2	Обучение персонала правилам безопасной работы	
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	

Согласно п. 27 Требований, установленных Приказом ФСТЭК № 239:

– 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 ПО), а также обеспечения безопасности программного обеспечения и программно-аппаратных средств, применяемых на значимых объектах.

Согласно п. 24 Требований, установленных Приказом ФСТЭК № 31:

– Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного ПО АСУ при их наличии.

В соответствии с Распоряжением ПАО «Россети» от 01.04.2016 г. № 140 Об утверждении минимальных требований к информационной безопасности АСТУ», в рамках разработки мер защиты, в СОИБ учтены требования к АС первой группы, класс защищенности 1 Г (по РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации». Далее – РД АС).

К классу защищенности 1 Г в общем виде предъявляются следующие требования:

1 Подсистема управления доступом.

(a) Идентификация, проверка подлинности и контроль доступа субъектов:

- в систему;
- к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;
- к программам;
- к томам, каталогам, файлам, записям, полям записей;

2 Подсистема регистрации и учета.

(a) Регистрация и учет:

- входа (выхода) субъектов доступа в (из) систему (узел сети);
- выдачи печатных (графических) выходных документов;
- запуска (завершения) программ и процессов (заданий, задач);
- доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи;
- доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;

(b) Учет носителей информации;

(c) Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей;

3 Подсистема обеспечения целостности:

(a) Обеспечение целостности программных средств и обрабатываемой информации;

(b) Физическая охрана средств вычислительной техники и носителей информации;

(c) Периодическое тестирование СЗИ НСД;

(d) Наличие средств восстановления СЗИ НСД;

Требования к АС класса 1Г выполняются мерами защиты в рамках подсистем СОИБ, разработанных согласно требованиям ФСТЭК к 3 классу защищенности (Приказ ФСТЭК №31).

Корреляция всех требований к 1 Г и разработанных в рамках текущего проекта подсистем СОИБ, представлена ниже.

1 Подсистема управления доступом согласно РД АС:

(a) должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов. Данное требование реализуется в подсистеме идентификации и аутентификации.

(b) должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам. Данное требование реализуется в подсистеме управления доступом;

(c) должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам. Данное требование реализуется в подсистеме идентификации и аутентификации;

(d) должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа. Данное требование реализуется в подсистеме управления доступом.

2 Подсистема регистрации и учета согласно РД АС:

(a) должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы (далее — ОС) и ее программного состава. Регистрация выхода из системы или остановка не проводится в моменты аппаратурного отключения АС. Данное требование реализуется в подсистеме идентификации и аутентификации. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- результат попытки входа: успешная или неуспешная – несанкционированная;
- идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- код или пароль, предъявленный при неуспешной попытке;

(b) должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию

(не актуально для существующей АС, т.к. в ее составе отсутствуют указанные устройства).

(c) – должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются (реализуется механизмом аутентификации согласно подсистеме СОИБ «Подсистема идентификация и аутентификация (ИАФ)):

- дата и время запуска;
- имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный – несанкционированный);

(d) должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. Данное требование реализуется в подсистеме идентификации и аутентификации. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;

(e) должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. Данное требование реализуется в подсистеме идентификации и аутентификации, подсистеме регистрации событий безопасности, подсистеме сбора, регистрации, корреляции и анализа событий безопасности. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];

(f) должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку). Реализуется организационными мерами, регламентируется внутренней нормативной документацией Общества;

(g) учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема). Реализуется организационными мерами, регламентируется внутренней нормативной документацией Общества;

(h) должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). Регламентируется внутренней нормативной документацией Общества.

3 Подсистема обеспечения целостности согласно РД АС:

(a) должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ. Реализуется организационными мерами, регламентируется внутренней нормативной документацией Общества.;
- целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации. Регламентируется внутренней нормативной документацией Общества., рассматривается состав ПО защищаемого объекта;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно

в нерабочее время. Реализуется организационными мерами, регламентируется внутренней нормативной документацией Общества.

(b) должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест – программ, имитирующих попытки НСД. Реализуется организационными мерами, регламентируется внутренней нормативной документацией Общества.

(c) должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности. Реализуется организационными мерами, регламентируется внутренней нормативной документацией Общества.

4. Описание решений по организационным и техническим мерам обеспечения информационной безопасности

4.1. Общие сведения по обеспечению информационной безопасности

СОИБ строится путем комплексного использования программно-аппаратных и организационных мер защиты, необходимых для обеспечения требуемых функций СОИБ.

На основании действующих нормативных документов Российской Федерации в области защиты информации, разрабатываемая СОИБ АС включает в себя комплекс организационных, программных и технических решений по обеспечению безопасности информации.

Эффективность защиты информационных ресурсов достигается комплексным применением различных защитных механизмов, функционирующих в рамках следующих общих принципов:

- учет требований нормативно-правовых и руководящих документов по обеспечению безопасности информации при разработке СОИБ;
- комплексный подход к построению СОИБ;
- обеспечение защиты информации, содержащейся в ИС на всех этапах ее обработки и во всех режимах функционирования;
- модульность построения системы защиты информации;
- обеспечение необходимого уровня защиты информации при минимальных финансовых затратах.

Состав мер, определенных согласно Приказам ФСТЭК № 239 и 31, был сокращен и распределён по подсистемам СОИБ согласно таблице 3. Состав оборудования, реализующего СОИБ, указан в таблице 6.

Таблица 3 – Соответствие подсистем СОИБ выделенным подсистемам и определенным мерам

№	Подсистема СОИБ	Меры согласно Приказу ФСТЭК № 31
1.	защиты каналов связи и МСЭ	ИАФ.2, ИАФ.7, УПД.13, УПД.14, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.8, ЗИС.19, ЗИС.20, ЗИС.34, ЗИС.35
2.	идентификации и аутентификации	ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5
3.	управления доступом	УПД.1, УПД.2, УПД.6, УПД.10, УПД.11,
4.	регистрации событий безопасности	АУД.3, АУД.4, АУД.5, АУД.6
5.	обеспечения целостности	ОПО.1, ОПО.2, ОПО.4
6.	обнаружения вторжений	СОВ.1, СОВ.2, АУД.3, АУД.4, АУД.5, АУД.6
7.	резервного копирования и восстановления информации, централизованного обновления ПО	ОДТ.4, ОДТ.5, ОДТ.6
8.	антивирусной защиты	АВЗ.1, АВЗ.4

В соответствии с определенным набором мер защиты информации, для СОИБ определены следующие подсистемы:

1 защиты каналов связи и МСЭ;

2 идентификации и аутентификации;

3 управления доступом;

4 регистрации событий безопасности;

5 обеспечения целостности;

6 обнаружения вторжений;

7 резервного копирования и восстановления информации, централизованного обновления ПО;

8 Антивирусной защиты

При проектировании и построении СОИБ максимально используются оборудование, технологические решения и применяемые СрЗИ, применяемые в Обществе. Проектируемая СОИБ учитывает существующую в настоящее время

организационную структуру обеспечения безопасности Общества.

СрЗИ, входящие в состав СОИБ, совместимы с имеющимися программно-техническими средствами.

Отдельные меры защиты подсистем защиты машинных носителей информации (ЗНИ), аудита безопасности (АУД), обеспечения доступности (ОДТ), защиты информационной (автоматизированной) системы и ее компонентов (ЗИС) реализуется на базе функций встроенной ОС серверов доступа к данным, технологического ПО контроллеров телемеханики, автоматов релейной защиты.

На уровне ПС СОИБ в рамках настоящего проекта реализуется следующими средствами (таблица 4).

Таблица 4 – СОИБ ПС

№	Наименование и техническая характеристика оборудования	Примечание
1	**Сетевое оборудование**	
1.1	Сетевой коммутатор TOPAZ SW528-4GTxSFP-24Tx-M-2LV-DGN-CS	
2	**Комплект Системы централизованного обновления (СЦО) TOPAZ.SCR-512 в составе:**	
2.1	Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (SCR) с СПО TOPAZ SCR	
2.2	Сертифицированная технологическая операционная система (ТОС) TOPAZ LINUX с сертифицированным установочным комплектом (далее — ТОС)	
3	**Комплект Системы обнаружения вторжений (СОВ) TOPAZ.IDS-04 в составе:**	
3.1	Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (IDS-04) с СПО TOPAZ IDS-04	
3.2	Средство обнаружения вторжений – Права на программу для ЭВМ. Право на использование Системы обнаружения вторжений СОВ «Кречет», с сертификатом активации сервиса совместной технической поддержки и установочным комплектом (Flash-накопитель)	
3.3	ТОС	
4	**Комплект Системы контроля целостности и резервного копирования (СКЦРК) TOPAZ.ICB-FW-512 в составе:**	
4.1	Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (ICB) с СПО TOPAZ ICB	
4.2	ТОС	
5.	**МСЭ/СКЗИ**	
5.1	ПАК ViPNet Coordinator IG 100 4.x (Utun) I4	
6.	**Kaspersky Industrial CyberSecurity for Netwoks**	
6.1	Сервер TOPAZ IEC DAS MX683 E6R4	
6.2	ПО KICS for Networks	
6.3	Astra Linux Special Edition	

Реализация подсистем СОИБ в комплексе приведена в таблице 5.

Таблица 5 – Средства реализации подсистем СОИБ

№	Подсистема	Средство реализации
1.	защиты каналов связи и МСЭ	ПАК ViPNet Coordinator IG 100 4.x (Utun) I4
		Сетевой коммутатор TOPAZ SW528-4GTxSFP-24Tx-M-2LV-DGN-CS
2.	идентификации и аутентификации	ПАК ViPNet Coordinator IG 100 4.x (Utun) I4
		ТОС
		Astra Linux Special Edition
3.	управления доступом	ПАК ViPNet Coordinator IG 100 4.x (Utun) I4
		ТОС
		Astra Linux Special Edition
		KICS for Networks
4.	регистрации событий безопасности	ПАК ViPNet Coordinator IG 100 4.x (Utun) I4
		ТОС
		Astra Linux Special Edition
		KICS for Networks
		Комплект Системы обнаружения вторжений (СОВ) TOPAZ.IDS-04
5.	обеспечения целостности	ПАК ViPNet Coordinator IG 100 4.x (Utun) I4
		Astra Linux Special Edition
		ТОС
		ПО резервного копирования и восстановления данных для рабочей станции (ФСТЭК) Кибер Бэкап
		Комплект Системы контроля целостности и резервного копирования (СКЦРК) TOPAZ.ICB-FW-512
6.	обнаружения вторжений	Комплект Системы обнаружения вторжений (СОВ) TOPAZ.IDS-04
		KICS for Networks

№	Подсистема	Средство реализации
7.	резервного копирования и восстановления информации, централизованного обновления ПО	ПО резервного копирования и восстановления данных для рабочей станции (ФСТЭК) Кибер Бэкап
		Комплект Системы централизованного обновления (СЦО) TOPAZ.SCR-512
		Комплект Системы контроля целостности и резервного копирования (СКЦРК) TOPAZ.ICB-FW-512
8.	антивирусной защиты	Kaspersky Industrial CyberSecurity for Linux Nodes, Workstation
		Kaspersky Industrial CyberSecurity for Linux Nodes, Server

Разработка технических решений проводилась с учетом пункта 8 Приказа ФСТЭК №31, в соответствии с которым разрабатываемые меры не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

4.2. Организационные меры

Следующие требования по обеспечению безопасности выполняются организационными мерами: ИАФ.0, УПД.0, УПД.5, ЗНИ.0, ЗНИ.1, ЗНИ.8, АУД.0, АУД.10, АВЗ.0, ОЦЛ.0, ОЦЛ.1, ОДТ.0, ОДТ.4, ОДТ.5, ОДТ.6, ОДТ.8, ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4, ЗИС.0, ЗИС.1, ЗИС.2, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4, ПЛН.0, ПЛН.1, ПЛН.2, ДНС.0, ДНС.1, ДНС.2, ДНС.5, ДНС.6, ИПО.0, ИПО.1, ИПО.2, ИПО.4, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5, УКФ.0, УКФ.2, УКФ.3.

Организационные меры реализуются следующим образом:

1 Все подсистемы СОИБ:

- наличие и выполнение утвержденных локально-нормативных актов Общества, регламентирующих правила и процедуры соответствующих подсистем ИБ.

2 Подсистема управления доступом (УПД)

- управление учетными записями на протяжении всего жизненного цикла учетной записи пользователя (создание, изменение, блокирование, удаление) в соответствии с требованиями локальных нормативных актов;
- реализация модели управления доступом в соответствии с требованиями локальных нормативных актов;
- разделение полномочий (ролей) пользователей и администраторов, обеспечивающих функционирование соответствующих компонент в соответствии с их должностными обязанностями (функциями) в соответствии с требованиями локальных нормативных актов, указанных в описании меры;
- назначение прав и привилегий, минимально необходимых для выполнения пользователями своих должностных обязанностей (функций);

3 Подсистема обеспечения доступности (ОДТ)

- наличие и выполнение утвержденных локально-нормативных актов Общества, регламентирующих правила и процедуры резервного копирования конфигураций (или файлов настройки) ПЛК.

4 Подсистема защиты технических средств (ЗТС):

- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

5 Подсистема защиты информационной (автоматизированной) системы и ее компонентов (ЗИС):

- разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями.

6 Подсистема обеспечения действий в нештатных ситуациях (ДНС)

- организация процесса обучения и отработки действий персонала в нештатных ситуациях;
- организация процесса ИБ по анализу возникших нештатных ситуаций и принятию мер по недопущению их повторного возникновения, в соответствии с требованиями локально-нормативных актов Общества, регламентирующих правила и процедуры обеспечения действий в нештатных ситуациях.

7 Подсистема реагирования на компьютерные инциденты (ИНЦ)

— организация процессов ИБ по выявлению компьютерных инцидентов, информированию о них, анализу, устранению последствий и принятию мер по предотвращению их повторного возникновения.

4.3. Общие требования к информационной безопасности технологического сегмента

В отношении общих принципов защиты информации в рамках всех объектов защиты технологического сегмента и ДП должны быть выполнены следующие условия (таблица 7).

Таблица 6 – Общие требования

№	Объект	Решение	Направление
1.	Все объекты	Заводские пароли по умолчанию изменяются	Управление доступом: идентификация и аутентификация
2.	Все объекты	Соответствие требованиям парольной политики. По сложности пароля: не менее 12 символов, наличие символов в разном регистре, наличие специальных символов. Устанавливается срок действия паролей и истории паролей.	Управление доступом: идентификация и аутентификация
3.	Все объекты	Доступ персонала персонализирован.	Управление доступом: идентификация и аутентификация
4.	Все объекты	При наличии технической возможности исключается возможность доступа к объектам защиты под одной учетной записью (одним паролем) для различных работников	Управление доступом: идентификация и аутентификация
5.	Все объекты	Неиспользуемые встроенные учетные записи на всех компонентах объектов защиты отключаются	Управление доступом: идентификация и аутентификация
6.	Все объекты	Высший приоритет применения на объектах защиты имеют механизмы доступа с применением многофакторной аутентификации	Управление доступом: идентификация и аутентификация
7.	Все объекты	Незадействованный функционал и компоненты объектов защиты отключаются	Состав объекта: функционал и компоненты
8.	Все объекты	Включены и настроены функции регистрации событий безопасности с передачей на специально выделенный сервер сбора событий ИБ в сегменте ДП	Состав объекта: функционал и компоненты
9.	Все объекты	Должны быть установлены процедуры обновлений безопасности, время применения обновления безопасности на компонентах объектов защиты не должно превышать 24 часов	Состав объекта: функционал и компоненты
10.	ДП	Должен быть организован периметр технологического сегмента ДП Объекта	Технические средства сегмента ДП: периметр
11.	ДП	Организация сетевого периметра ДП Объекта должна быть обеспечена посредством МСЭ	Технические средства сегмента ДП: периметр, МСЭ
12.	ДП	Физическое соединение технологического сегмента ДП Объекта с остальной информационно-телекоммуникационной сетью (далее — ИТС) Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции МСЭ	Технические средства сегмента ДП: периметр, МСЭ
13.	ДП	При наличии такой возможности, сегментирование реализуется одновременным применением следующих технологий и методов в порядке эффективности защиты: 1. физическое выделение, посредством организации сегментов за счет выделенных коммутирующих устройств, подключаемых только к межсетевым экранам (далее — МЭ); 2. VLAN с применением СКЗИ доступа к сети и защиты трафика (VPN с шифрованием).	Технические средства сегмента ДП: периметр, сегментирование
14.	ДП	Наличие сегмента управления (имеет доступ персонал, осуществляющий функции управления)	Объекты ДП: сегменты управления, обязательное наличие
15.	ДП	Наличие сегмента управления АСТУ/ССПИ/ТМ (имеет доступ персонал, осуществляющий функции управления АСТУ/ССПИ/ТМ)	Объекты ДП: сегменты управления, обязательное наличие
16.	ДП	Наличие сегмента управления подсистемами ИБ	Объекты ДП: сегменты управления, обязательное наличие
17.	ДП	Наличие сегмента оперативного управления (далее — ОПУ) Объектом (имеет доступ персонал, осуществляющий ОПУ оборудованием Объекта)	Объекты ДП: сегменты управления, обязательное наличие
18.	ДП	Доступ к технологическому сегменту ДП и другим входящим в него сегментам автоматизированной системы (далее — АС) только из	Объекты ДП: сегменты управления, доступ и

№	Объект	Решение	Направление
		сегмента ОПУ	взаимодействие
19.	ДП	Доступ к сегментам управления из других сегментов запрещен	Объекты ДП: сегменты управления, доступ и взаимодействие
20.	ДП	взаимодействие между сегментами исключительно через МСЭ	Объекты ДП: сегменты управления, доступ и взаимодействие
21.	ДП	в случае необходимости взаимодействия между сегментами АС, то обеспечивается посредством выделения специализированных «буферных» сегментов	Объекты ДП: сегменты управления, доступ и взаимодействие
22.	ДП	Правила на МСЭ максимально уточняются, включая указание адресов назначения и источника, портов назначения и источника	Технические средства сегмента ДП: периметр, МСЭ
23.	ДП	Для взаимодействия с внешними сетями и АС создаются «демилитаризованные» зоны	Технические средства сегмента ДП: периметр, МСЭ
24.	ДП	Служебные сервисы оборудования, образующего ДП, должны быть доступны только из сегмента управления ДП	Объекты ДП: сегменты управления, доступ и взаимодействие
25.	ДП	Неиспользуемые и небезопасные протоколы и сервисы на сетевом оборудовании отключаются	Состав объекта: функционал и компоненты
26.	ДП	Неиспользуемые порты на коммутационном оборудовании должны отключаются логически и физически	Состав объекта: функционал и компоненты
27.	ДП	В случае необходимости дополнительных мер доступ на уровне ИТС реализуется с применением протоколов 802.1x и фильтрации MAC адресов	Состав объекта: функционал и компоненты
28.	ДП	Технологические протоколы строго изолируются от внешнего проникновения	Состав объекта: функционал и компоненты
29.	ДП	Для контроля легитимности сетевых соединений реализуется сбор событий на уровне трафика в сети с передачей на сервер сбора событий ИБ	Состав объекта: функционал и компоненты
30.	Оборудование	На сетевом оборудовании должны быть включены функции от подмены сетевых адресов и меры защиты от внедрения ложной маршрутной информации в протоколы маршрутизации	Состав объекта: функционал и компоненты
31.	Оборудование	Функции безопасности, при их наличии, максимально используются на всем технологическом оборудовании Объекта и оборудовании безопасности, имеющем функции управления	Состав объекта: функционал и компоненты
32.	Оборудование	Оборудование подключается только к своим сегментам ДП	Состав объекта: функционал и компоненты
33.	Оборудование	Неиспользуемый функционал и интерфейсы связи отключены.	Состав объекта: функционал и компоненты

4.4. Структура системы обеспечения информационной безопасности

При проектировании и построении СОИБ максимально используются оборудование, технологические решения и применяемые СрЗИ, применяемые в Обществе.

Проектируемая СОИБ учитывает существующую в настоящее время организационную структуру обеспечения безопасности Общества.

Структурная схема СОИБ представлена в документе под шифром 6350-25-ИОС 5.3-ГЧ.1..

5. Система обеспечения информационной безопасности

5.1. Подсистема защиты каналов связи и межсетевого экранирования

5.1.1. Описание

Защита каналов реализуется посредством МСЭ и использованием СКЗИ.

Проектом предусмотрен МЭ — оборудование контроля и фильтрации пакетов информации сети передачи данных, осуществляющее контроль и фильтрацию проходящих через него пакетов информации сети передачи данных в соответствии с заданными правилами.

Установка МЭ, предусматривает фильтрацию пакетов выполняется в целях предотвращения передачи определенного вида трафика, как в сегмент сети передачи данных, так и из него.

МЭ, применяемый на объекте защиты, может иметь программное или программно-техническое исполнение и должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (IEC, Modbus, Profibus и (или) иные протоколы).

МЭ реализует следующие функции:

- фильтрация трафика с учетом полей сетевых пакетов (источник, получатель и сервис (порт));
- регистрация и учет фильтруемых пакетов с указанием адреса, времени и результата фильтрации;
- разбиение ЛВС на сегменты и обеспечение защиты периметров сегментов;
- идентификация и аутентификация администратора МЭ при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
- регистрация входа/выхода администратора МЭ в систему/из системы либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратного отключения МЭ);
- обеспечение отказоустойчивости комплекса МСЭ в случае программного или аппаратного сбоя;
- обеспечение производительности не ниже пропускной способности каналов связи, используемых для подключения защищаемых сегментов к остальной части ЛВС;
- резервирование настроек узлов МЭ в автоматическом режиме.

Проектом предусмотрено использование СКЗИ, которые обеспечивают:

- возможность построения защищённой VPN-сети и криптографической защиты информации, передаваемой с использованием стека протоколов TCP/IP, в произвольной телекоммуникационной инфраструктуре IP-сетей, включая сеть связи общего пользования;
- создание защищённых каналов посредством шифрования IP-трафика защищаемого сетевого узла и передачи этого IP-трафика на другие защищённые сетевые узлы или VPN-шлюзы;
- шифрование IP-пакетов;
- выработку имитовставки для IP-пакетов;
- постоянный контроль за состоянием служб и ведение статистики использования системных ресурсов;
- информирование о событиях сбоев служб;
- обнаружение факта сбоя службы и осуществление последующих попыток восстановления работоспособности службы;
- выполнение набора функций в соответствии с поставляемой вместе с изделием лицензией.

СКЗИ должен иметь действующий сертификат ФСБ России на соответствие требованиям к СКЗИ классов КС1, КС2, КС3.

Для удаленного доступа к файловой системе и функциям контроллеров используются организуемые по проекту защищенные шифрованные VPN тоннели.

Все сервисы ОС, не обеспечивающие шифрования при передаче данных, должны быть отключены при выполнении пуско-наладочных работ до включения системы для проведения автономных испытаний системы.

Трафик SSH, sFTP, HTTPS, SNMP разрешены только внутри шифрованного туннеля и в соответствующих сегментах (без возможности доступа из одного сегмента в другой). Весь трафик, кроме туннелированного

должен быть отключен и заблокирован.

Дополнительно, для организации удаленного доступа к функциям ОС контроллера используется протокол SSH, обеспечивающий безопасное управление за счет туннелирования TCP-соединений. Сервер SSH входит в состав стандартных сервисов встроенной ОС.

Для защиты конфигурации при удаленной передаче файлов конфигурации, средства конфигурирования контроллера используют безопасный протокол sFTP.

Для ввода конфигурации в действие, требуется независимое двухэтапное подтверждение. Первый этап подтверждения полномочий выполняется при консольном подключении по SSH. Все пользователи, имеющие права на подключение по SSH, не имеют прав на запись файлов в директорию конфигурации. Для получения прав на запись файлов конфигурации необходимо пройти вторую авторизацию.

Средства удаленного доступа, входящие в состав ПТК, обеспечивают ограничение длительности сессии удаленного доступа и обеспечивают закрытие сеанса при превышении установленного лимита времени.

5.1.2. Реализация

Защита каналов реализуется следующими программными и программно-аппаратными средствами:

- ПАК ViPNet Coordinator IG 100 4.x (Utun) I4.

ПАК ViPNet Coordinator IG 100 4.x (Utun) I4 выполняет функции МСЭ и СКЗИ на уроне ПС. Оборудование устанавливаются в точке подключения сегментов сети ПС к внешним сетям и служит для фильтрации входящего в локальные сети ПС сетевого трафика и разграничения доступа между существующими сегментами и сегментами, созданными в рамках проекта.

В рамках МСЭ, все сетевое взаимодействие осуществляется через защищенное соединение. Подсистема осуществляет контроль трафика между разными зонами и выполняет следующие основные функции:

1 сегментирование и разделение сетей;
2 защита периметра ИС;
3 пакетной фильтрации трафика;
4 статической и динамической трансляции сетевых адресов;
5 поддержку Stateful Packet Inspection;
6 организация DMZ зон;
7 разделение сетевых потоков;
8 балансировка нагрузки.

Для обеспечения разграничения доступа осуществляется сегментирование сети. Для каждого сегмента разрабатываются правила политики МСЭ.

Значения настраиваемых параметров определяются в ходе проведения работ по внедрению.

По умолчанию применяется правило «Запрещено все, что не разрешено».

Настройка разрешающих правил на МСЭ осуществляется согласно матрицы сетевого взаимодействия (таблица 8) и уточняется на этапе внедрения. Настройка разрешающих правил уточняется на этапе внедрения.

Администрирование МСЭ осуществляется через выделенный сетевой порт (таблица 9). Адресация систем определяется/уточняется на этапе внедрения.

Таблица 7 – Матрица сетевого взаимодействия.

Источник	Назначение	Протокол:порт	Описание
Администратор ИБ	МСЭ	TCP:10222	Администрирование МСЭ
МЭ	Сервер SIEM	UDP:514	Отправка событий
Коммутаторы	Сервер SIEM	UDP:514	Отправка событий

Таблица 8 – Правила проброса портов

Источник	Назначение	Внешний порт	Внутренний порт
Администратор ИБ	МСЭ	10222	22

Информация для отслеживания событий в защищенном сегменте сети передается на верхний уровень в ЦУС в существующую систему SIEM, события отслеживаются с АРМ Администратора безопасности (ЦУС расположен по адресу г. Москва, ул. Нижняя Красносельская, д. 6.)

5.2. Подсистемы идентификации и аутентификации. Подсистема управления доступом. Подсистема регистрации событий безопасности. Подсистема обеспечения целостности

5.2.1. Идентификация и аутентификация

Реализуются на уровне подсистемы идентификации и аутентификации^

- ТОС «TOPAZ LINUX»
- устройств «TOPAZ IEC DAS»;
- устройств «TOPAZ SW»;
- ПАК ViPNet Coordinator IG 100 4.x (Utun) I4.

Идентификация пользователей (в том числе администраторов) осуществляется по идентификаторам (именам учетных записей). Аутентификация пользователей осуществляется по паролям.

5.2.2. Управление доступом

ОС и ПО осуществляют ролевой контроль доступа для субъектов (администраторов, пользователей) к объектам (файлам).

5.2.3. Регистрация событий безопасности

Реализуются следующие возможности в части регистрации событий безопасности:

- предоставления администратору информации аудита;
- защиты хранимых записей регистрации событий безопасности;
- регистрации (аудита) событий безопасности;
- сохранения данных журнала регистрации событий безопасности;
- передачи данных аудита для внешнего хранения.

5.2.4. Обеспечение целостности

Реализуются следующие возможности:

- исключения непосредственного взаимодействия пользователей прикладного ПО с ОС;
- защиты хранимой аутентификационной информации от неправомерного доступа;
- предоставления меток времени при проведении аудита безопасности;
- защиты данных аудита при передаче;
- возможность защиты записей регистрации событий безопасности от несанкционированного доступа.

5.2.5. Реализация

На уровне ПС указанные подсистемы реализуются встроенными функциями ПАК ViPNet Coordinator.

На уровне ПС и ПП подсистемы реализуются ТОС, сертифицированной по требованиям безопасности информации.

ТОС встроена в промышленные контроллеры «TOPAZ» производства ООО «ПиЭлСи Технолоджи», и обеспечивает функционал защиты информации от несанкционированного доступа.

Технологическая операционная система «TOPAZ LINUX» сертифицирована по требованиям к ОС, профиль защиты ОС – Б четвертого класса защиты. ИТ.ОС.Б4.ПЗ, ЗБ, 4 уровень доверия. ТОС предназначена для реализации основных функций безопасности в рамках программно-технического комплекса автоматизированной системы.

ТОС обеспечивает:

1. выполнение целевых функций АСУ ТП на аппаратно-программных платформах с процессорной архитектурой ARM;
2. выбор устанавливаемых компонентов изделия;
3. настройку механизмов защиты информации при установке ОС;
4. настройку IP- адресов;
5. установку даты и времени на узлах сети с использованием NTP-сервера и NTP- клиента;

6 поддержку протокола синхронизации времени Precision Time Protocol v2 (PTP);
7 поддержку протоколов RSTP, STP, MSTP, PRP, HSR, sFTP;
8 поддержку SSH;
9 разрешение сетевых адресов и имен узлов сети с использованием DNS-сервера и DNS-клиента;
10 автоматизированную установку обновлений безопасности изделия.

ТОС обеспечивает следующие функциональные возможности ОС в части механизмов защиты:

1 идентификация и аутентификация пользователей до выполнения любых действий по доступу в информационную систему;
2 идентификация и аутентификация администраторов до выполнения действий по управлению ОС;
3 возможность идентификации субъекта доступа путем предъявления физического устройства идентификации до разрешения действия, выполняемого от имени этого субъекта доступа;
4 возможность задания политики дискреционного и (или) ролевого управления доступом для установленного множества операций, выполняемых субъектами доступа по отношению к объектам доступа;
5 возможность реализации дискреционного и (или) ролевого управления доступом на основе списков управления доступом (матрицы управления доступом) и (или) ролей;
6 возможность автоматического запуска прикладного программного обеспечения при старте СВТ;
7 возможность исключения непосредственного взаимодействия пользователей прикладного программного обеспечения с ОС;
8 возможность со стороны администратора управлять атрибутами безопасности;
9 возможность со стороны администратора управлять выполнением функций безопасности ОС;
10 возможность со стороны администратора управлять параметрами функций безопасности ОС, данными аудита;
11 поддержка определенных ролей для ОС и их ассоциации с пользователями ОС;
12 защита хранимой аутентификационной информации от неправомерного доступа к ней и раскрытия;
13 постоянный контроль и проверка правомочности обращений субъектов доступа к объектам доступа;
14 возможность предоставления надежных меток времени при проведении аудита безопасности;
15 возможность защиты данных аудита от несанкционированного раскрытия при их передаче;
16 возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, предоставляемая администратору;
17 возможность предоставления администратору всей информации аудита в понятном для него виде;
18 возможность защиты хранимых записей регистрации событий безопасности ОС (аудита) от несанкционированного удаления и предотвращения модификации записей аудита;
19 возможность регистрации (аудита) событий безопасности;
20 возможность выполнения действий, направленных на сохранение данных журнала регистрации событий безопасности ОС и обеспечивающих непрерывность
21 процесса аудита, если журнал регистрации событий безопасности ОС превысит определенный администратором размер;
22 возможность полнотекстовой регистрации привилегированных команд (команд, управляющих системными функциями);
23 возможность передавать данные аудита для внешнего хранения.

5.3. Подсистема обнаружения вторжений

5.3.1. Описание

Система обнаружения вторжения (далее СОВ) позволяет определять и регистрировать аномальные и важные, с точки зрения обеспечения безопасности эксплуатации оборудования, информационные события.

Применяемая система обнаружения вторжений включает компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

5.3.2. Реализация

Подсистема реализована на основе сервера доступа к данным с СПО «Кречет».

СОВ «Кречет» предназначена для применения в промышленных сетях. СОВ устанавливается на промышленные серверы доступа к данным линейки TOPAZ MX 681, аттестованные ПАО «Россети» (сервер доступа к данным TOPAZ IEC DAS MX681 E5R2 SSD512 (3GTx-2Tx-2R) (IDS-04), платформа TOPAZ IEC DAS включена в реестр российской радиоэлектронной продукции, № 10251251).

СОВ «Кречет» включена в реестр российского ПО (реестровая запись №22727) и сертифицирована по требованиям информационной безопасности (сертификат № 4770) к системам обнаружения вторжений.

СОВ позволяет определять и регистрировать аномальные и важные, с точки зрения обеспечения безопасности эксплуатации оборудования, информационные события.

Система анализирует копию трафика, проходящего через МСЭ, коммутаторы технологического сегмента.

Основные функциональные возможности СОВ:

- анализ промышленного протокола МЭК 60870-5-104;
- обнаружение в сети новых устройств;
- обнаружение подмены IP адреса;
- обнаружение сетевых атак и аномалий трафика;
- отправка событий в SIEM систему;
- возможность написания собственных правил.

Для управления системой используется SSH и web-интерфейс. Интерфейс позволяет отслеживать в реальном времени события СОВ, загрузку ЦП, сетевых интерфейсов, управлять правилами.

Обновление базы решающих правил осуществляется локально, согласно принятым в Компании политикам.

СПО «Кречет» обладает сертификатом соответствия требованиям информационной безопасности.

5.4. Подсистема резервного копирования и восстановления информации, централизованного обновления ПО

5.4.1. Описание

Резервное копирование осуществляется согласно принятой в Организации технической политики в области резервного копирования.

Комплекс резервного копирования выполняет следующие функции:

- обеспечение резервного копирования и восстановления данных СрЗИ;
- выполнение резервного копирования по расписанию;
- управление процессами резервного копирования и восстановления данных.

Требование по обновлению программного обеспечения является обязательным для систем АС третьего класса защищенности и для нейтрализации актуальных угроз безопасности.

Требование по резервному копированию информации и возможности ее восстановления является обязательным для систем АС третьего класса защищенности и для нейтрализации актуальных угроз безопасности.

5.4.2. Реализация

Проектом предусмотрена установка комплекта Системы контроля целостности и резервного копирования, а также комплекта Системы централизованного обновления, выполняющих функции обновления ПО СОИБ, резервное копирование информации и ее восстановления:

- Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) с СПО TOPAZ ICB;
- Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) с СПО TOPAZ SCR.

Резервное копирование настроек МЭ реализуется встроенными средствами ПО ПАК ViPNet Coordinator.

5.5. Подсистема анализа сетевого трафика и обнаружения компьютерных атак

Подсистема анализа сетевого трафика и обнаружения компьютерных атак реализуется в виде решения с централизованным управлением.

Анализ сетевого трафика производится за счёт подключения сервера с ПО KICS for Netwoks к порту коммутатора TOPAZ SW528, на который зеркалируется трафик сегментов сети ПС 220 кВ Мельниково.

ПО Kaspersky Security Center, установленное на главном сервере в ЦУС ПАО «Россети Московский регион», за счёт интеграции с KICS for Netwoks позволяет проводить обновления ПО, правил корреляции событий безопасности, а также сигнатурных баз.

ПО Kaspersky Update Utility, установленное на сервере обновлений в ЦУС ПАО «Россети Московский регион», позволяет получать обновления ПО и сигнатурных баз.

ПО Kaspersky Industrial CyberSecurity for Networks (KICS for Netwoks) обеспечивает функции регистрации узлов объекта и сетевого взаимодействия между ними, анализа сетевого трафика на канальном, сетевом и транспортном уровнях, детектирования аномалий технологического процесса, разбора, анализа и регистрации технологических параметров и сообщений, передаваемых на прикладном уровне с помощью промышленных коммуникационных протоколов, сбора и хранения событий безопасности.

5.6. Централизованное управление и мониторинг

Для централизованного сбора событий информационной безопасности на верхнем уровне решением предусмотрен централизованный сервер сбора и хранения событий информационной безопасности – Positive Technologies Max Patrol SIEM (далее MP SIEM). Компоненты СОИБ должны быть настроены на отправку событий по протоколу syslog в MP SIEM. Источниками событий для системы могут служить:

- операционные системы;
- системы управления базами данных;
- средства защиты информации;
- прикладное программное обеспечение;
- активное сетевое оборудование и т.п.

Процесс деятельности системы включает следующие автоматизированные и неавтоматизированные процедуры:

- источники событий, входящие в состав ИС формируют сообщения о событиях ИБ, происходящих в ИС.
- данные события ИБ передаются в систему, где происходит их нормализация (приведение к единому формату) и анализ.
- на основе анализа событий ИБ выявляются зависимости между ними. В случае, если установленные зависимости будут отнесены системой к разряду инцидентов, происходит формирование соответствующего сообщения и осуществляется информирование персонала (пользователей) MP SIEM.
- получив сообщение об инциденте персонал анализирует полученное сообщение и в случае необходимости принимает меры, направленные на устранение возникшего инцидента.
- после устранения возникшего инцидента и ликвидации его последствий осуществляется выявление причин возникновения инцидента.
- на основе знания о причинах возникновения инцидента разрабатывается комплекс мер, направленных на недопущение повторения ситуации, приведшей к возникновению инцидента.

Функциональные компоненты программных средств MP SIEM развернуты на физическом оборудовании, расположенном в ЦУС, расположенном по адресу г. Москва, ул. Нижняя Красносельская, д. 6.

6. Проверка информационной безопасности системы

6.1. Проверка конфигурации оборудования

Проверка конфигурации оборудования АС производится на этапе создания конфигурации контролируемого пункта.

Проверяются настройки описания магистрали обмена данными с вышестоящими системами.

В настройках магистрали должны быть указаны только сервера диспетчерских центров, участвующих в информационном обмене.

6.2. Проверка интерфейсов и сетевых настроек

Необходимо отключить порты съемных носителей (при наличии).

Необходимо закрыть все неиспользуемые порты Ethernet, оставив открытыми только порт для обмена данными по МЭК 60870-5-104, и порты, используемые для организации удаленного доступа и мониторинга.

6.3. Настройка удаленного доступа

При наличии удаленного доступа необходимо выполнить настройки защищенного доступа через web-интерфейс и SSH:

- произвести настройку пользователей, произвести настройку ограничения длительности сессии;
- отключить telnet.

6.4. Проверка сервисов операционной системы

Необходимо отключить неиспользуемые сервисы ОС, отключить rpc, portmap, tftp, IPv6.

При организации синхронизации по ntp, отключить ptpd2.

6.5. Конфигурация сетевого оборудования

Помимо выполнения требований информационной безопасности для всех объектов, информационная безопасность технологической вычислительной сети передачи на стороне РТП/РП/ТП обеспечивается следующими настройками:

- отключить свободные порты (shutdown);
- отключить telnet, настроить SSH, изменить management VLAN;
- настроить SNMP с аутентификацией для удалённого мониторинга и управления;
- настроить журнал событий, включив запись истории изменения конфигурации при доступе на устройство;
- разрешить прохождение только трафика системы телемеханики энергообъекта РТП/РП/ТП (при наличии технической возможности);
- включить функцию Port Security (фильтрация MAC-адреса отправителя) (при наличии технической возможности);
- обеспечить сегментирование сети с использованием протокола 802.1 Q (VLAN) (при наличии технической возможности).

6.6. Конфигурация серверов диспетчерских пунктов

Настоящим документом не рассматриваются мероприятия, выполняемые на серверах ДП.

На виртуальных магистралях обмена данными КП и ПУ должны быть указаны идентичные настройки протокола МЭК 60870-104.

6.7. Общие мероприятия

Проверку общих мероприятий, обеспечивающих информационную безопасность функционирования системы, выполняют одновременно с выполнением визуального осмотра технических средств, при проверке каналов передачи данных, а также при проведении специальных проверочных мероприятий.

При выполнении визуального осмотра проверяют:

- наличие пломб производителя или подрядных организаций на корпусах контроллеров и телекоммуникационных модулей;
- блокировку портов и устройств для подключения съемных носителей.

При проведении испытаний каналов передачи данных проверяют:

- изоляцию технологической сети от сетей общего пользования и обеспечение безопасности периметра сети;
- изоляцию трафика различных систем в технологической сети.

При проведении специальных проверочных мероприятий проверяют:

- разграничение доступа к файлам конфигурации;
- блокировку сервисов, не используемых для выполнения производственных задач.
- блокировку виртуальных портов, не используемых для выполнения производственных задач.

Проверке также подлежат следующие функции:

- разграничение уровней доступа к технологической информации и соответствие объема информации каждому уровню;
- разграничение прав пользователей на выполнение действий в системе;
- журналирование регистрации событий и авторизации пользователей в системе.

По итогам внедрения системы ИБ проводится комплексная проверка решения (системы АС и СрЗИ) на уязвимости (с актуальным Банком уязвимостей) и анализ защищенности с помощью специализированного сертифицированного программного обеспечения.

7. Мероприятия по подготовке к вводу в эксплуатацию

7.1. Подготовка объекта

Для проведения монтажа оборудования обеспечивается место в монтажных шкафах оборудованного помещения и доступ специалистов Исполнителя в это помещение в рабочее время.

К моменту начала развертывания системы силами Общества обеспечивается настройка телекоммуникационного оборудования и сетевой инфраструктуры.

Силами Общества до начала развертывания выполняются следующие мероприятия:

1. Проведена подготовка ИТ-инфраструктуры к модернизации:

- выделение портов;
- IP-адресов;
- настройка портов;
- согласование предполагаемой схемы включения СрЗИ СОИБ.

2. Определение настроек локальных и сетевых клиентских компонент СрЗИ СОИБ.
3. В серверных помещениях объектов по согласованию с Исполнителем должны быть выделены:

- соответствующее спецификации ТП свободное место в серверных шкафах, источники бесперебойного питания;
- физические/виртуальные серверы для установки средств управления СрЗИ.

4. Проведено резервирование системного и прикладного ПО серверов и рабочих станций, на которые предлагается установка компонентов СрЗИ.
5. Обеспечено сетевое взаимодействие между компонентами СОИБ.
6. Обеспечено прохождение сетевого трафика между компонентами внедряемых СрЗИ СОИБ.

7.2. Подготовка помещений

Силами Общества в срок до начала проведения пусконаладочных работ осуществлена подготовка помещений для размещения СОИБ.

Помещение считается подготовленным к выполнению работ, если выполнены следующие требования:

- отсутствует мебель и предметы, мешающие проведению работ;
- электропитание технических средств осуществляется от однофазной промышленной сети переменного тока напряжением 220 В частотой 50 Гц;
- обеспечено защитное заземление в соответствии с ГОСТ 25861–83. Провод защитного заземления должен присоединяться к контакту защитного заземлителя объекта. Сопротивление защитного заземлителя не должно превышать 4 Ом;
- технические средства запитаны от отдельных автоматических выключателей на щите электропитания объекта.

В состав организационных мероприятий, выполняемых на объекте силами Заказчика, входят:

- предоставление сведений, необходимых для развертывания системы;
- выделение технических специалистов на время развертывания и эксплуатации системы;
- определение согласовывающих лиц.

7.3. Ввод в эксплуатацию

На стадии ввода СОИБ в эксплуатацию осуществляются:

- предварительные испытания;
- опытная эксплуатация;
- приемочные испытания и передача в промышленную эксплуатацию СОИБ;

Ввод в действие СОИБ осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, и с учетом ГОСТ 34.601 после выполнения технического проектирования и разработки соответствующей рабочей документации СОИБ и после проведения

оценки соответствия принятых мер защиты.

7.4. Предварительные испытания

На стадии предварительных испытаний проводят:

- испытания СОИБ на работоспособность компонентов;
- устранение неисправностей в соответствии с протоколом испытаний;
- оформление акта о приемке СОИБ в опытную эксплуатацию.

Оформляемые документы подписываются членами комиссии по проведению предварительных испытаний и утверждаются Обществом.

7.5. Опытная эксплуатация

На стадии опытной эксплуатации проводят:

- опытную эксплуатацию СОИБ;
- анализ результатов опытной эксплуатации СОИБ;
- доработку (при необходимости) средств и систем СОИБ;
- оформление акта о завершении опытной эксплуатации.

Сроки проведения опытной эксплуатации оговариваются с Компанией.

7.6. Приемочные испытания

На стадии приемочных испытаний проводят:

- испытания на соответствие техническому заданию в соответствии с программой и методикой приемочных испытаний;
- анализ результатов испытания СОИБ и устранение недостатков, выявленных при испытаниях;
- оформление акта о приемке СОИБ в промышленную эксплуатацию.

8. Сведения о соответствии применяемого оборудования и программного обеспечения требованиям ФЗ

Применяемое оборудование и программное обеспечение соответствует требованиям п.8 ст.3 Федерального закона от 18.07.2011 №223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», п.2 постановления Правительства РФ от 16.11.2015 №1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

Аппаратное обеспечение СОИБ включено в единый реестр российской радиоэлектронной продукции:

- номер реестровой записи «Сервер доступа к данным TOPAZ IEC DAS» – 10251251;
- номер реестровой записи «ПАК ViPNet Coordinator IG 4, исполнение ViPNet Coordinator IG100 4 (аппаратная платформа IG100 I4)» – 10533945.

Программное обеспечение — Российского производства.

9. Перечень принятых сокращений

В настоящем документе приняты следующие сокращения.

Сокращение	Определение
АС	Автоматизированная система
АСУ	Автоматизированная система управления
АСУ ТП	Автоматизированная система управления технологическими процессами
ГОСТ	Государственный стандарт
ДП	Диспетчерский пункт
ЗП	Задание на проектирование
ИБ	Информационная безопасность
ИС	Информационная система
ИТ	Информационные технологии
КИИ	Критическая информационная инфраструктура
МСЭ	Межсетевое экранирование
МЭ	Межсетевой экран
Общество	Публичное акционерное общество «Россети Московский регион»
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПС	Подстанция электрическая
ПО	Программное обеспечение
РФ	Российская Федерация
САВЗ	Средство антивирусной защиты
СОИБ	Система обеспечения информационной безопасности
СКЗИ	Средство криптографической защиты информации
СрЗИ	Средства защиты информации
ТОС	Технологическая операционная система «TOPAZ LINUX»
ТМ	Телемеханика
ФСТЭК	Федеральная служба технического и экспортного контроля
ФСБ	Федеральная служба безопасности
MP SIEM	MaxPatrol SIEM

Таблица регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	Номер докум.	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных				

Взам. инв. №

Подпись и дата

Инв. № подл.

Позиция	Наименование и техническая характеристика	Тип, марка, обозначение документа, опросного листа	Код оборудования, изделия, материала	Завод-изготовитель Поставщик	Единица измерения	Количество	Масса единицы, кг	Примечания
1	2	3	4	5	6	7	8	9
	Оборудование ПС Мельниково.							
1.	**Шкаф информационной безопасности TOPAZ-ИБ.ПС Мельниково. в составе**	**TOPAZ-ИБ.ПС Мельниково**		ООО «ПиЭлСи Технолоджи»	**к-т.**	**1**		**Шкаф СОИБ**
1.1.	Шкаф напольный телекоммуникационный 42U (600x600x2000мм) с вентиляторным модулем. Передняя дверь – металл, задняя дверь – металл. Цоколь – 200 мм				шт.	1		
1.2.	Концевой выключатель двери с кронштейном				шт.	2		
1.3.	Панель заземления				шт.	1		
1.4.	Сетевой коммутатор TOPAZ SW528-4GTxSFP-24Tx-M-2LV-DGN-CS			ООО «ПиЭлСи Технолоджи»	шт.	2		
1.5.	Модуль ТС TOPAZ TM DIN16C-24-2Tx-2LV-Pr			ООО «ПиЭлСи Технолоджи»	шт.	1		
1.6.	Датчик температуры TOPAZ PSC DT				шт.	1		
1.7.	Клемма проходная четырёхполюсная, 2,5 кв.мм, синяя, серая жёлто-зелёная,				шт.	41		
1.8.	Клемма проходная четырёхполюсная, 4 кв.мм, синяя, серая жёлто-зелёная,				шт.	6		
1.9.	Выключатель автоматический, 6 кА, 2П, 6А, характеристика С, АС 400 В, с вспомогательным контактом (НЗ)				шт.	2		
1.10.	Выключатель автоматический, 6 кА, 2П, 25А, характеристика С, DC 60 В, с вспомогательным контактом (НЗ)				шт.	2		
1.11.	Розетка модульная с заземляющим контактом на DIN-рейку, 16 А, 250 В				шт.	2		
1.12.	Лампа светодиодная зелёная, АС 220 В				шт.	2		Врезается в наружную дверь
1.13.	Датчик контроля напряжения TOPAZ ADS-1				шт.	2		
1.14.	IT-светильник на светодиодах, 24 В				шт.	1		
1.15.	Модуль контроля питания TOPAZ PSC 24V40A			ООО «ПиЭлСи Технолоджи»	шт.	2		
1.16.	Блок питания TOPAZ PW220/24V480W-AC/DC-DGN				шт.	2		
1.17.	Аккумуляторный блок TOPAZ AU 40AH/24V				шт.	2		
1.18.	Кабельный органайзер				к-т.	1		Устанавливается по месту
1.19.	DIN рейка				м	3		Отрезается по месту

Взаим. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.	Лист	№док.	Подп.	Дата	6350-25-ИОС5.3-СО		
						Строительство ПС 220/20 кВ Мельниково		
Разраб.		Соловьев			08.25	Информационная безопасность	Стадия	Лист	Листов
Пров.		Булаев			08.25		П	1	4
Н. Контр.		Николаев			08.25	Спецификация оборудования, изделий и материалов	ООО «Интеллектуальные сети и системы»		
ГИП		Булаев			08.25				

Позиция	Наименование и техническая характеристика	Тип, марка, обозначение документа, опросного листа	Код оборудования, изделия, материала	Завод-изготовитель Поставщик	Единица измерения	Количество	Масса единицы, кг	Примечания
1	2	3	4	5	6	7	8	9
1.20.	**Комплект Системы централизованного обновления (СЦО) TOPAZ.SCR-512 в составе:**			**ООО «ПиЭлСи Технолоджи»**	**к-т.**	**1**		**Установка в шкаф СОИБ**
1.20.1.	Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (SCR) с СПО TOPAZ SCR				шт.	1		
1.20.2.	Сертифицированная технологическая операционная система (ТОС) TOPAZ LINUX с технической поддержкой уровня "Стандарт" на 1 год				шт.	1		
1.21.	**Комплект Системы обнаружения вторжений (СОВ) TOPAZ.IDS-04 в составе:**			**ООО «ПиЭлСи Технолоджи»**	**к-т.**	**1**		**Установка в шкаф СОИБ**
1.21.1.	Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (IDS-04) с СПО TOPAZ IDS-04				шт.	1		
1.21.2.	Средство обнаружения вторжений - Права на программу для ЭВМ. Право на использование Системы обнаружения вторжений СОВ «Кречет», с сертификатом активации сервиса совместной технической поддержки и установочным комплектом (Flash-накопитель)				шт.	1		
1.21.3.	Сертифицированная технологическая операционная система (ТОС) TOPAZ LINUX с сертифицированным установочным комплектом				шт.	1		
1.21.4.	Техническая поддержка «Сертифицированная технологическая операционная система (ТОС) TOPAZ LINUX» -8/5-12				шт.	1		
1.22.	**Комплект Системы контроля целостности и резервного копирования (СКЦРК) TOPAZ.ICB-FW-512 в составе:**			**ООО «ПиЭлСи Технолоджи»**	**к-т.**	**1**		**Установка в шкаф СОИБ**
1.22.1.	Сервер доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (ICB) с СПО TOPAZ ICB				шт.	1		
1.22.2.	Сертифицированная технологическая операционная система (ТОС) TOPAZ LINUX с сертифицированным установочным комплектом				шт.	1		
1.22.3.	Техническая поддержка «Сертифицированная технологическая операционная система (ТОС) TOPAZ LINUX» -8/5-12				шт.	1		
1.23.	**Сервер доступа к данным для установки Kaspersky Industrial CyberSecurity for Networks: TOPAZ IEC DAS MX683 E6R4 3.8GHz (ECX-1210A)/ DVI-DP/1HDD1T/2SATA/64Gb/1SSD1T/2mSATA1T/RKIT/4GTx/LV**				**шт.**	**1**		**Установка в шкаф СОИБ**
1.24.	**ПАК ViPNet Coordinator IG100 4.x (Utun) I4 (с Сертификатом активации сервиса совместной технической поддержки ПАК ViPNet Coordinator IG100 4.x (Utun) I4 на срок 1 год, уровень - Стандартный**			**ООО «Инфотекс»**	**шт.**	**2**		**Установка в шкаф СОИБ**
1.25.	Патч-корд rj-45 – rj-45, UTP 5e, 4x2x0,52, 1,5м				шт.	11		**в шкаф СОИБ**

Позиция	Наименование и техническая характеристика	Тип, марка, обозначение документа, опросного листа	Код оборудования, изделия, материала	Завод-изготовитель Поставщик	Единица измерения	Количество	Масса единицы, кг	Примечания
1	2	3	4	5	6	7	8	9
2.	**АРМ ИБ MSI Modern 15 F13MG (9S7-15S122-605)**				**шт.**	**1**		**АРМ ИБ**
3.	**Программное обеспечение**							
3.1.	Промышленный антивирус (ФСТЭК), включая техническую поддержку на 1 год, Kaspersky Industrial CyberSecurity for Linux Nodes, Workstation, Enterprise Russian Edition 1 - Node 1 year Base License			Лаборатория Касперского	шт.	1		АРМ ИБ
3.2.	Промышленный антивирус (ФСТЭК), включая техническую поддержку на 1 год, Kaspersky Industrial CyberSecurity for Linux Nodes, Server, Enterprise Russian Edition 1 - Node 1 year Base License			Лаборатория Касперского	шт.	1		Сервер ИБ (1.23)
3.3.	ПО для резервного копирования и восстановления данных для рабочей станции (ФСТЭК) с технической поддержкой на 1 год, Кибер Бэкап Расширенная редакция для рабочей станции Linux, ФСТЭК			Киберпротект	шт.	1		АРМ ИБ
3.4.	Сертификат на техническую поддержку ПО Кибер Бэкап Расширенная редакция для рабочей станции Linux, ФСТЭК			Киберпротект	шт.	1		АРМ ИБ
3.5.	Базовый пакет для сертифицированной версии программного комплекса Кибер Бэкап Расширенная редакция для рабочей станции, ФСТЭК			Киберпротект	шт.	1		АРМ ИБ
3.6.	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи BOX, серверная до 2 сокетов или 1 виртуальный сервер, на срок действия исключительного права, с включенными обновлениями Тип 1 на 12 мес.			АНПО РусБИТех	шт.	1		Сервер ИБ (1.23)
3.7.	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи BOX, для рабочей станции, на срок действия исключительного права, с включенными обновлениями Тип 1 на 12 мес.			АНПО РусБИТех	шт.	1		АРМ ИБ
3.8.	Kaspersky Industrial CyberSecurity for Networks Standard Server Russian Edition			Лаборатория Касперского	шт.	1		Сервер ИБ (1.23)
	Кабели и материалы							
4.	Кабель для информационных сетей, экранированный	FTP 5e 4x2x0,52			м	150		
5.	Кабель ВВГнг-LS 3x2,5	ВВГнг-LS 3x2,5			м	150		

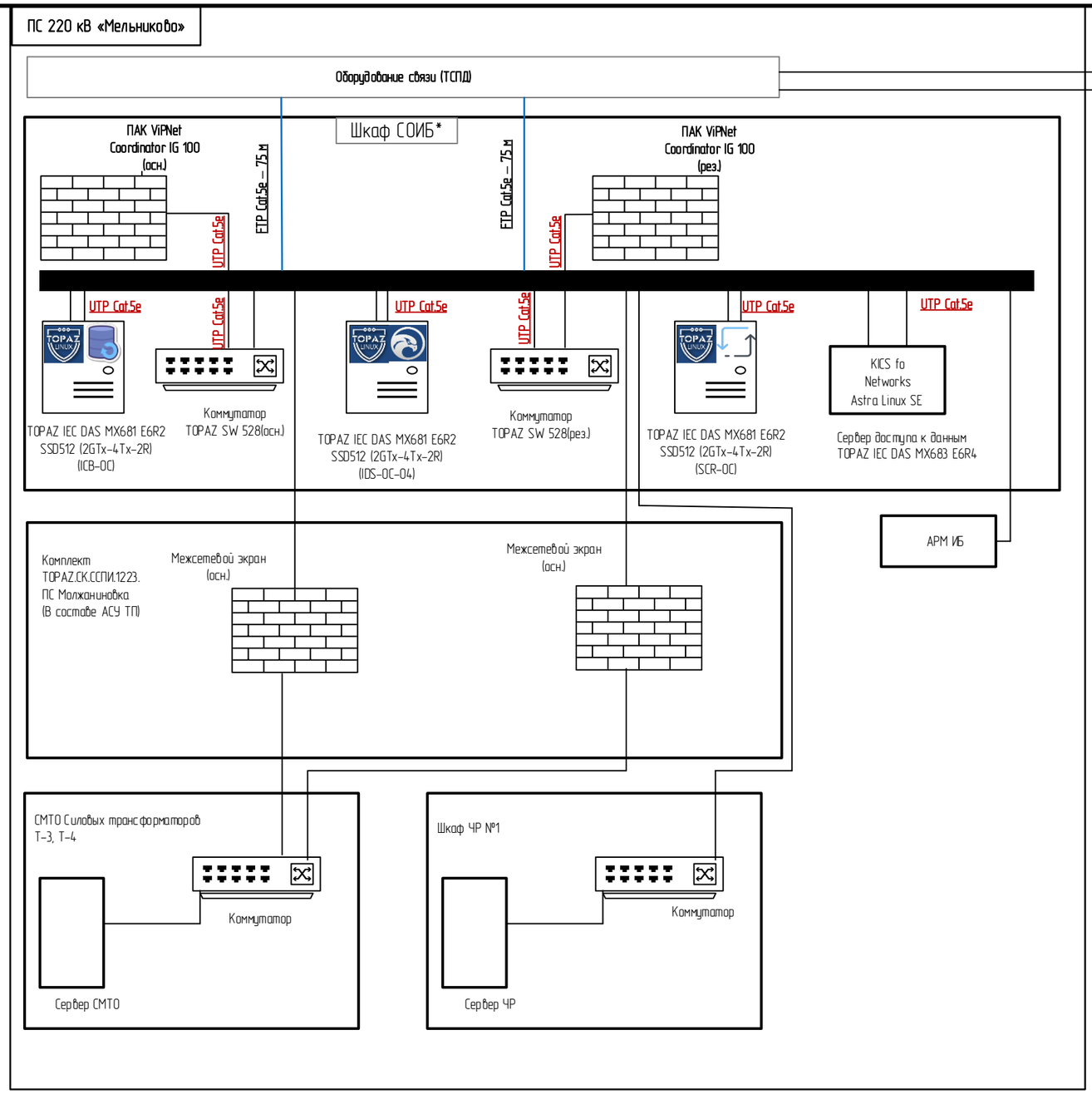
Взаим. инв. №

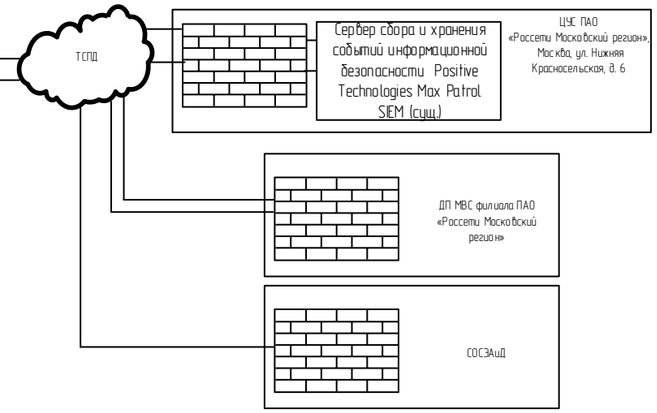
Подп. и дата

Инв. № подл.

Позиция	Наименование и техническая характеристика	Тип, марка, обозначение документа, опросного листа	Код оборудования, изделия, материала	Завод-изготовитель Поставщик	Единица измерения	Количество	Масса единицы, кг	Примечания
1	2	3	4	5	6	7	8	9
6.	Коннектор RJ45 для витой пары разъём RJ-45 штекер TP-8P8C				шт.	4		
7.	Провод ПуГВнг(А)-LS для заземления	ПуГВнг(А)-LS 1х6			м	10		

№ строки	Наименование вида работ	Ед. изм.	Коли-чество	Примечание
	Монтажные работы			
1	Монтаж шкафа информационной безопасности TOPAZ-ИБ.ПС Мельниково в помещении ЩУ ПС Мельниково	шт.	1	
2	Прокладка кабеля FTP 5e 4x2x0,52 по установленным конструкциям	м	150	
3	Прокладка кабеля силового ВВГнг-LS 3x2,5 в проложенных трубах, блоках и коробах в здании ПС Мельниково	м	150	
4	Монтаж кабеля заземления ПуГВнг(А)- LS 1x6мм^2	м	10	
5	Монтаж коннекторов RJ-45 на концах кабеля FTP 5e 4x2x0,52	шт.	4	
	Пусконаладочные работы			
6	Настройка сетевого коммутатора TOPAZ SW528-4GTxSFP-24Tx-M-2LV-DGN-CS	шт.	2	
7	Настройка сервера доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (IDS-04)	шт.	1	
8	Настройка сервера доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (ICB)	шт.	1	
9	Настройка сервера доступа к данным TOPAZ IEC DAS MX681 E6R2 SSD512 (2GTx-4Tx-2R) (SCR)	шт.	1	
10	Настройка сервера доступа к данным для установки Kaspersky Industrial CyberSecurity for Networks TOPAZ IEC DAS MX683 E6R4	шт.	1	
11	Настройка ПАК ViPNet Coordinator IG100 4.x (Utun) I4	шт.	2	
12	Настройка основных сетевых трактов между сетевыми элементами сети ИБ	шт.	5	
13	Настройка резервных сетевых трактов между сетевыми элементами сети ИБ	шт.	5	
14	Установка операционной системы специального назначения «Astra Linux Special Edition» на сетевой элемент сети ИБ	шт.	2	
15	Контрольные приёмо-сдаточные испытания системы ИБ ПС Мельниково	объект	1	





Пояснения

На уровне ПС СОИБ реализуется следующим составом подсистем: защиты каналов связи и МСЭ, идентификации и аутентификации, управления доступом, регистрации событий безопасности, обеспечения целостности, обнаружения вторжений, резервного копирования и восстановления информации, централизованного обновления ПО. В составе*:

- ПАК ViPNet Coordinator IG 100 4.x (Utun) I4;
- Комплект Системы обнаружения вторжений (СОВ) TOPAZ.IDS-OC-04;
- Комплект Системы централизованного обновления (СЦО) TOPAZ.SCR-OC-512;
- Комплект Системы контроля целостности и резервного копирования (СКЦРК) TOPAZ.ICB-FW-OC-512;
- Сервер доступа к данным TOPAZ IEC DAS MX683 E6R4 с установленным ПО KICS fo Networks

Сертифицированная технологическая операционная система (ТОС) «TOPAZ LINUX»	**ПС** – подстанция электрическая
Межсетевое экранирование в составе сертифицированной ТОС	**ПП** – переходной пункт
Сертифицированное ПО СКЗИ	**ПАК** – программно-аппаратный комплекс
Сертифицированный комплект системы обнаружения вторжений (СОВ) TOPAZ.IDS-OC-04	**СОВ** – система обнаружения вторжений
Комплект Системы централизованного обновления (СЦО) TOPAZ.SCR-OC-512	**СЦО** – система централизованного обновления
Комплект Системы контроля целостности и резервного копирования (СКЦРК) TOPAZ.ICB-FW-OC-512	**СЦРК** – система контроля целостности и резервного копирования
Пограничные МСЭ/СКЗИ ПС, АСУ ТП	**СКЗИ** – Средство криптографической защиты информации
	МСЭ – Межсетевое экранирование

Взам. инв. №

Подпись и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№ док	Подпись	Дата
Разработал		Соловьев			08.25
Проверил		Булаев			08.25
Н. Контроль		Николаев			08.25

6350-25-ИОС5.3-ГЧ.1

Строительство ПС 220/20 кВ Мельниково

Информационная безопасность

Стадия	Лист	Листов
П	-	1

Схема структурная системы обеспечения информационной безопасности

ООО «Интеллектуальные сети и системы»

Приложение 1 к тому проектной документации

6350-25-ИОС5.3

МОДЕЛЬ УГРОЗ

МОДЕЛЬ НАРУШИТЕЛЯ И МОДЕЛЬ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ТИПОВАЯ МОДЕЛЬ УГУРОЗ

г. Москва 2025

Содержание

1. Общие положения ... 3
1.1. Назначение и область действия ... 3
1.2. Источники разработки ... 4
1.3. Обладатель информационной (автоматизированной) системы ... 5
1.4. Данные о разработчике модели угроз ... 5
1.5. Методика оценки угроз ... 6
2. Описание систем и сетей и их характеристика как объектов защиты ... 8
2.1. Наименование объекта защиты ... 8
2.2. Классификация объекта защиты ... 8
2.3. Разработка объекта защиты ... 8
2.4. Назначение объекта защиты ... 10
2.5. Бизнес-процессы на объекте защиты ... 10
2.6. Характеристики объекта защиты ... 11
2.7. Пользователи объекта защиты ... 12
2.8. Внешние интерфейсы ... 13
2.9. Дополнительные сведения ... 13
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации ... 15
3.1. Виды рисков ... 15
3.2. Негативные последствия ... 16
4. Возможные объекты воздействия угроз безопасности информации ... 17
4.1. Компоненты объекта защиты ... 17
4.2. Виды воздействия ... 17
5. Источники угроз безопасности информации (модель нарушителя) ... 18
5.1. Характеристика нарушителя ... 18
5.2. Актуализация нарушителя ... 19
5.3. Возможности актуального нарушителя ... 23
6. Способы реализации (возникновения) угроз безопасности информации ... 24
6.1. Возникновение и реализация угроз ... 24
6.2. Реализация нарушителем угроз безопасности информации через доступ к интерфейсам воздействия ... 24
7. Актуальные угрозы безопасности информации ... 25
7.1. Моделирование угроз безопасности информации ... 25
7.2. Возможные сценарии реализации угроз безопасности информации ... 37
7.3. Перечень актуальных угроз ... 42
8. Принятые термины, определения и сокращения ... 44

1. Общие положения

1.1. Назначение и область действия

Настоящая модель угроз безопасности информации (далее — МУ) рассматривает угрозы безопасности информации ПС 220 кВ Мельниково

Объектом защиты является комплекс автоматизированных систем (далее — АС) ПС 220 кВ Мельниково.

Настоящая МУ содержит описание угроз безопасности данных при их обработке на объекте защиты.

Моделирование угроз безопасности информации (далее — УБИ) включает в себя выявление и описание угроз несанкционированного, в том числе случайного, доступа (далее — НСД) к данным при их обработке в АС.

УБИ могут стать неправомерные действия с информацией и используемыми для обработки информации технологиями:

- несанкционированные уничтожение, изменение, блокирование, копирование, предоставление, распространение обрабатываемой информации;
- нарушение конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации;
- нарушение корректной работы средств обработки и защиты информации, ведущие к нарушению или прекращению функционирования АС.

Угрозы, рассматриваемые в МУ, обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, создающими условия для нарушения безопасности данных.

в системах и сетях.

МУ является методическим документом, предназначенным для ответственных лиц филиалов Общества, которые организуют и (или) осуществляют защиту информации в АС.

Содержащиеся в настоящей МУ угрозы безопасности данных, обрабатываемых в АС, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств их реализации в информационных системах (далее — ИС).

Анализ и моделирование угроз проведены для получения качественной и количественной оценки реальных угроз, актуальных для АС.

Основными задачами, решаемыми в ходе оценки угроз безопасности информации, являются:

- определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
- инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
- определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
- оценка способов реализации (возникновения) угроз безопасности информации;
- оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
- оценка сценариев реализации угроз безопасности информации.

При разработке МУ в качестве основополагающих использовались нормативные документы Федеральной службы безопасности (далее — ФСБ) и Федеральной службы технического и экспортного контроля (далее — ФСТЭК) Российской Федерации, определяющие подходы к безопасности информации.

Построение МУ основывалось на классификации, анализе и оценке актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой информации, несанкционированными и непреднамеренными воздействиями на информацию и на оборудование, осуществляющее ее обработку.

В ходе моделирования идентифицированы возможные источники угроз, возможные уязвимости идентифицированы и сопоставлены с идентифицированными источниками угроз, идентифицированные источники угроз и уязвимости сопоставлены со способами их реализации.

Определение перечня технических угроз и нарушителей информационной безопасности (далее — ИБ), которые являются актуальными для АС, может послужить основой для проведения мероприятий по проектированию и внедрению системы обеспечения ИБ (далее — СОИБ) для АС.

Пересмотр и изменение МУ осуществляется в случаях:

- изменения требований нормативных правовых актов Российской Федерации и методических документов ФСТЭК, регламентирующих вопросы оценки угроз безопасности информации;
- изменения архитектуры и условий функционирования АС, режима обработки информации и правового режима информации на объекте защиты, влияющих на угрозы безопасности информации;
- выявления новых УБИ или новых сценариев реализации существующих угроз, в том числе по результатам контроля уровня защищенности АС;
- включения в банк данных УБИ ФСТЭК сведений о новых угрозах безопасности информации, сценариях (тактиках, техниках) их реализации.

Разработка МУ предусматривает ее применение к нескольким однотипным объектам защиты.

Внесение изменений в МУ осуществляется по указанию генерального директора Общества в установленном порядке.

1.2. Источники разработки

Для оценки УБИ и разработки МУ были использованы следующие нормативные правовые акты, методические документы и национальные стандарты.

Источниками разработки стали:

1. Федеральное законодательство:

- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Федеральный закон от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

2. Указы президента РФ:

- Указ Президента РФ от 22.05.2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации»;
- Указ Президента РФ от 06.031997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

3. Постановления Правительства:

- Постановление Правительства РФ от 08.02.2018 г № 127-ПП «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».

4. Приказы ФСТЭК:

- Приказ ФСТЭК от 14.03.2014 г. № 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»;
- Приказ ФСТЭК от 21.12.2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5. Приказы Министерства энергетики:

- Приказ Министерства энергетики от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и

последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования».

6. Государственные стандарты:

— ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
— ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
— ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»;
— ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие требования».

7. Методические документы:

— Методика оценки угроз безопасности информации (утв. ФСТЭК 05.02.2021 г.);
— Выписка из Требований по безопасности информации, утвержденных приказом ФСТЭК России от 30 июля 2018 г. № 131 (от 30.07.2018).

8. Информационные сообщения:

— Информационное сообщение ФСТЭК России от 29 марта 2019 г. № 240/24/1525 О требованиях по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий;
— Информационное сообщение ФСТЭК России от 9 апреля 2020 г. № 240/22/1534 о разработке методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах».

9. Информационные ресурсы:

— http://bdu.fstec.ru.

1.3. Обладатель информационной (автоматизированной) системы

Владелец ИС — ПАО «Россети Московский Регион».
Статус организации: владелец объектов защиты.
Сфера функционирования: энергетика (электроэнергетика).
Объекты защиты: АС.

Подразделения и должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей, определяются внутренними нормативными документами Общества.

1.4. Данные о разработчике модели угроз

1.4.1. Состав экспертной группы

Для оценки УБИ по решению Общества, в соответствии с законодательством Российской Федерации, были привлечены специалисты сторонней организации.

С целью снижения субъективных факторов при оценке угроз безопасности информации было проведено формирование экспертной группы. В связи с особенностями функционирования АС и привлечением к моделированию угроз специалистов компании согласно пункту 1.3.1 МУ, определен следующий состав экспертной группы:

1. Руководитель отдела специальных проектов и технической защиты информации, председатель экспертной группы.
2. Руководитель отдела телекоммуникаций и связи.
3. Руководитель отдела управления проектами.

Для оценки УБИ, в соответствии с рекомендациями ФСТЭК, привлеченные специалисты обладают следующими знаниями и умениями:

— основ оценки рисков, а также основных рисков от нарушения функционирования систем и сетей и нарушения безопасности обрабатываемой информации;

- УБИ и способов их реализации (возникновения);
- тактик и техник проведения компьютерных атак (реализации угроз безопасности информации);
- основных типов компьютерных инцидентов и причин их возникновения;
- основных уязвимостей систем и сетей;
- нормативных правовых актов по созданию и функционированию
- систем и сетей, защите информации (обеспечению безопасности) в них, основных (критических) процессов (бизнес-процессов) обладателя информации и (или) оператора;
- оценивать информационные риски;
- классифицировать и оценивать угрозы безопасности информации;
- определять сценарии (тактики, техники) реализации УБИ;
- определять источники и причины возникновения компьютерных инцидентов;
- проводить инвентаризацию систем и сетей, анализ уязвимостей, тестирование на проникновение систем и сетей с использованием соответствующих автоматизированных средств;
- оценку уровня защищенности (аудит) систем и сетей и содержащейся в них информации.

Эксперты обладают независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения.

В состав экспертной группы входит 3 (три) эксперта.

При проведении экспертной оценки принимаются меры, направленные на снижение уровня субъективности и неопределенности при определении каждой из угроз безопасности информации.

Экспертная оценка проводится в отношении следующих параметров:

- негативного последствия от реализации УБИ;
- целей нарушителей по реализации УБИ;
- сценария действий нарушителей при реализации УБИ.

Решения, принимаемые экспертами при оценке УБИ, исходят из принципа «гарантированности», при котором заведомо обусловлено, что нарушитель находится в наилучших условиях для реализации УБИ.

1.4.2. Сведения о наличии лицензий

Лицензии компании ООО «Интеллектуальные сети и системы» описаны в документации (приложения) к проекту с децимальным номером 6350-25-ИОС5.3.

1.5. Методика оценки угроз

По результатам анализа исходных данных, оценки нарушителей ИБ и УБИ выявляются актуальные УБИ, реализация (возникновение) которых может привести к нарушению безопасности информации. Результаты оценки УБИ направлены на оценку эффективности принятых технических мер, в том числе используемых средств защиты информации (далее — СрЗИ).

Результаты оценки УБИ отражаются в МУ. На основании Методики оценки УБИ, утвержденной ФСТЭК 5 февраля 2021 года (далее — Методика), была определена схема проведения оценки угроз (рисунок 1).

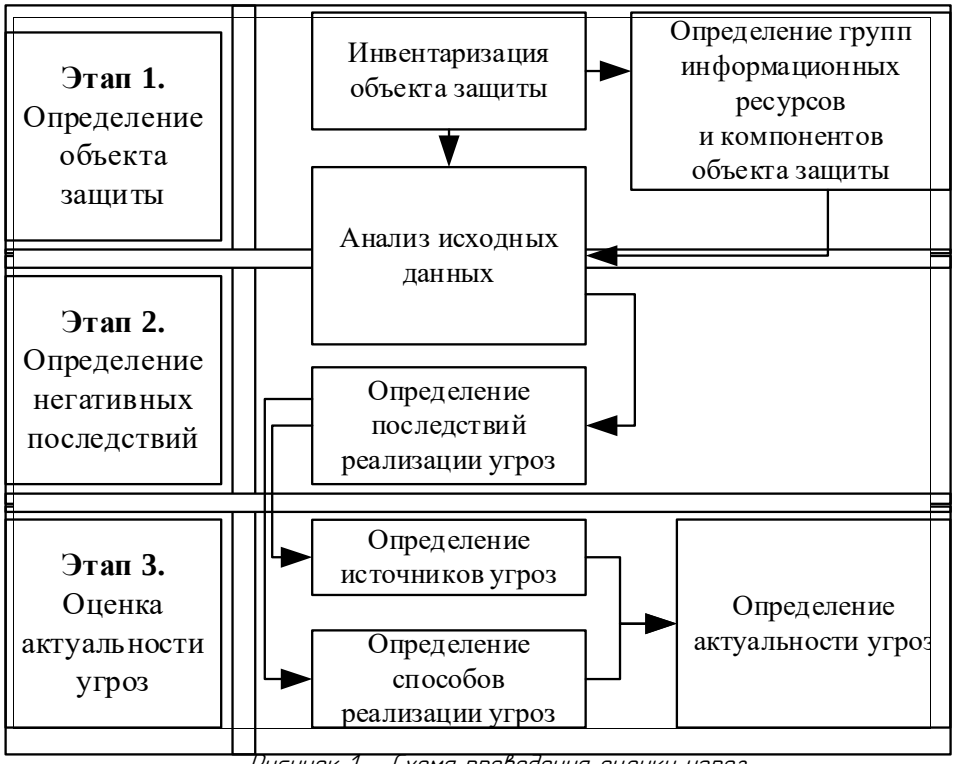


Рисунок 1 – Схема проведения оценки угроз

Для указанных в настоящей МУ информационных ресурсов и компонентов объекта защиты определены виды воздействия, которые могут привести к негативным последствиям.

Для реализации процессов, необходимых при моделировании УБИ, сформирована экспертная группа.

Указанные исходные данные уточняются и дополняться с учетом сферы функционирования объекта защиты.

2. Описание систем и сетей и их характеристика как объектов защиты

2.1. Наименование объекта защиты

Полное наименование объекта защиты: комплекс телемеханики ПС 220 кВ Мельниково.
Принятое сокращение: АС.

2.2. Классификация объекта защиты

АС предварительно присвоены:

- **3 (третья) категория значимости объекта критической информационной инфраструктуры**, согласно Постановлению Правительства Российской Федерации от 8 февраля 2018 г. № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской федерации и их значений»;
- **3 (третий) класс защищенности**, согласно Требованиям 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, утвержденным Приказом ФСТЭК от 14 марта 2014 г.

2.3. Разработка объекта защиты

АС создается и функционирует в соответствии со следующими нормативными правовыми актами:

- ГОСТ 12.1.003-2014. Система стандартов безопасности труда. Шум. Общие требования безопасности;
- ГОСТ 12.1.030-81. Система стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление;
- ГОСТ 12.2.003-91. Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности;
- ГОСТ 12.2.007.0-75. Система стандартов безопасности труда. Изделия электротехнические. Общие требования безопасности;
- ГОСТ 12.2.091-2012. Безопасность электрического оборудования для измерения, управления и лабораторного применения. Часть 1. Общие требования;
- ГОСТ 24.701-86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения;
- ГОСТ 34.201-2020 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;
- ГОСТ 1983-2015. Трансформаторы напряжения. Общие технические условия;
- ГОСТ 6651-2009. Государственная система обеспечения единства измерений. Термопреобразователи сопротивления из платины, меди и никеля. Общие технические требования и методы испытаний;
- ГОСТ 7746-2015. Трансформаторы тока. Общие технические условия;
- ГОСТ 14254-2015. Степени защиты, обеспечиваемые оболочками (Код IP);
- ГОСТ 15543.1-89. Изделия электротехнические. Общие требования в части стойкости к климатическим внешним воздействующим факторам;
- ГОСТ 30631-99. Общие требования к машинам, приборам и другим техническим изделиям в части стойкости к механическим внешним воздействующим факторам при эксплуатации;
- ГОСТ 30804.3.2-2013. Совместимость технических средств электромагнитная. Эмиссия гармонических составляющих тока техническими средствами с потребляемым током не более 16 А (в одной фазе). Нормы и методы испытаний;
- ГОСТ 30805.22-2013. Совместимость технических средств электромагнитная. Оборудование информационных технологий. Радиопомехи индустриальные. Нормы и методы измерений;
- ГОСТ 31565-2012. Кабельные изделия. Требования пожарной безопасности;
- ГОСТ Р 2.105-2019. Единая система конструкторской документации. Общие требования к текстовым документам;

- ГОСТ Р 2.601-2019. Единая система конструкторской документации. Эксплуатационные документы;
- ГОСТ Р 8.596-2002. Государственная система обеспечения единства измерений. Метрологическое обеспечение измерительных систем. Основные положения;
- ГОСТ Р 21.101-2020. Система проектной документации для строительства (СПДС). Основные требования к проектной и рабочей документации;
- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
- ГОСТ Р 51317.6.5-2006. Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых на электростанциях и подстанциях. Требования и методы испытаний;
- ГОСТ Р 51318.11-2006. Совместимость технических средств электромагнитная. Промышленные, научные, медицинские и бытовые (ПНМБ) высокочастотные устройства. Радиопомехи индустриальные. Нормы и методы измерений;
- ГОСТ Р 51321.1-2007 (МЭК 60439-1:2004). Устройства комплектные низковольтные распределения и управления. Часть 1. Устройства, испытанные полностью или частично. Общие технические требования и методы испытаний;
- ГОСТ Р 52931-2008. Приборы контроля и регулирования технологических процессов. Общие технические условия;
- ГОСТ Р 56498-2015/IEC/PAS 62443-3:2008. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления;
- ГОСТ IEC 60950-1-2014. Оборудование информационных технологий. Требования безопасности. Часть 1. Общие требования;
- ГОСТ IEC 60870-4-2011. Устройства и системы телемеханики. Часть 4. Технические требования;
- Действующая редакция Федерального закона от 22.07.2008 №123-ФЗ «Технический регламент о требованиях пожарной безопасности»;
- СТО 34.01-6-005-2019. «Коммутаторы энергообъектов. Общие технические требования»;
- СТО 34.01-6.1-002-2016. «Программно-технические комплексы подстанций 35-110 (150) кВ. Общие технические требования»;
- СТО 34.01-21-004-2019. «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ»;
- СТО 34.01-21-005-2019. «Цифровая электрическая сеть. Требования проектированию цифровых распределительных электрических сетей 0,4-220кВ»;
- СТО 56947007-25.040.40.226-2016. Стандарт организации ПАО «ФСК ЕЭС» «Общие технические требования к АСУТП ПС ЕНЭС. Основные требования к программно-техническим средствам и комплексам»;
- СТО 56947007-29.240.01.244-2017. Нормы точности измерений режимных и технологических параметров, измеряемых на объектах ПАО "ФСК ЕЭС". Методические указания по определению метрологических характеристик измерительных каналов и комплексов;
- СТО 56947007-29.240.10.167-2014. «Информационно-технологическая инфраструктура подстанций. Типовые технические решения»;
- СТО 56947007-29.240.10.303-2020. Стандарт организации ПАО «ФСК ЕЭС» «Методические указания по реализации мониторинга работоспособности измерительной части терминалов РЗА, АСУ ТП и других средств измерений вторичных цепей средствами АСУ ТП на объектах ПАО «ФСК ЕЭС»;
- СТО 56947007-29.240.10.248-2017. Стандарт организации ПАО «ФСК ЕЭС» «Нормы технологического проектирования ПС переменного тока с высшим напряжением 35-750 кВ»;
- СТО 56947007-29.240.043-2010. «Руководство по обеспечению электромагнитной совместимости вторичного оборудования и систем связи электросетевых объектов»;
- СТО 56947007-29.240.044-2010. Стандарт организации ПАО «ФСК ЕЭС» «Методические указания по обеспечению электромагнитной совместимости на объектах электросетевого хозяйства»;
- СО 153-34.20.501-03. Правила технической эксплуатации электрических станций и сетей Российской Федерации;
- СНиП 12-03-2001. Безопасность труда в строительстве. Часть 1. Общие требования;

— Постановление Правительства Российской Федерации в ред. от 15.07.2021г. №87 «О составе разделов проектной документации и требованиях к их содержанию»;
— Действующая редакция «Правила устройства электроустановок» (ПУЭ);
— «Правила разработки и применения графиков аварийного ограничения режима потребления электрической энергии (мощности) и использования противоаварийной автоматики», утвержденные приказом Министерства энергетики РФ от 06.06.2013 №290.

2.4. Назначение объекта защиты

АС представляет собой систему, использующуюся для реализации следующих функций на энергообъектах:

— автоматизированный контроль и управление режимами электроснабжения;
— автоматизированный контроль и управление режимами работы электрооборудования;
— централизованный контроль и мониторинг за состоянием технологического оборудования и режимами электроснабжения;
— оперативное диспетчерское управление схемой электроснабжения;
— регистрация нормальных и аварийных событий и процессов;
— контроль электропотребления;
— диагностика состояния основного оборудования, аппаратуры управления и каналов связи и т.д.

Наличие системы телеизмерений и передачи в режиме реального времени телеинформации о текущем режиме работы электроустановок обеспечивает быстрое выявление предаварийных и аварийных ситуаций в электроснабжении и является обязательным условием его безопасной эксплуатации.

Источниками информации для АС являются следующие информационно-технологические системы:

— релейная защита и автоматика;
— противоаварийная автоматика;
— комплекс средств связи;
— комплекс систем технических средств безопасности (КСТСБ) (пожарная и охранная сигнализация зданий, охранная сигнализация периметра, контроль и управление доступом).

Средствами АС в диспетчерские пункты (далее — ДП) и Региональное диспетчерское управление (далее — РДУ) готовится и передается технологическая информация, которая обеспечивает решение задач диспетчерско-технологического и производственно-технического управления электрическими сетями:

— информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная-выходная информация);
— управляющая (командная) информация;
— контрольно-измерительная информация;
— критически важная (технологическая) информация.

Информация, обрабатываемая в рамках АС, относится информации с ограниченным правовым доступом: доступом к данным обладает только владелец АС, данные передаются в рамках реализации функционала АС.

2.5. Бизнес-процессы на объекте защиты

В Обществе определены следующие бизнес-процессы:

— основные – обеспечение работоспособности сетей электроснабжения, производство электрической энергии, технологическое присоединение к распределительным электросетям, обеспечение работы распределяющей системы, продажа электроэнергии пользователю;
— обеспечивающие бизнес-процессы – ИТ-обеспечение и связь, юридическое обеспечение, административно-хозяйственное обеспечение, внутренний контроль, управление делопроизводством и документооборотом, управление рисками, бухгалтерский учет и отчетность, налоговый учет и отчетность, формирование отчетности;

— управляющие бизнес-процессы — стратегическое управление, управление финансами, управление персоналом и организационной структурой.

Среди указанных процессов к критическим относятся основные.

С целью обеспечения основных (критических) процессов была создана в том числе АС, как система автоматизированного контроля и управления режимами электроснабже и режимами работы электрооборудования. В рамках работы АС реализуется следующий бизнес-процесс: обеспечение работоспособности сетей электроснабжения.

Корреляция между функционалом объекта защиты, обрабатываемой им информацией и бизнес-процессами описана в таблице 1.

Таблица 1 - Функционал, обрабатываемая информация и бизнес-процессы

№	Функционал защищаемого объекта	Бизнес-процессы	Состав обрабатываемой информации
1.	технологическое управление оборудованием	обеспечение работоспособности сетей электроснабжения	— командная информация; — технологическая информация.
2.	мониторинг технического состояния электрической сети	обеспечение работоспособности сетей электроснабжения	— входная-выходная информация; — технологическая информация.
3.	передача телеизмерений в ДП и РДУ с подстанции	обеспечение работоспособности сетей электроснабжения	— контрольно-измерительная информация; — технологическая информация.
4.	передача телесигнализации состояния оборудования электросетевых объектов в ДП и РДУ с подстанции	обеспечение работоспособности сетей электроснабжения	— контрольно-измерительная информация; — технологическая информация.
5.	передача сигналов аварийно-предупредительной сигнализации в ДП и РДУ	обеспечение работоспособности сетей электроснабжения	— входная-выходная информация; — командная информация; — контрольно-измерительная информация; — технологическая информация.

2.6. Характеристики объекта защиты

АС представляет собой систему, выполненную на базе микропроцессорного программно-технического комплекса (далее — ПТК) «TOPAZ» производства ООО «ПиЭлСи Технолоджи».

АСУ ТП имеет многоуровневую структуру:

— уровень операторского управления (верхний уровень)

— уровень автоматического управления (средний уровень)

— уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень).

В АСУ ТП уровня ПС объектами защиты являются:

— информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса, управляющая (командная) информация, контрольно-измерительная информация и иная критически важная (технологическая) информация, нарушение безопасности которой оказывает влияние на технологические процессы;

— ПТК, включающий технические средства (в том числе телекоммуникационное оборудование, каналы связи, ПЛК, исполнительные устройства), программное обеспечение (далее — ПО) (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации;

— оборудование и ПО, выполняющее непосредственные функции управления технологическим процессом и наблюдения (контроля) за технологическим процессом;

— телекоммуникационное оборудование, линии, каналы и сети связи, обеспечивающие связность уровней управления;

— оборудование, ПО и системы, входящие в состав информационной инфраструктуры, обеспечивающей работоспособность системы АСУ ТП и взаимодействие с внешними сетями и системами;

— процессы технологического управления;

— процессы информационной и физической безопасности.

Нижний уровень представляет собой комплекты оборудования АСУ ТП, устанавливаемые на ПС и переходных пунктах (далее- ПП), включая устройства релейной защиты и автоматики (далее — РЗА), которые осуществляют передачу телеинформации в объеме, получаемом с уровня телемеханики.

Второй уровень системы ТМ представляет собой коммутаторы, а также серверы доступа к данным (контроллеры) с функциями шлюза безопасности, который осуществляет обмен данными между устройствами телемеханики и телесигнализации на уровне ПС и ДП с другой стороны по каналам связи.

Уровень диспетчерского управления реализуется оборудованием уровня ДП.

Для передачи телеинформации с подстанций на ДП используются каналы связи GPRS.

Состав объекта защиты показан в таблице 2.

Оборудование скомпоновано в запираемые шкафы. Описание интерфейсов АСУ ТП и устанавливаемое на оборудование общесистемное и прикладное ПО представлены в части «4 ОБЪЕКТЫ ВОЗДЕЙСТВИЯ» настоящей МУ.

Рассматривая АСУ ТП как объект защиты, к компонентам АСУ ТП в том числе рассматриваются интерфейсы. Интерфейс это:

- согласно ГОСТ Р 52872-2012 — «совокупность правил взаимодействия устройств и программ между собой или с пользователем и средств, реализующих это взаимодействие»;
- согласно Р 50.1.041-2002 — «общая граница между двумя функциональными объектами, требования к которой определяются стандартом».

Интерфейсы включают в себя:

- аппаратные и программные средства, связывающие различные устройства или программы между собой или с пользователем;
  правила и алгоритмы, на основе которых эти средства созданы

Таблица 2 - Характеристика объекта защиты

№	Характеристика	ПС 220 кВ Мельниково	Переходной пункт
Уровни и классы защищенности			
1.	Категория значимости	3	3
2.	Класс защищенности	3	3
Состав и архитектура. Вид и тип			
3.	Вид объекта защиты	Подстанция электрическая	Переходной пункт
4.	Тип объекта защиты	Автоматизированная система управления (комплекс телемеханики)	
5.	Тип сети объекта защиты	Технологическая сеть	
Состав и архитектура. Технологии			
6.	Автоматизированные рабочие места	–	–
7.	Беспроводные точки доступа	–	–
8.	Виртуализация	–	–
9.	ГРИД	–	–
10.	Машинное обучение	–	–
11.	Мобильные устройства	–	–
12.	Облачные технологии	–	–
13.	Суперкомпьютеры	–	–
14.	Технология «толстый клиент»	–	–
15.	Технология «тонкий клиент»	–	–
16.	Управление технологическими процессами	+	+
17.	Хранилище больших данных	–	–
18.	Резервирование средств и систем	+	+
Взаимодействие с сетями электросвязи			
19.	Категория сети электросвязи	Технологическая	
20.	Протоколы взаимодействия, используемые при взаимодействии с сетью электросвязи	МЭК 60870-5-104, МЭК 61850-5-101, NTP v4, PRP B, PRP A	
21.	Тип доступа к сети электросвязи	Проводной	
22.	Цель взаимодействия с сетью электросвязи	Контроль за технологическим, производственным оборудованием (исполнительными устройствами)	
Каналы связи			
23.	Основной канал связи	Ethernet	Кросс оптический
24.	Резервный шифрованный канал связия	GPRS (МЭК 60870-5-104)	
25.	Синхронизация времени	ГЛОНАСС/GPS	
26.	Наличие подключения к сети «Интернет»	Подключение к сети «Интернет» отсутствует	

2.7. Пользователи объекта защиты

Для АСУ ТП характерны следующие группы пользователей, представленные в таблице 3.

Внутренние пользователи — лица, имеющие возможность постоянного или разового доступа к автоматизированной системе или ее отдельным компонентам.

Внешние пользователи — лица, не имеющие возможности физического доступа к автоматизированной системе или к ее отдельным компонентам.

Таблица 3 - Пользователи объекта защиты

№	Тип пользователя	Полномочия пользователя	Права доступа
1.	**Внутренний пользователь**		
1.1.	Администратор	Администрирование элементов объекта	Физический доступ на территорию и в помещения с компонентами
			Доступ к элементам объекта с полномочиями администратора
			Полный доступ к компонентам объекта и функциям конфигурирования, перепрограммирования и администрирования
1.2.	Пользователь (оператор, диспетчер)	Контроль функционала отдельных компонентов объекта	Физический доступ на территорию и в помещения с компонентами
			Ограниченный доступ к элементам объекта

№	Тип пользователя	Полномочия пользователя	Права доступа
			Доступ к отдельным компонентам и функциям объекта
1.3.	Обслуживающий персонал	Обслуживание помещений, где расположены элементы	Физический доступ на территорию и в помещения с компонентами объекта
			Ограниченный доступ к элементам объекта
1.4.	Внешние субъекты, занимающиеся обслуживанием	Администрирование элементов объекта	Физический доступ на территорию и в помещения с компонентами
			Полный доступ к компонентам объекта и функциям конфигурирования, перепрограммирования и администрирования во время проведения работ по договору
2.	**Внешний пользователь**		
2.1.	Администратор	Администрирование элементов объекта	Логический доступ к компонентам объекта
			Доступ к элементам объекта с полномочиями администратора
			Полный доступ к компонентам объекта и функциям конфигурирования, перепрограммирования и администрирования
2.2.	Пользователь (оператор, диспетчер)	Контроль функционала отдельных компонентов объекта	Логический доступ к компонентам объекта
			Ограниченный доступ к элементам объекта
			Доступ к отдельным компонентам и функциям объекта

В качестве нарушителей безопасности информации рассматриваются в том числе пользователи АСУ ТП. Полное описание модели нарушителя представлено в части «5. ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ (МОДЕЛЬ НАРУШИТЕЛЯ)».

2.8. Внешние интерфейсы

Описание интерфейсов АСУ ТП представлено в части «4 ОБЪЕКТЫ ВОЗДЕЙСТВИЯ» настоящей МУ.

Внешние сетевые (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.) включают в себя интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями на объекте защиты отсутствуют.

2.9. Дополнительные сведения

В соответствии с Методикой, в части описания объекта защиты (АСУ ТП), должна быть рассмотрена следующая информация:

- 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.

Вышеуказанная информация относится к следующим технологиям обработки данных:

- «центр (хранения и) обработки данных» (ЦОД / ЦХОД) — представляет собой специализированное **здание для размещения (хостинга) серверного и сетевого оборудования** и подключения абонентов к каналам сети Интернет. **Согласно ГОСТ** Р 58811-2020, ЦОД — это «специализированный объект, представляющий собой связанную систему ИТ-инфраструктуры и инженерной инфраструктуры, оборудование и части которых размещены в здании или помещении, подключенном к внешним сетям, как инженерным, так и телекоммуникационным». **Согласно стандарту TIA-942**, центр обработки данных (ЦОД) — это «здание (или его часть), основная функция которого состоит в том, что в нем находятся машинный зал и вспомогательные (подсобные) помещения для него».
- «облачные технологии» — технологии распределенной обработки данных, в которых компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис в режиме реального времени. **Согласно ГОСТ** ISO/IEC 17788-2016, облачные вычисления — это «парадигма для предоставления возможности сетевого доступа к масштабируемому и эластичному пулу общих физических или виртуальных ресурсов с предоставлением самообслуживания и администрированием по требованию».

Указанные технологии, включая элементы, связанные с предоставлением вычислительных услуг и распределением соответствующей ответственности, **не актуальны** для объекта защиты, так как:

- АСУ ТП реализует **автоматизированный контроль и управления режимами** электроснабжения и режимами работы электрооборудования в рамках ПС (энергообъекты, таблица 2);
- АСУ ТП **не использует** «облачные технологии» и технологии типа «центр обработки данных», и **не взаимодействует** с системами, применяющими указанные технологии;

— В рамках АСУ ТП **запрещено подключение к сети Интернет**.

Таким образом, в рамках АСУ ТП не рассматриваются технологии на базе информационно-телекоммуникационной инфраструктуры ЦОД или облачной инфраструктуры.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

3.1. Виды рисков

В ходе оценки УБИ определяются негативные последствия, которые могут наступить от реализации (возникновения) УБИ. **Типовые** виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации представлены в таблице 4.

Таблица 4 - Виды рисков (ущерба) и типовые негативные последствия от реализации угроз безопасности информации

№	Номер ущерба	Вид ущерба	Негативные последствия
1.	У1	Ущерб физическому лицу	– Угроза жизни или здоровью. – Унижение достоинства личности. – Нарушение свободы, личной неприкосновенности. – Нарушение неприкосновенности частной жизни. – Нарушение личной, семейной тайны, утрата чести и доброго имени. – Нарушение тайны переписки, телефонных переговоров, иных сообщений. – Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах. – Финансовый, иной материальный ущерб физическому лицу. – Нарушение конфиденциальности (утечка)персональных данных. – «Травля» гражданина в сети «Интернет». – Разглашение персональных данных граждан
2.	У2	Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью	– Нарушение законодательства Российской Федерации. – Потеря (хищение) денежных средств. – Недополучение ожидаемой (прогнозируемой) прибыли. – Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций. – Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. – Срыв запланированной сделки с партнером. – Необходимость дополнительных (незапланированных) затрат на восстановление деятельности. – Потеря клиентов, поставщиков. – Потеря конкурентного преимущества. – Невозможность заключения договоров, соглашений. – Нарушение деловой репутации. – Снижение престижа. – Дискредитация работников. – Утрата доверия. – Причинение имущественного ущерба. – Неспособность выполнения договорных обязательств. – Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). – Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций). – Принятие неправильных решений. – Простой информационной системы или сети. – Публикация недостоверной информации на веб-ресурсах организации. – Использование веб-ресурсов для распространения и управления ВПО. – Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени. – Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)
3.	У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	– Причинение ущерба жизни и здоровью людей. – Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения. – Прекращение или нарушение функционирования объектов транспортной инфраструктуры. – Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия). – Прекращение или нарушение функционирования сети связи. – Отсутствие доступа к государственной услуге. – Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации. – Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием. – Возникновение ущерба бюджетам Российской Федерации. – Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка. – Вредные воздействия на окружающую среду. – Прекращение или нарушение функционирования пункта управления (ситуационного центра). – Снижение показателей государственного оборонного заказа.

№	Номер ущерба	Вид ущерба	Негативные последствия
			– Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка. – Нарушение законодательства Российской Федерации. – Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др. – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов. – Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком. – Нарушение выборного процесса. – Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации. – Организация пикетов, забастовок, митингов и других акций. – Массовые увольнения. – Увеличение количества жалоб в органы государственной власти или органы местного самоуправления. – Появление негативных публикаций в общедоступных источниках. – Создание предпосылок к внутриполитическому кризису. – Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов. – Доступ к системам и сетям с целью незаконного использования вычислительных мощностей. – Использование веб-ресурсов государственных органов для распространения и управления ВПО. – Утечка информации ограниченного доступа. – Непредоставление государственных услуг

3.2. Негативные последствия

Для определения негативных последствий при реализации УБИ рассматриваются характерные (актуальные) для объекта защиты и Общества виды рисков и ущербов, которые могут наступить от нарушения или прекращения основных процессов.

Негативные последствия от реализации УБИ были конкретизированы и дополнены в соответствии с особенностями области деятельности, в которой функционирует АСУ ТП.

Виды ущерба, их оценка и негативные последствия от реализации УБИ, **актуальные** для данной АСУ ТП, представлены в таблице 5.

Таблица 5 - Актуальные виды ущерба и негативные последствия

№	Номер ущерба	Вид ущерба	Негативные последствия	Оценка риска
4.	У1	Ущерб физическому лицу	Ущерб жизни и здоровью людей	Маловероятно
5.	У2	Ущерб юридическому лицу	Нарушение законодательства РФ	Средний
			Порча данных	Средний
			Нарушение штатного режима функционирования	Средний
			Ухудшение состояния носителей данных	Средний
			Ошибка в использовании объекта защиты	Средний
			Простой объекта защиты	Низкий
			Нарушение обслуживания	Низкий
			Отказ оборудования	Средний
			Затраты на восстановление работоспособности объекта защиты	Средний
			Негативное воздействие на репутацию Общества	Низкий
			Нарушение штатного режима функционирования АСУ	Средний
6.	У3	Ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	Причинение ущерба жизни и здоровью людей	Маловероятно

В соответствии с ГОСТ Р 51901.1-2002, под риском понимается сочетание вероятности события и его последствий. В настоящей МУ риски оцениваются в соответствии со значениями из таблицы 6.

Таблица 6 - Оценка (критерии) рисков

№	Оценка риска	Описание оценки риска	Описание оценки последствий риска
1.	Маловероятно	Отсутствуют объективные предпосылки для возникновения ущерба	Ущерб не наступает
2.	Низкий	Нанесенный ущерб ведет к незначительным негативным последствиям	Ущерб компенсируются принятыми мерами
3.	Средний	Нанесенный ущерб ведет к средним негативным последствиям	Для компенсации необходимы дополнительные трудозатраты
4.	Высокий	Нанесенный ущерб ведет к значительным негативным последствиям	Компенсация ведет к значительным трудозатратам
5.	Критический	Нанесенный ущерб ведет к критическим негативным последствиям	Последствия оказывают значительное влияние на деятельность Общества

4. Возможные объекты воздействия угроз безопасности информации

4.1. Компоненты объекта защиты

Оценка угроз безопасности информации проводится на основе их предполагаемых архитектуры и условий функционирования, определенных по результатам изучения и анализа исходных данных на них.

В ходе оценки УБИ определены следующие объекты воздействия: информационные ресурсы и компоненты объекта защиты, НСД к которым или воздействие на которые в ходе реализации (возникновения) УБИ может привести к негативным последствиям.

Границы процесса оценки УБИ в МУ определены совокупностью объектов воздействия и их интерфейсов. В соответствии с Методикой определены объекты воздействия на следующих уровнях: аппаратном, системном, прикладном, сетевом, уровне пользователей.

Объекты воздействия и виды воздействия на них конкретизированы применительно к архитектуре и условиям функционирования объекта защиты, а также областям и особенностям деятельности владельца АСУ ТП. Объекты воздействия на вышеуказанных уровнях, дополненные в соответствии с особенностями архитектуры АСУ ТП, описаны в таблице 7.

Таблица 7 - Объекты и уровни воздействия

№	Уровень системы	Объекты воздействия и уровни воздействия				
		Аппаратный	Сетевой	Системный	Прикладной	Пользовательский
1. 2.	Уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень)	Устройства ТМ / АСУ ТП	– RS-485: МЭК 60870-5-101 – RS-485: ModBus	Отсутствуют		
3.	Уровень автоматического управления (средний уровень)	TOPAZ IEC DAS	– Ethernet: МЭК 60870-5-104 – RS-485: МЭК 60870-5-101	ТОС: Topaz Linux	ПАК ViPNet Coordinator СКЗИ Drypt	
4.	Уровень диспетчерского управления (верхний уровень)	Описан во внутренней документации Общества	– Ethernet: МЭК 60870-5-104 – Ethernet: МЭК 61850	– ОС: Linux – ОС: Windows	ПО описано во внутренней документации Общества	
5.	Каналы связи	Основной и резервный шифрованный канал связи	GPRS (МЭК 60870-5-104)	Отсутствуют		

4.2. Виды воздействия

Основными видами воздействия на ТМ являются различные НСД и (или) деструктивные действия по отношению к объекту защиты и обрабатываемой им информации:

- утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности);
- НСД к компонентам, защищаемой информации, системным, конфигурационным и иным данным;
- отказ в обслуживании компонентов (нарушение доступности);
- несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных данных (нарушение целостности);
- несанкционированное использование вычислительных ресурсов систем и сетей в интересах решения несвойственных им задач;
- нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации.

Объекты воздействия и виды воздействия на них конкретизированы применительно к архитектуре и условиям функционирования систем и сетей, а также областям и особенностям деятельности обладателя информации и оператора.

5. Источники угроз безопасности информации (модель нарушителя)

5.1. Характеристика нарушителя

5.1.1. Источники угроз безопасности информации: определение нарушителя

В ходе оценки УБИ определены возможные антропогенные источники УБИ: лица (нарушители), осуществляющие реализацию УБИ путем НСД и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей.

Исходными данными для определения возможных актуальных нарушителей стали:

- документы, указанные в части «1.2. Источники обработки»;
- негативные последствия от реализации (возникновения) угроз безопасности информации, определенные в части «3. РИСКИ И ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗ»;
- объекты воздействия угроз безопасности информации и виды воздействия на них, определенные в части «4. ОБЪЕКТЫ ВОЗДЕЙСТВИЯ».

При формировании предположений о потенциальных возможностях реальных нарушителей при реализации ими угроз безопасности информации в АСУ ТП рассматриваются:

- уровень физического доступа к информации и (или) к компонентам;
- уровень логического доступа к информации и (или) к компонентам;
- уровень квалификации нарушителя безопасности информации;
- уровень оснащенности нарушителя безопасности информации;
- мотивация нарушителя безопасности информации.

При детализации угроз существенное значение имеет потенциал нарушителя, определяемый его возможностями и характером воздействия (преднамеренное или случайное).

В качестве нарушителей информационной безопасности АСУ ТП определены лица, осуществляющие преднамеренные и непреднамеренные действия, которые могут привести к нарушению безопасности информации, функционирования АСУ ТП или обслуживающей ее инфраструктуры.

5.1.2. Источники угроз безопасности информации: оценка нарушителя

Целью оценки возможностей нарушителей по реализации УБИ является формирование предположений о типах, видах нарушителей, которые могут реализовать угрозы безопасности информации в АСУ ТП, а также потенциале этих нарушителей, возможных способах и сценариях реализации УБИ.

Исходными данными для определения возможных актуальных нарушителей являются:

- общий перечень УБИ, содержащийся в БДУ ФСТЭК России (bdu.fstec.ru);
- документация на АСУ ТП (в части сведений о назначении и функциях, составе и архитектуре АСУ ТП, о группах пользователей и уровне их полномочий, и типах доступа, о внешних и внутренних интерфейсах);
- результаты оценки ущерба (рисков), определенные в настоящей МУ;
- негативные последствия от реализации (возникновения) УБИ, определенные в настоящей МУ;
- объекты воздействия УБИ и виды воздействия на них, определенные в настоящей МУ.

Нарушители признаются актуальными, когда возможные цели реализации ими УБИ могут привести к определенным для объекта защиты негативным последствиям и соответствующим рискам (видам ущерба).

Для актуальных нарушителей определены их категории в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования этих систем и сетей, а также от установленных возможностей нарушителей.

По результатам определения источников угроз безопасности информации определены:

- виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности;
- категории актуальных нарушителей, которые могут реализовывать угрозы безопасности информации, в том числе непреднамеренные угрозы.

5.1.3. Возможные цели реализации угроз безопасности информации: мотивация нарушителя

В качестве возможных целей (мотивации) реализации нарушителями УБИ АСУ ТП определены:

- нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики;
- реализация УБИ по идеологическим или политическим мотивам;
- организация террористического акта;
- причинение имущественного ущерба путем мошенничества или иным преступным путем;
- дискредитация или дестабилизация деятельности органов государственной власти, организаций;
- получение конкурентных преимуществ;
- внедрение дополнительных функциональных возможностей в ПО или программно-технические средства на этапе разработки;
- любопытство или желание самореализации;
- выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды;
- реализация УБИ из мести;
- реализация УБИ непреднамеренно из-за неосторожности или неквалифицированных действий.

Среди возможных целей реализации УБИ определены следующие, не являющиеся актуальными:

- нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики не рассматривается в качестве актуальной мотивации нарушителя, так как при нарушении ИБ объекта защиты ущерб государству, отдельным его сферам или секторам экономики не наступает;
- реализация УБИ по идеологическим или политическим мотивам не рассматривается в качестве актуальной мотивации нарушителя, так как нарушение ИБ объекта защиты не имеет политического веса;
- дискредитация или дестабилизация деятельности органов государственной власти, организаций не рассматривается в качестве актуальной мотивации нарушителя, так как при нарушении ИБ объекта защиты дискредитация или дестабилизация деятельности органов государственной власти не наступает;
- получение конкурентных преимуществ не рассматривается в качестве актуальной мотивации нарушителя, так как объект защиты находится под управлением организации, не имеющей конкурентов в своей сфере деятельности.

Предположения о целях (мотивации) нарушителей делаются с учетом целей и задач объекта защиты, вида обрабатываемой информации, а также с учетом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации.

Виды нарушителей, характерных (актуальных) для объекта защиты, определяются на основе предположений (прогноза) о возможных целях (мотивации) при реализации УБИ этими нарушителями.

Экспертным путем для АСУ ТП устанавливаются актуальные виды потенциальных нарушителей, их мотивации с учетом специфики обработки информации и уровня ущерба, который может быть причинен от реализации УБИ. Модель нарушителей, актуальных для АСУ ТП, приведена в таблице 8.

5.2. Актуализация нарушителя

5.2.1. Типы нарушителя

Типы (категория) нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам АСУ ТП, а также анализа возможностей нарушителей по доступу к компонентам объекта защиты исходя из структурно-функциональных характеристик и особенностей его функционирования.

В зависимости от имеющихся прав доступа нарушители могут иметь легитимный физический (непосредственный) и (или) логический доступ к компонентам информационной системы и (или) содержащейся в них информации или не иметь такого доступа. При этом уровень физического доступа нарушителя определяется исходя из наличия возможности физического доступа к информации и компонентам объекта защиты.

С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам объекта защиты нарушители подразделяются на два типа:

- внутренние нарушители — лица, имеющие право постоянного или разового доступа к объекту защиты, его отдельным компонентам.

— внешние нарушители — лица, не имеющие права доступа к объекту защиты, его отдельным компонентам и реализующие УБИ из-за границ контролируемой зоны (далее — КЗ).

Наибольшими возможностями по реализации УБИ обладают внутренние нарушители. Возможности нарушителя данного типа существенным образом зависят от установленного порядка допуска физических лиц к объекту защиты и его компонентам, а также мер по контролю за доступом и работой этих лиц. Внутренние нарушители первоначально могут иметь разный уровень прав доступа к компонентам объекта защиты: к ним относятся пользователи, имеющие как непривилегированные (пользовательские), так и привилегированные (административные) права доступа к компонентам объекта защиты. Внутренние нарушители реализуют УБИ преднамеренно или непреднамеренно, с использованием программных, программно-аппаратных средств или без использования таковых.

Внешний нарушитель рассматривается в качестве актуального во всех случаях, когда объект защиты обладает подключением к внешним информационно-телекоммуникационным сетям и (или) имеются линии связи, выходящие за пределы КЗ, используемые для иных подключений. Внешние нарушители реализуют УБИ преднамеренно с использованием программных, программно-аппаратных средств или без использования таковых.

5.2.2. Виды и потенциал нарушителя

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определяются виды нарушителей, актуальных для систем и сетей. Основными видами нарушителей, подлежащих оценке, являются:

— специальные службы иностранных государств;
— террористические, экстремистские группировки;
— преступные группы (криминальные структуры);
— отдельные физические лица (хакеры);
— конкурирующие организации;
— разработчики программных, программно-аппаратных средств;
— лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
— поставщики услуг связи, вычислительных услуг;
— лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
— лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем;
— авторизованные пользователи систем и сетей;
— системные администраторы и администраторы безопасности;
— бывшие (уволенные) работники (пользователи).

Указанные виды нарушителей могут быть дополнены иными нарушителями с учетом особенностей области деятельности, в которой функционируют системы и сети. Для одной системы и сети актуальными могут являться нарушители нескольких видов.

В части «3.4. Пользователи объекта защиты» были определены пользователи объекта защиты, являющиеся потенциальными нарушителями безопасности информации:

— администратор (входит в «системные администраторы и администраторы безопасности»);
— пользователь (входит в «авторизованные пользователи систем и сетей»);
— обслуживающий персонал (входит в «лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем»);
— внешние субъекты, занимающиеся обслуживанием (входит в «лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ»).

Нарушители имеют разные уровни компетентности, оснащенности ресурсами и мотивации для реализации УБИ.

Наибольшую вероятность реализовать УБИ и нанести ущерб АСУ ТП имеют пользователи с полномочиями администратора баз данных, системного администратора ЛВС/администратора системы ИБ. Администраторы потенциально могут реализовывать УБИ, используя возможности по непосредственному доступу к компонентам АСУ ТП. К лицам данных категорий ввиду их роли в ПТК АСУ ТП должен применяться комплекс организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Совокупность данных характеристик определяет уровень возможностей нарушителей по реализации УБИ. Потенциал нарушителей и их возможности установлены в соответствии с Методикой и приведены в таблице 8.

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации УБИ, описаны в таблице 12.

5.2.3. Определение актуальности нарушителя

Таблица 8 - Уровни возможностей нарушителя

№	Категория нарушителя	Виды нарушителей	Уровень возможностей нарушителей	Возможности нарушителей по реализации УБИ	Актуальность нарушителя
Уровень возможностей нарушителя Н1					
1.	Внутренний	Бывшие (уволенные) работники (пользователи)	Нарушитель, обладающий базовыми возможностями	– использует только известные уязвимости, скрипты и инструменты; – использует средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами; – имеет минимальные знания механизмов их функционирования, доставки и выполнения ВПО, эксплойтов; – обладает базовыми знаниями и навыками на уровне пользователя; – при наличии физического доступа имеет возможность реализации угроз за счет физических воздействий на элементы объекта защиты и обеспечивающих систем и сетей	Неактуален: нарушитель не имеет доступа к компонентам
2.	Внутренний	Авторизованные пользователи систем и сетей			Актуален
3.	**Примечание:**	Нарушители имеют возможность реализовывать только известные угрозы/уязвимости, с использованием общедоступных инструментов			
Уровень возможностей нарушителя Н2					
4.	Внутренний	Системные администраторы и администраторы безопасности	Нарушитель, обладающий базовыми повышенными возможностями	– владеет инструментами, свободно распространяемыми в сети «Интернет», может вносить изменения в их функционирование для повышения эффективности реализации угроз; – оснащен и владеет фреймворками и наборами средств, инструментов для реализации УБИ и использования уязвимостей; – навыки самостоятельного планирования и реализации сценариев УБИ. – практические знания о функционировании систем и сетей, ОС; – знание защитных механизмов, применяемых в ПО, программно-аппаратных средствах	Актуален
5.	Внутренний	Отдельные физические лица (хакеры)			Актуален
6.	Внешний	Отдельные физические лица (хакеры)			
7.	Внутренний	Авторизованные пользователи			Актуален
8.	Внутренний	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ			Актуален
9.	Внешний	Конкурирующие организации			Неактуален: отсутствует мотивация
10.	**Примечание:**	Обладает всеми возможностями нарушителей Н1. Может реализовывать угрозы, направленные на недокументированные уязвимости, с использованием инструментов, свободно распространяемых в сети «Интернет». Без возможностей реализации угроз на физически изолированные сегменты систем и сетей			
Уровень возможностей нарушителя Н3					
11.	Внутренний	Системные администраторы и администраторы безопасности	Нарушитель, обладающий средними возможностями	– возможность приобретать информацию об уязвимостях; – возможность приобретать дорогостоящие средства для реализации угроз; – возможность самостоятельно разрабатывать инструменты, необходимые для реализации УБИ, реализовывать угрозы с их использованием; – возможность получения доступа к программно-аппаратным средствам для проведения их анализа; – обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях; – обладает высокими знаниями и практическими навыками о функционировании систем и сетей, ОС; – глубокое понимание защитных механизмов, применяемых в ПО, программно-аппаратных средствах. – возможность реализовывать УБИ в составе группы лиц	Актуален
12.	Внутренний	Лица, обеспечивающие системы и сети или обеспечивающие системы оператора			Актуален
13.	Внутренний	Разработчики программных, программно-аппаратных средств			Актуален
14.	Внешний	Поставщики программно-аппаратных средств, обеспечивающих систем			Актуален
15.	Внутренний	Поставщики вычислительных услуг, услуг связи			Актуален
16.	Внутренний	Преступные группы (криминальные структуры)			Актуален
17.	Внешний	Преступные группы (криминальные структуры)			
18.	Внешний	Террористические, экстремистские организации			Актуален
19.	**Примечание:**	Обладает всеми возможностями нарушителей с Н2. Может реализовывать угрозы с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты систем и сетей			
Уровень возможностей нарушителя Н4					
20.	Внешний	Специальные службы иностранных государств	Нарушитель, обладающий высокими возможностями	– получение доступа к исходному коду ПО программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня»; – внедрение закладок или уязвимостей на различных этапах поставки ПО или программно-аппаратных средств; – создание методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение; – реализация угроз с привлечением специалистов уровня Н1-Н3; – создание и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений; – возможность долговременно и незаметно для операторов систем и сетей реализовывать УБИ; – обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, ОС,	Неактуален: отсутствует мотивация
21.	Внутренний	Специальные службы иностранных государств			

№	Категория нарушителя	Виды нарушителей	Уровень возможностей нарушителей	Возможности нарушителей по реализации УБИ	Актуальность нарушителя
				аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в ПО, программно-аппаратных средствах атакуемых систем и сетей	
22.	**Примечание:**	Обладает всеми возможностями нарушителей со средними возможностями. Имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей			

5.2.4. Перечень актуальных нарушителей

При определении актуального нарушителя были сделаны следующие выводы:

- **сотрудники**, обладающие правами доступа типа «администратор» к ПТК АСУ ТП, не заинтересованы в причинении ущерба объекту защиты по причине отсутствия объективных мотивов для реализации УБИ. Таким образом, предполагается, что для данного вида нарушителя характерна (актуальна) **реализация угроз за счет непреднамеренных, неосторожных или неквалифицированных действий;**
- с учетом сферы деятельности, у Общества **отсутствуют конкурирующие организации**;
- **разработчики программных, программно-аппаратных средств,** применяемых в ПТК АСУ ТП, не заинтересованы в причинении ущерба объекту защиты по причине отсутствия объективных мотивов для реализации УБИ. Таким образом, предполагается, что для данного вида нарушителя характерна (актуальна) **реализация угроз за счет непреднамеренных, неосторожных или неквалифицированных действий;**
- **поставщики услуг связи и вычислительных услуг** не заинтересованы в причинении ущерба объекту защиты по причине отсутствия объективных мотивов для реализации УБИ. Таким образом, предполагается, что для данного вида нарушителя характерна (актуальна) **реализация угроз за счет непреднамеренных, неосторожных или неквалифицированных действий;**
- **лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ**, выполняемых в ПТК АСУ ТП, не заинтересованы в причинении ущерба объекту защиты по причине отсутствия объективных мотивов для реализации УБИ. Таким образом, предполагается, что для данного вида нарушителя характерна (актуальна) **реализация угроз за счет непреднамеренных, неосторожных или неквалифицированных действий**;
- **специальные службы иностранных государств**, в силу специфики их деятельности, не обладают мотивацией (отсутствие на объекте защиты процессов обработки информации, содержащей сведения, составляющие государственную тайну) для проведения атаки на объект защиты. Также учитывается, что применение специальных средств и аппаратуры экономически нецелесообразно для нарушителя.

Определен следующий перечень актуальных нарушителей:

1. авторизованные пользователи систем и сетей (Общества);
2. системные администраторы и администраторы безопасности (Общества);
3. отдельные физические лица (хакеры);
4. лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
5. лица, обеспечивающие системы и сети (АСУ ТП) или обеспечивающие системы оператора (Общества);
6. разработчики программных, программно-аппаратных средств;
7. поставщики программно-аппаратных средств, обеспечивающих систем;
8. поставщики вычислительных услуг (неактуально), услуг связи (актуально);
9. преступные группы (криминальные структуры);
10. террористические, экстремистские организации.

5.3. Возможности актуального нарушителя

Нарушителями могут быть реализованы следующие УБИ, применительно к назначению, составу и архитектуре АСУ ТП. Подробнее возможности нарушителей раскрыты в таблице 9.

Таблица 9 - Возможности нарушителя относительно АСУ ТП.

№	Виды нарушителей	Возможности нарушителей по реализации УБИ	Предполагаемые последствия реализации УБИ
1.	авторизованные пользователи систем и сетей (Общества)	– возможность реализации УБИ за счет физических воздействий	– доступ к аутентификационной информации; – изменение аутентификационной информации; – обнаружение открытых портов; – обнаружение хостов; – определение топологии вычислительной сети; – перезагрузка АСУ ТП; – перехват данных, передаваемых АСУ ТП; – приведение АСУ ТП в состояние «отказ в обслуживании»; – физическое выведение из строя АСУ ТП; – неправомерное шифрование информации; – несанкционированное изменение параметров настройки средств защиты информации; – использование информации идентификации/аутентификации, заданной по умолчанию;
2.	системные администраторы и администраторы безопасности (Общества)	– наличие инструментов для реализации УБИ и использования уязвимостей; – навыки самостоятельного планирования и реализации сценариев УБИ. – практические знания о функционировании систем и сетей, ОС; – знание защитных механизмов, применяемых в ПО, программно-аппаратных средствах	
3.	отдельные физические лица (хакеры)		
4.	авторизованные пользователи (АСУ ТП)		
5.	лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ		
6.	системные администраторы и администраторы безопасности	– возможность приобретать информацию об уязвимостях; – возможность приобретать дорогостоящие средства для реализации УБИ; – возможность самостоятельно разрабатывать инструменты, необходимые для реализации УБИ, реализовывать угрозы с их использованием; – возможность получения доступа к программно-аппаратным средствам для проведения их анализа; – знания и практические навыки проведения анализа программного кода для получения информации об уязвимостях; – знания и практические навыки о функционировании систем и сетей, ОС; – понимание защитных механизмов, в том числе применяемых в АСУ ТП – возможность реализовывать УБИ в составе группы лиц	– внедрение кода или данных; – изменение системных и глобальных переменных; – неправомерные действия в каналах связи; – перебора всех настроек и параметров АСУ ТП; – получение предварительной информации об АСУ ТП; – преодоление физической защиты; – наличие механизмов разработчика; – перехват управления АСУ ТП; – изменение ВПО значений параметров программируемых логических контроллеров; – нарушение работы АСУ ТП; – перехват управление информационной системой.
7.	лица, обеспечивающие системы и сети (АСУ ТП) или обеспечивающие системы оператора (Общества)		
8.	разработчики программных, программно-аппаратных средств		
9.	поставщики программно-аппаратных средств, обеспечивающих систем;		
10.	поставщики вычислительных услуг (неактуально), услуг связи (актуально)		
11.	преступные группы (криминальные структуры)		
12.	террористические, экстремистские организации		

6. Способы реализации (возникновения) угроз безопасности информации

6.1. Возникновение и реализация угроз

Возможные для АСУ ТП УБИ, к которым относятся осуществляемые нарушителем воздействия на компоненты объекта защиты, определяются на основе анализа исходных данных.

УБИ возможна при совпадении следующих факторов:

- имеется нарушитель или иной источник угрозы;
- есть объект, на который осуществляются воздействия;
- существуют способы реализации УБИ (сценарии реализации УБИ);
- реализация угрозы может привести к негативным последствиям.

В ходе оценки УБИ определены негативные последствия, которые могут наступить от реализации (возникновения) УБИ. Негативные последствия от реализации УБИ описаны в части «3. РИСКИ И ПОСЛЕДСТВИЯ РЕАЛИЗАЦИИ УГРОЗ» настоящей МУ.

В ходе оценки УБИ определены способы реализации угроз. Способы реализации угроз описаны в частях «7.2. Возможные сценарии реализации угроз безопасности информации» и «5. Источники угроз безопасности информации (модель нарушителя)» настоящей МУ.

В ходе оценки УБИ определены интерфейсы объектов воздействия, доступных для использования нарушителями способов реализации УБИ. Интерфейсы воздействия описаны в частях «4. ОБЪЕКТЫ ВОЗДЕЙСТВИЯ» и «6.2. Реализация нарушителем угроз безопасности информации через доступ к интерфейсам воздействия» настоящей МУ.

6.2. Реализация нарушителем угроз безопасности информации через доступ к интерфейсам воздействия

Условием, позволяющим нарушителям использовать способы реализации УБИ, является наличие у них возможности доступа к следующим типам интерфейсов объекта защиты:

- внешние сетевые интерфейсы, обеспечивающие взаимодействие с сетью «Интернет», смежными (взаимодействующими) системами или сетями (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- внутренние сетевые интерфейсы, обеспечивающие взаимодействие (в том числе через промежуточные компоненты) с компонентами систем и сетей, имеющими внешние сетевые интерфейсы (проводные, беспроводные);
- интерфейсы для пользователей (проводные, беспроводные, веб-интерфейсы, интерфейсы удаленного доступа и др.);
- интерфейсы для использования съемных МНИ и периферийного оборудования;
- интерфейсы для установки, настройки, испытаний, пусконаладочных работ (в том числе администрирования, управления, обслуживания) обеспечения функционирования компонентов систем и сетей;
- возможность доступа к поставляемым или находящимся на обслуживании, ремонте в сторонних организациях компонентам систем и сетей.

Наличие указанных интерфейсов определяется архитектурой, составом и условиями функционирования систем и сетей, группами пользователей, их типами доступа и уровнями полномочий.

В ходе анализа определены логические и физические интерфейсы объектов воздействия, в том числе требующие физического доступа к ним. Интерфейсы определены на аппаратном, системном и прикладном уровнях, а также для телекоммуникационного оборудования.

Возможность использования интерфейсов объекта защиты на указанных уровнях определяется возможностями актуальных нарушителей.

7. Актуальные угрозы безопасности информации

7.1. Моделирование угроз безопасности информации

7.1.1. Предварительная актуализация угроз безопасности информации

В соответствии с методическими документами, указанными в части «1.2. Источники разработки», сформирован перечень возможных УБИ для объекта защиты.

При рассмотрении были исключены угрозы, направленные на информационные технологии, не используемые в АСУ ТП (таблица 10).

Таблица 10 - Неактуальные угрозы

№	Неиспользуемые технологии	№ УБИ
1.	АРМ	26, 67, 68, 93, 121, 158, 160
2.	BIOS/UEFI	4, 5, 9, 13, 18, 24, 32, 39, 45, 53, 72, 87, 123, 129, 144, 150
3.	Беспроводные точки доступа	11, 83, 125, 126, 133
4.	Виртуализация	10, 44, 46, 48, 52, 58, 59, 75, 76, 77, 78, 79, 80, 84, 85, 108, 119, 120
5.	Грид-системы	1, 2, 47, 81, 110, 147
6.	Сеть Интернет и электронная почта	16, 17, 19, 41, 42, 49, 61, 62, 130, 131, 135, 145, 151, 154, 159, 167, 168, 171, 172, 173, 174, 175, 186, 190, 197, 201, 215
7.	Искусственный интеллект и машинное обучение	218, 219, 220, 221, 222
8.	Мобильные устройства	184, 194, 195, 196, 199 ,200, 202, 208, 216
9.	Облачные технологии	20, 21, 40, 43, 54, 55, 56, 64, 65, 66, 70, 96, 101, 134, 135, 136, 137 138, 141, 142, 164
10.	Системы хранения больших данных	38, 50, 57, 60, 84, 97, 105, 136, 148
11.	Суперкомпьютеры	29, 82, 106, 146, 161
12.	Подсистема температурного режима	180
13.	Многофакторная аутентификация	213

Также были исключены угрозы, для которых отсутствует актуальный нарушитель (Н4):

— УБИ 35, УБИ 92, УБИ 193, УБИ 206, УБИ 210.

Неактуальными признаются угрозы, риск которых маловероятен (см. таблица 7) и риск которых в сочетании с потенциалом нарушителя недостаточны для реализации УБИ. Соответствующие угрозы были исключены:

— УБИ 3, УБИ 7, УБИ 8, УБИ 12, УБИ 14, УБИ 15, УБИ 23, УБИ 27, УБИ 28, УБИ 30, УБИ 31, УБИ 33, УБИ 34, УБИ 35, УБИ 36, УБИ 37, УБИ 51, УБИ 63, УБИ 71, УБИ 73, УБИ 88, УБИ 89, УБИ 90, УБИ 94, УБИ 95, УБИ 100, УБИ 102, УБИ 107, УБИ 111, УБИ 112, УБИ 114, УБИ 115, УБИ 117, УБИ 118, УБИ 122, УБИ 124, УБИ 127, УБИ 128, УБИ 143, УБИ 149, УБИ 152, УБИ 155, УБИ 156, УБИ 162, УБИ 163, УБИ 165, УБИ 166, УБИ 177, УБИ 178, УБИ 179, УБИ 181, УБИ 182, УБИ 187, УБИ 188, УБИ 189, УБИ 191, УБИ 192, УБИ 198, УБИ 203, УБИ 205, УБИ 207, УБИ 209, УБИ 211, УБИ 214, УБИ 217.

7.1.2. Модель угроз безопасности информации

Актуальность возможных угроз безопасности информации определяется наличием сценариев их реализации.

Способы реализации (возникновения) угроз безопасности информации определяются применительно к объектам воздействия. Способы являются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз безопасности и имеются или созданы условия, при которых такая возможность может быть реализована в отношении объектов воздействия. Одна угроза безопасности информации может быть реализована несколькими способами.

Модель угроз приведена в таблице 11 и включает в себя следующие элементы:

— № УБИ — включает номер угрозы (угроз) в соответствии с БДУ ФСТЭК;

— Наименование угрозы — включает название УБИ или группы угроз;

— Категория нарушителей и уровень возможностей нарушителя — включает тип актуального нарушителя, способного на реализацию угрозы, и уровень возможностей нарушителя

— Объекты воздействия — включает элементы объекта защиты (общее наименование элемента), на которые возможно негативное воздействие;

— Уязвимости — включает описание уязвимостей в соответствии с базой данных гроз ФСТЭК;

— Способ реализации угрозы — включает описание способов реализации угрозы;

— Негативные последствия — включает описание негативных последствий в случае реализации угрозы;

— Возможность реализации угрозы — включает описание возможности/невозможности реализации угрозы;

— Сценарий реализации угрозы (техники) – включает сценарии реализации и тактики УБИ;

— Актуальность угрозы — включает отметку актуальности/неактуальности угрозы.

В МУ, представленной в таблице 11, не указываются угрозы, направленные на информационные технологии, не используемые в АСУ ТП (таблица 10), а также угрозы, для которых отсутствует актуальный нарушитель (Н4).

Таблица 11 - Перечень возможных (вероятных) угроз безопасности информации ПТК АСУ ТП

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
1.	003	Угроза анализа криптографических алгоритмов и их реализации	Внешний: Н2, Н3 Внутренний:Н2, Н3	Метаданные, ПО	Используются проверенные СКЗИ, прошедшие сертификацию ФСТЭК, что уменьшает возможность анализа криптоалгоритмов нарушителем	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
2.	**006**	Угроза внедрения кода или данных	Внутренний: Н2	Системное ПО, прикладное ПО, сетевое ПО	Недостаточность антивирусных мер ЗИ и разграничения доступа пользователей, наличие открытых портов.	В случае работы с файлами из недоверенных источников и/или при наличии привилегий установки ПО: возможность внедрения нарушителем ВПО	Внедрение ВПО, отказ в обслуживании	Средняя	Т2.2., Т2.8., Т2.10. Т2.11., Т6.8., Т1.18. Т7.10., Т7.15.	**Актуальна**
3.	007	Угроза воздействия на программы с высокими привилегиями	Внешний: Н2, Н3 Внутренний:Н2, Н3	ИС, сетевое ПО , сетевой трафик	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
4.	008	Угроза восстановления аутентификационной информации	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО , микро-ПО, учетные данные пользователя	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
5.	012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний: Н1	Системное ПО , прикладное ПО , сетевое ПО , микро-ПО, метаданные, объекты файловой системы, реестр	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
6.	014	Угроза длительного удержания вычислительных ресурсов пользователями	Внешний: Н2 Внутренний: Н1, Н2	ИС, сетевой узел, МНИ, системное ПО , сетевое ПО , сетевой трафик	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
7.	015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний: Н2 Внутренний: Н1, Н2	Объекты файловой системы	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
8.	**022**	Угроза избыточного выделения оперативной памяти	Внешний: Н2 Внутренний: Н1, Н2	Аппаратное обеспечение, системное ПО, сетевое ПО	Наличие слабостей механизма контроля выделения оперативной памяти различных программам	При условии нахождения ВПО в системе в активном состоянии: возможность выделения оперативной памяти для обслуживания запросов ВПО	Снижение объема ресурсов оперативной памяти, доступных в системе	Средняя	Т6.8., Т10.10., Т10.12.	**Актуальна**
9.	023	Угроза изменения компонентов системы	Внутренний: Н1	Аппаратное обеспечение	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
10.	**025**	Угроза изменения системных и глобальных переменных	Внутренний: Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО	Слабости механизма контроля доступа к разделяемой памяти. Уязвимости модулей ПО, реализующих контроль	Осуществление нарушителем НСД к переменным, в том числе из-за отсутствия проверки целостности их значений	Нарушение целостности данных, НСД к компонентам системы	Средняя	Т1.18, Т2.5., Т6.3, Т10.2. Т10.3. Т10.4. Т10.5. Т10.6.	**Актуальна**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
					целостности внешних переменных.					
11.	027	Угроза искажения вводимой и выводимой на периферийные устройства информации	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО , прикладное ПО , сетевое ПО , аппаратное обеспечение	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
12.	028	Угроза использования альтернативных путей доступа к ресурсам	Внешний: Н2 Внутренний: Н1, Н2	Сетевой узел, объекты файловой системы, прикладное ПО , системное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
13.	030	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	Внешний: Н3 Внутренний: Н1	СрЗИ,, системное ПО, сетевое ПО , микро-ПО, программно-аппаратные средства со встроенными функциями ЗИ	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
14.	031	Угроза использования механизмов авторизации для повышения привилегий	Внутренний: Н1, Н2	Системное ПО, прикладное ПО, сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
15.	033	Угроза использования слабостей кодирования входных данных	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО, прикладное ПО, сетевое ПО, микро-ПО, реестр	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
16.	034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО, сетевое ПО, сетевой трафик	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
17.	035	Угроза использования слабых криптографических алгоритмов BIOS	Внешний: Н3	Микро-ПО BIOS/UEFI	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
18.	036	Угроза исследования механизмов работы программы	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО , микро-ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
19.	037	Угроза исследования приложения через отчеты об ошибках	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО , микро-ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
20.	051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний: Н1	Рабочая станция, МНИ, системное ПО , метаданные, объекты файловой системы, реестр	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
21.	063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО , микро-ПО, аппаратное обеспечение	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
22.	**069**	Угроза неправомерных действий в каналах связи	Внешний: Н2	Сетевой трафик	Возможности внесения нарушителем изменений в работу сетевых протоколов	Использование уязвимостей сетевого оборудования и ПО, например путем добавления или	Нарушение доступности, отказ в обслуживании	Средняя	Т1, Т2, Т4, Т5, Т6, Т7, Т8, Т1.3, Т1.4, Т1.5, Т2.3, Т4.4, Т5.6, Т6.3, Т7.21, Т8.5	**Актуальна**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
					для оказания влияния на работу объекта защиты или получения доступа к информации, передаваемой по каналу связи	удаления данных из информационного потока				
23.	071	Угроза несанкционированного восстановления удаленной защищаемой информации	Внешний: Н2 Внутренний: Н1, Н2	МНИ	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
24.	073	Угроза НСД к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети	Внешний: Н2, Н3 Внутренний:Н2, Н3	Сетевое оборудование, микро-ПО, сетевое ПО , виртуальные устройства	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
25.	**074**	Угроза НСД к аутентификационной информации	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО, объекты файловой системы, учетные данные пользователя, реестр, МНИ	Возможность извлечения учетных данных из оперативной памяти или хищения (копирования) файлов паролей (в том числе хранящихся в открытом виде) с МНИ	При успешном осуществлении НСД к участкам оперативного или постоянного запоминающих устройств, в которых хранится информация аутентификации	Нарушение конфиденциальности	Средняя	Т1.9, Т1.12, Т2.5, Т2.6, Т2.10, Т2.11, Т6.8, Т10.1, Т10.2, Т10.3	**Актуальна**
26.	**086**	Угроза несанкционированного изменения аутентификационной информации	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО, объекты файловой системы, учетные данные пользователя, реестр	Возможность нарушителем осуществления доступа к аутентификационной информации других пользователей с помощью штатных средств ОС или специального ПО	Реализация данной угрозы может способствовать дальнейшему проникновению нарушителя в систему под учетной записью дискредитированного пользователя	Нарушение целостности Нарушение доступности	Средняя	Т1.9, Т1.12, Т2.5, Т2.6, Т2.10, Т2.11, Т6.8, Т10.1, Т10.2, Т10.3, Т10.7, Т10.8, Т10.9	**Актуальна**
27.	088	Угроза несанкционированного копирования защищаемой информации	Внешний: Н2 Внутренний: Н1, Н2	Объекты файловой системы, МНИ	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
28.	**089**	Угроза несанкционированного редактирования реестра	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО, использующее реестр, реестр	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
29.	090	Угроза несанкционированного создания учетной записи пользователя	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
30.	**091**	Угроза несанкционированного удаления защищаемой информации	Внешний: Н2 Внутренний: Н1, Н2	Метаданные, объекты файловой системы, реестр	Причинение нарушителем ущерба собственнику и оператору неправомерно удаляемой информации путем осуществления деструктивного программного или физического воздействия на МНИ	Возможно в случае получения нарушителем системных прав на стирание данных или физического доступа к МНИ на расстояние, достаточное для оказания эффективного деструктивного воздействия"	Нарушение доступности	Средняя	Т6.8, Т10.1, Т10.8	**Актуальна**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
31.	094	Угроза несанкционированного управления синхронизацией и состоянием	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО , микро-ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
32.	095	Угроза несанкционированного управления указателями	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
33.	**098**	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	Внешний: Н2	Сетевой узел, сетевое ПО, сетевой трафик	Сканирование нарушителем портов для получения сведений, позволяющих нарушителю определить по каким портам деструктивные воздействия могут быть осуществлены напрямую, а по каким —с использованием специальных техник обхода МСЭ	Возможно при условии наличия у нарушителя подключения к объекту защиты и специализированного ПО, реализующего функции сканирования портов и анализа сетевого трафика	Нарушение конфиденциальности	Средняя	Т7.21, Т8.5	**Актуальна**
34.	**099**	Угроза обнаружения хостов	Внешний: Н2	Сетевой узел, сетевое ПО, сетевой трафик	Сканирование нарушителем вычислительной сети для выявления работающих сетевых узлов	Возможно при условии наличия у нарушителя подключения к объекту защиты и специализированного ПО, реализующего функции анализа сетевого трафика	Нарушение конфиденциальности	Средняя	Т7.21, Т8.5	**Актуальна**
35.	100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО, сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
36.	102	Угроза опосредованного управления группой программ через совместно используемые данные	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
37.	**103**	Угроза определения типов объектов защиты	Внешний: Н2	Сетевой узел, сетевое ПО, сетевой трафик	Проведение нарушителем анализа выходных данных объекта защиты с помощью метода «fingerprinting». Не наносит прямого вреда, но собранные данные позволяют нарушителю выявить слабые места объекта защиты, которые могут быть использованы в дальнейшем	Возможна в случае наличия у нарушителя сведений о взаимосвязи выходных данных с конфигурацией объекта защиты (документация на программные средства, стандарты передачи данных, спецификации и т.п.)	Нарушение конфиденциальности	Средняя	Т1.9, Т1.12, Т2.5, Т2.6, Т2.10, Т2.11, Т6.8, Т10.1, Т10.2, Т10.3, Т10.7, Т10.8, Т10.9	**Актуальна**
38.	**104**	Угроза определения топологии вычислительной сети	Внешний: Н2	Сетевой узел, сетевое ПО, сетевой трафик	Сканирование сети нарушителем для получения сведений о топологии, которые могут быть использованы в дальнейшем при попытках реализации других угроз	Реализация возможна в случае наличия у нарушителя возможности подключения к исследуемой сети и наличием специализированного ПО, реализующего функцию анализа сетевого трафика	Нарушение конфиденциальности	Низкая	Т7.21, Т8.5	**Актуальна**
39.	107	Угроза отключения контрольных датчиков	Внешний: Н3 Внутренний: Н1	Системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
40.	**109**	Угроза перебора всех настроек и параметров приложения	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО , микро-ПО, реестр	Получение нарушителем доступа к дополнительному скрытому функционалу или приведению системы в состояние «отказ в обслуживании» при задании нарушителем некоторых параметров конфигурации, достигая таких значений параметров путем перебора всех возможных комбинаций.	Возможно при условии наличия у нарушителя привилегий на изменение конфигурации ПО. При реализации данной угрозы нарушитель действует простым путем перебора всевозможных комбинаций"	Нарушение целостности Нарушение доступности	Средняя	T1, T2, T4, T5, T6, T7, T8, T1.3, T1.4, T1.5, T2.3, T4.4, T5.6, T6.3, T7.21, T8.5	**Актуальна**
41.	111	Угроза передачи данных по скрытым каналам	Внешний: Н2, Н3 Внутренний:Н2, Н3	Сетевой узел, сетевое ПО , сетевой трафик	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
42.	112	Угроза передачи запрещенных команд на оборудование с числовым программным управлением	Внутренний: Н1	Системное ПО , прикладное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
43.	**113**	Угроза перезагрузки аппаратных и программно-аппаратных СВТ	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО, аппаратное обеспечение	Сброс пользователем (нарушителем) состояния оперативной памяти (обнуления памяти) путем случайного или намеренного осуществления перезагрузки отдельных устройств, блоков или системы в целом	Возможно аппаратным способом (нажатием кнопки), программным (локально или удаленно) при выполнении следующих условий: – наличие в системе открытых сессий работы пользователей; – наличие у нарушителя прав в системе (или физической возможности) на осуществление форсированной перезагрузки	Нарушение целостности Нарушение доступности	Средняя	T1.9, T1.12, T2.5, T2.6, T2.10, T2.11, T6.8, T10.1, T10.2, T10.3, T10.7, T10.8, T10.9	**Актуальна**
44.	114	Угроза переполнения целочисленных переменных	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО, прикладное ПО, сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
45.	115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внешний: Н2 Внутренний: Н1, Н2	Системное ПО , прикладное ПО , аппаратное обеспечение	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
46.	**116**	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний: Н2	Сетевой узел, сетевой трафик	НСД к сетевому трафику в пассивном («прослушивание» трафика) или активном (подмена пакетов, изменение их содержимого) режиме для сбора и анализа сведений, которые могут быть использованы в дальнейшем для реализации других угроз	Возможно в следующих условиях: – наличие у нарушителя доступа к сети объекта защиты; – неспособность технологий, с помощью которых реализована передача данных, предотвратить возможность осуществления скрытного прослушивания потока данных	Нарушение конфиденциальности	Средняя	T1.3, T1.4, T1.5, T2.3, T2.4	**Актуальна**
47.	117	Угроза перехвата привилегированного потока	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
48.	118	Угроза перехвата привилегированного процесса	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , прикладное ПО , сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
49.	122	Угроза повышения привилегий	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО , сетевое ПО, ИС	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
50.	124	Угроза подделки записей журнала регистрации событий	Внешний: Н2 Внутренний: Н1	Системное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
51.	127	Угроза подмены действия пользователя путем обмана	Внешний: Н3	Прикладное ПО , сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
52.	128	Угроза подмены доверенного пользователя	Внешний: Н2	Сетевой узел, сетевое ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
53.	**132**	Угроза получения предварительной информации об объекте защиты	Внешний: Н3	Сетевой узел, сетевое ПО, сетевой трафик, прикладное ПО	Раскрытие нарушителем сведений о состоянии объекта защиты., путем проведения мероприятий по сбору и анализу доступной информации. Обусловлено наличием уязвимостей в сетевом ПО, позволяющим получить сведения о конфигурации отдельных программ или объекта защиты в целом.	Возможно при условии получения информации об объекте защиты с помощью одного из следующих способов: – анализ реакций на сетевые запросы к открытым сетевым сервисам, которые могут стать причиной вызова необработанных исключений с подробными сообщениями об ошибках, содержащих защищаемую информацию; – анализ реакций системы на строковые URI-запросы..	Нарушение конфиденциальности	Низкая	Т2.2., Т2.8., Т2.10. Т2.11., Т6.8., Т1.18. Т7.10., Т7.15.	**Актуальна**
54.	**139**	Угроза преодоления физической защиты	Внешний: Н3	Сервер, рабочая станция, МНИ, аппаратное обеспечение	Осуществление нарушителем деструктивных действий в отношении объекта защиты при получении физического доступа к аппаратным СВТ путем преодоления системы контроля физического доступа, организованной в здании предприятия	Реализация возможна при условии успешного применения нарушителем любого из методов проникновения на объект	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	Низкая	Т2.2., Т2.8., Т2.10. Т2.11., Т6.8., Т1.18. Т7.10., Т7.15	**Актуальна**
55.	**140**	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний: Н2 Внутренний: Н1	ИС, сетевой узел, системное ПО, сетевое ПО, сетевой трафик, телекоммуникационное устройство	Отказ в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с объектом защиты или при использовании недостатков реализации сетевых протоколов	Реализация возможна при условии превышения объема запросов над объемами доступных для их обработки ресурсов или наличия ошибок реализации сетевых протоколов	Нарушение доступности	Средняя	Т1.3, Т1.4., Т1.5, Т2.3, Т2.4., Т2.5, Т3.1, Т4.1, Т4.4., Т6.1, Т6.2, Т6.3, Т6.4., Т6.6, Т7.1, Т10.10	**Актуальна**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
56.	143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний: Н2, Н3 Внутренний:Н2, Н3	МНИ, микро-ПО, аппаратное обеспечение, телекоммуникационное устройство	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
57.	149	Угроза, сбоя обработки специальным образом измененных файлов	Внешний: Н2, Н3 Внутренний:Н2, Н3	Метаданные, объекты файловой системы, системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
58.	152	Угроза удаления аутентификационной информации	Внешний: Н2 Внутренний: Н1	Системное ПО, микро-ПО, учетные данные пользователя	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
59.	155	Угроза утраты вычислительных ресурсов	Внешний: Н2 Внутренний: Н1	ИС, сетевой узел, МНИ, системное ПО, сетевое ПО, сетевой трафик	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
60.	156	Угроза утраты носителей информации	Внутренний: Н1	МНИ	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
61.	**157**	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний: Н2	Сервер, рабочая станция, МНИ, аппаратное обеспечение	Умышленное выведения из строя средств хранения, обработки и (или) ввода/ вывода/ передачи информации, что может привести к нарушению доступности, а в некоторых случаях и целостности защищаемой информации.	Получение нарушителем физического доступа к МНИ, средствам обработки информации и средствам ввода/ вывода информации	Нарушение целостности Нарушение доступности	Средняя	Т2.2., Т2.8., Т2.10. Т2.11., Т6.8., Т1.18. Т7.10., Т7.15	**Актуальна**
62.	162	Угроза эксплуатации цифровой подписи программного кода	Внешний: Н2 Внутренний: Н1	Системное ПО , прикладное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
63.	163	Угроза перехвата исключения/сигнала из привилегированного блока функций	Внешний: Н2, Н3 Внутренний:Н2, Н3	Системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
64.	165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний: Н2, Н3	ПО, техническое средство, ИС, ключевая система информационной инфраструктуры	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
65.	166	Угроза внедрения системной избыточности	Внутренний: Н2, Н3	ПО, ИС	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
66.	**169**	Угроза наличия механизмов разработчика	Внутренний: Н2, Н3	ПО, техническое средство	Перехват управления за счет использования отладочных механизмов	Если в ПО не удалены отладочные механизмы	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	Средняя	Т1.18, Т2.5., Т6.3, Т10.2. Т10.3. Т10.4. Т10.5. Т10.6.	**Актуальна**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
67.	**170**	Угроза неправомерного шифрования информации	Внешний: Н2	Объект файловой системы	Потеря доступности данных из-за их несанкционированного криптографического преобразования нарушителем с помощью известного только ему секретного ключа.	Возможна при условии успешной установки нарушителем средства криптографического преобразования информации, а также успешного обнаружения нарушителем защищаемых файлов	Нарушение доступности	Средняя	Т2.2., Т2.8., Т2.10. Т2.11., Т6.8., Т1.18. Т7.10., Т7.15	**Актуальна**
68.	**176**	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Внешний: Н2	СрЗИ	Приведение в состояние «отказ в обслуживании» или нарушения штатного режима функционирования из-за временной задержки в системах реального времени, вносимой в процессы передачи и обработки защищаемой информации СрЗИ, вызванной необходимостью обработки передаваемой/обрабатываемой информации на предмет выявления и нейтрализации УБИ	На реализацию данной угрозы влияют применяемые СрЗИ, параметры их настройки, объем передаваемой/ обрабатываемой информации, а также текущая активность внешних нарушителей, программные воздействия которых обрабатываются средствами защиты информации	Нарушение доступности	Средняя	Т1, Т2, Т4, Т5, Т6, Т7, Т8, Т1.3, Т1.4, Т1.5, Т2.3, Т4.4, Т5.6, Т6.3, Т7.21, Т8.5	**Актуальна**
69.	177	Угроза неподтвержденного ввода данных оператором в систему, связанную с безопасностью	Внутренний: Н1	Системное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	**Неактуально**
70.	178	Угроза несанкционированного использования системных и сетевых утилит	Внешний: Н2 Внутренний: Н1	Системное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	**Неактуально**
71.	179	Угроза несанкционированной модификации защищаемой информации	Внешний: Н2 Внутренний: Н1	Объекты файловой системы	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровня риска	**Неактуально**
72.	181	Угроза перехвата одноразовых паролей в режиме реального времени	Внешний: Н3	Сетевое ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
73.	182	Угроза физического устаревания аппаратных компонентов	Внутренний: Н1	Аппаратное средство	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
74.	**183**	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Внешний Внутренний	ПО автоматизированной системы управления технологическими процессами	Осуществление нарушителем НСД к информационной инфраструктуре за счет получения нарушителем права управления входящей в ее состав АСУ ТП путем эксплуатации уязвимостей ее ПО или слабостей технологических протоколов передачи данных.	Возможно при условии наличия у нарушителя прав на осуществление взаимодействия с АСУ ТП.	Нарушение целостности Нарушение доступности	Средняя	Т1.18, Т2.5., Т6.3, Т10.2. Т10.3. Т10.4. Т10.5. Т10.6.	**Актуальна**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
75.	**185**	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний: Н2 Внутренний: Н1	СрЗИ	Осуществление несанкционированного изменения параметров настройки СрЗИ. Обусловлено слабостями мер разграничения доступа к конфигурационным файлам СрЗИ	Возможно при условии получения нарушителем прав доступа к программному интерфейсу управления СрЗИ, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации СрЗИ	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	Средняя	Т1.3, Т1.4, Т1.5, Т2.3, Т2.4, Т2.5, Т3.1, Т4.1, Т4.4, Т6.1, Т6.2, Т6.3, Т6.4, Т6.6, Т7.1, Т10.10	**Актуальна**
76.	187	Угроза несанкционированного воздействия на СрЗИ	Внешний: Н2, Н3 Внутренний:Н2, Н3	СрЗИ	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
77.	188	Угроза подмены ПО	Внутренний: Н2, Н3	Прикладное ПО , сетевое ПО , системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
78.	189	Угроза маскирования действий ВПО	Внешний: Н3	Прикладное ПО , сетевое ПО , системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
79.	191	Угроза внедрения ВПО в дистрибутив ПО	Внешний: Н2 Внутренний: Н1	Прикладное ПО , сетевое ПО , системное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
80.	192	Угроза использования уязвимых версий ПО	Внешний: Н3	Прикладное ПО , сетевое ПО , системное ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
81.	198	Угроза скрытной регистрации ВПО учетных записей администраторов	Внешний: Н3	Система управления доступом, встроенная в ОС компьютера (ПО)	В рамках объекта защиты отсутствует Интернет-соединение	Не рассматривается: неиспользуемые технологии	Не рассматривается: неиспользуемые технологии	Маловероятная	Не рассматривается: неиспользуемые технологии	**Неактуально**
82.	203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внешний: Н2, Н3 Внутренний:Н2, Н3	ПО	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Не рассматривается: недостаточный уровень риска	Маловероятная	Не рассматривается: недостаточный уровень риска	**Неактуально**
83.	**204**	Угроза несанкционированного изменения ВПО значений параметров программируемых логических контроллеров	Внешний: Н3	Аппаратное устройство	Несанкционированное изменение ВПО значений параметров контроля и управления исполнительными устройствами в ПЛК после проникновения и авторизации на данных устройствах.	Возможно при условии, что существует возможность доступа к элементам АСУ ТП	Нарушение целостности	Высокая	Т1.3., Т1.4. Т1.5. Т1.6. Т1.9. Т1.10. Т1.11. Т1.12. Т1.13. Т1.15. Т1.17.	**Актуально**
84.	205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем СрЗИ	Внешний: Н2	Аппаратное устройство, ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
85.	207	Угроза НСД к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)	Внутренний: Н1	Аппаратное устройство, ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
86.	209	Угроза НСД к защищаемой памяти ядра процессора	Внешний: Н2 Внутренний: Н1	Аппаратное устройство	Не рассматривается: недостаточный уровень	Не рассматривается: недостаточный уровень	Не рассматривается: недостаточный уровень	Низкая	Не рассматривается: недостаточный уровень	**Неактуально**

№	№УБИ	Наименование угрозы	Категория и ур. возможностей нарушителей	Объекты воздействия	Уязвимости	Способ реализации угрозы	Негативные последствия	Возможность реализации угрозы	Сценарий реализации угрозы (техники)	Актуальность угрозы
1	2	3	4	5	6	7	8	9	10	11
					возможностей нарушителя для текущего уровне риска	возможностей нарушителя для текущего уровне риска	риска при уровне нарушителя		возможностей нарушителя для текущего уровне риска	
87.	211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого ПО администрирования ИС	Внутренний: Н1	Системное ПО	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Низкая	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
88.	**212**	Угроза перехвата управления ИС	Внутренний: Н2, Н3	Инфраструктура информационных систем	НСД к ресурсам в результате подмены средств централизованного управления объекта защиты или компонентами.	Возможно при условии наличия у нарушителя прав на осуществление взаимодействия со средствами централизованного управления.	Нарушение конфиденциальности Нарушение целостности Нарушение доступности	Средняя	Т1.18, Т2.5., Т6.3, Т10.2. Т10.3. Т10.4. Т10.5. Т10.6.	**Актуально**
89.	214	Угроза несвоевременного выявления и реагирования компонентами ИС (в том числе СрЗИ) на события безопасности информации	Внутренний: Н2, Н3	ПО, каналы связи (передачи) данных	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	Не рассматривается: недостаточный уровень риска при уровне нарушителя	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**
90.	217	Угроза использования скомпрометированного доверенного источника обновлений ПО	Внешний: Н3 Внутренний: Н3	ИС, файлы	В рамках объекта защиты отсутствует Интернет-соединение	Не рассматривается: неиспользуемые технологии	Не рассматривается: неиспользуемые технологии	Маловероятная	Не рассматривается: недостаточный уровень возможностей нарушителя для текущего уровне риска	**Неактуально**

7.2. Возможные сценарии реализации угроз безопасности информации

7.2.1. Определение сценариев реализации угроз

Сценарии реализации УБИ определены для соответствующих способов реализации УБИ применительно к объектам воздействия и видам воздействия на них. Определение сценариев реализации УБИ включает в себя:

- анализ исходных данных, применяемых средств защиты информации, и определение планируемых к применению автоматизированных средств;
- проведение инвентаризации информационных систем и сетей и определение объектов воздействия и их интерфейсов;
- определение внешних интерфейсов, которые могут быть задействованы при реализации УБИ;
- определение внутренних интерфейсов, которые могут быть задействованы при реализации угроз безопасности информации;
- выявление уязвимостей объектов воздействия, а также компонентов систем и сетей, имеющих внешние интерфейсы, с которыми посредством внутренних интерфейсов взаимодействуют объекты воздействия;
- проведение тестирования на проникновение, подтверждающего возможность использования выявленных уязвимостей или выявления новых сценариев реализации угрозы безопасности информации;
- поиск последовательности тактик и техник, применение которых может привести к реализации угрозы безопасности информации, исходя из уровня возможностей актуальных нарушителей, а также результатов инвентаризации, анализа уязвимостей и тестирования на проникновение;
- составление сценариев реализации угрозы безопасности информации применительно к объектам и видам воздействия, а также способам реализации угроз безопасности информации.

Перечень основных тактик и соответствующих им типовых техник, используемых для построения сценариев реализации угроз безопасности информации представлены в таблице 12.

Таблица 12 - Сценарии (способы) реализации угроз

№	Условное обозначение	Основные техники	Примечание	Нарушитель			
				Н1	Н2	Н3	Н4
Т1		Сбор информации о системах и сетях					
Тактическая задача		Нарушитель стремится получить любую техническую информацию, которая может оказаться полезной в ходе реализации УБИ					
1.	Т1.3.	Пассивный сбор информации	Сбор данных о подключенных к сети устройствах		+	+	+
2.	Т1.4.	Направленное сканирование при помощи специализированного ПО подключенных к сети устройств	С целью идентификации сетевых сервисов, типов и версий ПО этих сервисов, а также с целью получения конфигурационной информации компонентов систем и сетей, ПО сервисов и приложений			+	+
3.	Т1.5.	Сбор информации о пользователях, устройствах, приложениях, а также сбор конфигурационной информации компонентов систем и сетей, ПО сервисов и приложений	Поиск и эксплуатация уязвимостей подключенных к сети устройств		+	+	+
4.	Т1.6.	Сбор информации о пользователях, устройствах, приложениях, авторизуемых сервисами вычислительной сети	Путем перебора		+	+	+
5.	Т1.9.	Сбор информации о пользователях, устройствах, приложениях	Поиск информации в памяти, файлах, каталогах, БД, прошивках устройств, репозиториях исходных кодов ПО	+	+	+	+
6.	Т1.10.	Кража цифровых сертификатов, включая кражу физических токенов, либо неавторизованное выписывание новых сертификатов	Возможно после компрометации инфраструктуры доменного регистратора или аккаунта администратора зоны на стороне жертвы		+	+	+
7.	Т1.11.	Сбор информации о пользователях, устройствах, приложениях, внутренней информации о компонентах систем и сетей	При помощи социальной инженерии, в том числе фишинга	+	+	+	+
8.	Т1.12.	Сбор идентификационной информации	Сбор личной идентификационной информации	+	+	+	+
9.	Т1.13.	Сбор информации	Получение доступа к системам физической безопасности и видеонаблюдения		+	+	+
10.	Т1.15.	Поиск и покупка БД идентификационной информации, скомпрометированных паролей и ключей	Реализуется на специализированных нелегальных площадках		+	+	+
11.	Т1.17.	Пассивный сбор и анализ данных телеметрии для получения информации о технологическом процессе, технологических установках, системах и ПО	На предприятиях в АСУ ТП, в том числе на критически важных объектах			+	+
12.	Т1.18.	Сбор и анализ данных о прошивках устройств, количестве и подключении этих устройств, используемых промышленных протоколах для получения информации о технологическом процессе, технологических установках, системах и ПО	На предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах		+	+	+
13.	Т1.19.	Сбор и анализ специфических для отрасли или типа предприятия характеристик технологического процесса для получения информации о технологических установках, системах и ПО	На предприятиях в автоматизированных системах управления производственными и технологическими процессами, в том числе на критически важных объектах		+	+	+
Примечание		Сбор информации может выполняться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно информации для реализации другой тактики в продолжении атаки					
Т2		Получение первоначального доступа к компонентам систем и сетей					
Тактическая задача		Нарушитель, находясь вне инфраструктуры сети или системы, стремится получить доступ к любому узлу в инфраструктуре и использовать его как плацдарм для дальнейших действий					
14.	Т2.2.	Использование устройств, датчиков, систем, расположенных на периметре или вне периметра физической защиты объекта	Для получения первичного доступа к системам и компонентам внутри этого периметра.		+	+	
15.	Т2.3.	Эксплуатация уязвимостей сетевого оборудования и средств защиты вычислительных сетей	Для получения доступа к компонентам систем и сетей при удаленной атаке		+	+	

№	Условное обозначение	Основные техники	Примечание	Нарушитель			
				Н1	Н2	Н3	Н4
16.	Т2.4.	Использование ошибок конфигурации сетевого оборудования и средств защиты, в том числе слабых паролей и паролей по умолчанию	Для получения доступа к компонентам систем и сетей при удаленной атаке		+	+	
17.	Т2.5.	Эксплуатация уязвимостей компонентов систем и сетей	При удаленной или локальной атаке	+	+	+	
18.	Т2.6.	Использование недокументированных возможностей ПО сервисов, приложений, оборудования	Включая использование отладочных интерфейсов, программных, программно-аппаратных закладок	+	+	+	
19.	Т2.8.	Использование методов социальной инженерии, в том числе фишинга	Для получения прав доступа к компонентам системы	+	+	+	
20.	Т2.10.	НСД путем подбора учетных данных сотрудника или легитимного пользователя	Путем подбора учетных данных сотрудника или легитимного пользователя	+	+	+	+
21.	Т2.11.	НСД путем компрометации учетных данных сотрудника организации	В том числе через компрометацию многократно используемого в различных системах пароля	+	+	+	
Примечание		Получение доступа может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки					
Т4		Закрепление (сохранение доступа) в системе или сети					
Тактическая задача		получив доступ к узлу сети с помощью некоторой последовательности действий, нарушитель стремится упростить себе повторное получение доступа к этому узлу, если он ему впоследствии понадобится (например, устанавливает средства удаленного управления узлом, изменяет настройки средств защиты и другие действия)					
22.	Т4.5.	Внесение соответствующих записей в реестр, автозагрузку, планировщики заданий	Обеспечение запуска ВПО при перезагрузке системы или сети	+	+	+	+
23.	Т4.7.	Резервное копирование ВПО в областях, редко подвергаемых проверке	Возможно заражение резервных копий, сохранение образов в неразмеченных областях жестких дисков и сменных носителей	+	+	+	+
Примечание		Закрепление (сохранение доступа в системе) может производиться с использованием одной или более из перечисленных выше техник					
Т5		Управление ВПО и (или) компонентами, к которым ранее был получен доступ					
Тактическая задача		Внедрив ВПО или обеспечив постоянное присутствие на узле сети, нарушитель стремится автоматизировать управление внедренными инструментальными средствами, организовав взаимодействия скомпрометированным узлом и сервером управления, который может быть размещен в сети Интернет или в инфраструктуре организации					
24.	Т5.5.	Управление	Через съемные МНИ		+	+	
25.	Т5.6.	Проксирование трафика управления, дублирование каналов связи, обфускация и разделение трафика управления	Маскировка сетевой активности, обход правил на МСЭ, сокрытие адресов инфраструктуры нарушителей во избежание обнаружения.		+	+	
26.	Т5.7.	Туннелирование трафика управления	Через VPN		+	+	
27.	Т5.8.	Туннелирование трафика управления в поля заполнения и данных служебных протоколов	Возможно туннелирование трафика управления в поля данных и заполнения протоколов DNS, ICMP или другие		+	+	
28.	Т5.9.	Управление через подключенные устройства	Дополнительный канал связи с внешними системами или между скомпрометированными системами в сети		+	+	
29.	Т5.10.	Использование средств обфускации, шифрования, стеганографии	Для сокрытия трафика управления		+	+	
Примечание		Управление ВПО и (или) компонентами, к которым ранее был получен доступ, может производиться нарушителем с использованием одной или более из перечисленных выше техник для управления труднодоступными компонентами или для реализации резервных каналов управления					
Т6		Повышение привилегий по доступу к компонентам систем и сетей					
Тактическая задача		Тактическая задача: получив первоначальный доступ к узлу с привилегиями, недостаточными для совершения нужных ему действий, нарушитель стремится повысить полученные привилегии и получить контроль над узлом					
30.	Т6.2.	Подбор пароля или другой информации	Для аутентификации от имени привилегированной учетной записи		+	+	
31.	Т6.3	Эксплуатация уязвимостей ПО	Уязвимостей ПО к повышению привилегий.		+	+	
32.	Т6.6.	Обход политики ограничения пользовательских учетных записей в выполнении групп операций	Групп операций, требующих привилегированного режима		+	+	
33.	Т6.7.	Использование уязвимостей конфигурации системы, служб и приложений	В том числе предварительно сконфигурированных профилей привилегированных пользователей, автоматически запускаемых от имени привилегированных пользователей скриптов, приложений и экземпляров окружения, позволяющих ВПО выполняться с повышенными привилегиями.		+	+	
34.	Т6.8.	Эксплуатация уязвимостей, связанных с отдельным, и вероятно менее строгим контролем доступа к некоторым ресурсам	Для непривилегированных учетных записей	+	+	+	
Примечание		Повышение привилегий по доступу к компонентам систем и сетей может производиться с использованием одной или более из перечисленных выше техник, пока нарушитель не получит достаточно привилегий для реализации другой тактики в продолжении атаки					
Т7		Сокрытие действий и применяемых при этом средств от обнаружения					
Тактическая задача		Тактическая задача: нарушитель стремится затруднить применение мер защиты информации, которые способны помешать его действиям или обнаружить их					
35.	Т7.2.	Очистка/затирание истории команд и журналов регистрации	Перенаправление записей в журналы регистрации, переполнение истории команд и журналов регистрации, затруднение доступа к журналам регистрации для авторизованных пользователей	+	+	+	
36.	Т7.3.	Удаление файлов, переписывание файлов произвольными данными	И форматирование съемных МНИ	+	+	+	
37.	Т7.4.	Отключение средств защиты от УБИ	В том числе средств антивирусной защиты, механизмов аудита, консолей оператора мониторинга и СрЗИ других типов	+	+	+	
38.	Т7.5.	Отключение систем и средств мониторинга и защиты	От угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса	+	+	+	
39.	Т7.6.	Подделка данных вывода средств защиты от УБИ	Подделка ПО СрЗИ, ВПО	+	+	+	
40.	Т7.7.	Подделка данных телеметрии, данных вывода автоматизированных систем управления, данных систем и средств мониторинга и защиты	От угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности автоматизированной системы управления технологическими процессами и управляемого (контролируемого) объекта и (или) процесса, данных видеонаблюдения и других визуально или автоматически интерпретируемых данных	+	+	+	
41.	Т7.8.	Выполнение атаки отказа в обслуживании на основные и резервные каналы связи	Каналы связи могут использоваться для доставки сообщений о неработоспособности систем или их компонентов или о других признаках атаки	+	+	+	
42.	Т7.9.	Подписание кода	Включая использование скомпрометированных сертификатов авторитетных производителей ПО для подписания модулей ВПО.	+	+	+	
43.	Т7.10.	Внедрение ВПО в доверенные процессы ОС и другие объекты, которые не подвергаются анализу на наличие такого кода	Для предотвращения обнаружения в системе	+	+	+	+
44.	Т7.11.	Модификация модулей и конфигурации ВПО	Для затруднения его обнаружения в системе	+	+	+	+
45.	Т7.13.	Создание скрытых объектов	Скрытых файлов, скрытых учетных записей	+	+	+	
46.	Т7.15.	Внедрение ВПО выборочным/целевым образом на наиболее важные системы или системы, удовлетворяющие определенным критериям	Во избежание преждевременной компрометации информации об используемых при атаке уязвимостях и обнаружения факта атаки	+	+	+	+
47.	Т7.16.	Искусственное временное ограничение распространения или активации ВПО внутри сети	Во избежание преждевременного обнаружения факта атаки.	+	+	+	+

№	Условное обозначение	Основные техники	Примечание	Нарушитель			
				Н1	Н2	Н3	Н4
48.	Т7.17.	Обфускация, шифрование, упаковка с защитой паролем или сокрытие стеганографическими методами программного кода ВПО, данных и команд управляющего трафика	В том числе при хранении этого кода и данных в атакуемой системе, при хранении на сетевом ресурсе или при передаче по сети	+	+	+	+
49.	Т7.19.	Туннелирование трафика управления	Через VPN	+	+	+	
50.	Т7.20.	Туннелирование трафика управления	В поля заполнения и данных служебных протоколов	+	+	+	
51.	Т7.21.	Изменение конфигурации сети	Включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами	+	+	+	
52.	Т7.22.	Подмена и компрометация прошивок	Буткиты	+	+	+	
53.	Т7.23.	Подмена файлов легитимных программ и библиотек	Подмена, реализуемая непосредственно в системе	+	+	+	
54.	Т7.24.	Подмена легитимных программ и библиотек, а также легитимных обновлений ПО	В отношении поставляемых производителем удаленно через сети связи, в репозиториях поставщика или при передаче через сети связи.	+	+	+	
55.	Т7.25.	Подмена ссылок на легитимные программы и библиотеки, а также на легитимные обновления ПО, поставляемые производителем удаленно через сети связи, информации о таких обновлениях	Включая атаки на инфраструктурные сервисы поставщика (такие как DNS hijacking), атаки на третьесторонние ресурсы, атаки на электронную почту и другие средства обмена сообщениями.	+	+	+	
56.	Т7.27.	Компрометация сертификата, используемого для цифровой подписи образа ПО	Включая кражу этого сертификата у производителя ПО или покупку краденого сертификата на нелегальных площадках в сетях связи и подделку сертификата с помощью эксплуатации уязвимостей ПО, реализующего функции генерирования криптографических ключей, хранения и управления цифровыми сертификатами	+	+	+	
57.	Т7.28.	Компрометация средств создания программного кода приложений в инфраструктуре разработчика этих приложений	Для последующего автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы	+	+	+	
58.	Т7.29.	Компрометация средств сборки, конфигурирования и развертывания программного кода, а также средств создания узкоспециализированного кода, в инфраструктуре целевой системы	Для автоматизированного внесения изменений в этот код, устанавливаемый авторизованным пользователем на целевые для нарушителя системы	+	+	+	
Примечание		Сокрытие действий и применяемых при этом средств от обнаружения может производиться с использованием одной или более из перечисленных выше техник для сокрытия разных свидетельств компрометации системы или для более эффективного сокрытия					
Т8		Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям					
Тактическая задача		получив доступ к некоторым узлам инфраструктуры, нарушитель стремится получить доступ к другим узлам. Подобное распространение доступа может быть нецеленаправленным: так, еще не зная, к каким именно компонентам инфраструктуры требуется получить доступ для того, чтобы вызвать нужные ему негативные последствия, нарушитель может стремиться получить контроль над как можно большей частью инфраструктуры систем и сетей					
59.	Т8.5.	Изменение конфигурации сети	Включая изменение конфигурации сетевых устройств, организацию прокси-соединений, изменение таблиц маршрутизации, сброс и модификацию паролей доступа к интерфейсам управления сетевыми устройствами	+	+	+	
60.	Т8.6.	Копирование ВПО	На съемные МНИ	+	+	+	+
Примечание		Получение доступа (распространение доступа) к другим компонентам систем и сетей или смежным системам и сетям может выполняться в несколько шагов с использованием одной или более из перечисленных выше техник, пока нарушитель не достигнет целевой системы или не будет вынужден прибегнуть к другой тактике для продолжения атаки					
Т9		Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз					
Тактическая задача		в ходе реализации угроз безопасности информации, нарушителю может потребоваться получить и вывести за пределы инфраструктуры большие объемы информации, избежав при этом обнаружения или противодействия					
61.	Т9.3.	Вывод информации	На известные порты на внешних серверах, разрешенные на МСЭ	+	+	+	
62.	Т9.5.	Отправка данных	По известным протоколам управления и передачи данных	+	+	+	
63.	Т9.7.	Проксирование трафика передачи данных	Маскировка сетевой активности, обход правил МСЭ, сокрытие адресов инфраструктуры нарушителей во избежание обнаружения.	+	+	+	
64.	Т9.8.	Туннелирование трафика передачи данных	Через VPN	+	+	+	
65.	Т9.9.	Туннелирование трафика управления	В поля заполнения и данных служебных протоколов	+	+	+	
66.	Т9.13.	Вывод информации через предоставление доступа к файловым хранилищам и БД в инфраструктуре скомпрометированной системы или сети,	В том числе путем создания новых учетных записей или передачи данных для аутентификации и авторизации имеющихся учетных записей	+	+	+	+
67.	Т9.14.	Вывод информации на публичных ресурсах	Размещение сообщений или файлов на публичных ресурсах, доступных для анонимного нарушителя	+	+	+	
Примечание		Сбор и вывод из системы или сети информации, необходимой для дальнейших действий при реализации угроз безопасности информации или реализации новых угроз может выполняться с использованием одной или более из перечисленных выше техник для реализации резервных каналов вывода информации					
Т10		НСД и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящие к негативным последствиям					
Тактическая задача		достижение нарушителем конечной цели, приводящее к реализации моделируемой угрозы и причинению недопустимых негативных последствий					
68.	Т10.1.	НСД к информации	В памяти, файловой системе, БД, репозиториях, программных модулях и прошивках	+	+	+	
69.	Т10.2.	Несанкционированное воздействие	На системное ПО, его конфигурацию и параметры доступа	+	+	+	
70.	Т10.3.	Несанкционированное воздействие	На программные модули прикладного ПО	+	+	+	
71.	Т10.4.	Несанкционированное воздействие на программный код, конфигурацию и параметры доступа	Прикладного ПО	+	+	+	
72.	Т10.5.	Несанкционированное воздействие на программный код, конфигурацию и параметры доступа	Системного ПО	+	+	+	
73.	Т10.6.	Несанкционированное воздействие на программный код, конфигурацию и параметры доступа	Прошивки устройства	+	+	+	
74.	Т10.7.	Подмена информации	В памяти или информации, хранимой в виде файлов, информации в БД и репозиториях, информации на неразмеченных областях дисков и сменных МНИ	+	+	+	
75.	Т10.8.	Уничтожение информации	Включая информацию, хранимую в виде файлов, информацию в БД и репозиториях, информацию на неразмеченных областях дисков и сменных МНИ	+	+	+	
76.	Т10.9.	Добавление информации	Включая информацию, хранимую в виде файлов, информацию в БД и репозиториях, информацию на неразмеченных областях дисков и сменных МНИ	+	+	+	
77.	Т10.10.	Организация отказа в обслуживании	В отношении одной или нескольких систем, компонентов системы или сети	+	+	+	
78.	Т10.12.	Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или нарушения функций управления	В том числе на АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов.	+	+	+	
79.	Т10.13.	Несанкционированное воздействие на автоматизированные системы управления с целью вызова отказа или поломки оборудования	В том числе АСУ критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов	+	+	+	

№	Условное обозначение	Основные техники	Примечание	Нарушитель			
				Н1	Н2	Н3	Н4
80.	Т10.14.	Отключение систем и средств мониторинга и защиты от угроз промышленной, физической, пожарной, экологической, радиационной безопасности, иных видов безопасности	В том числе критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов	+	+	+	
Примечание		НСД и (или) воздействие на информационные ресурсы или компоненты систем и сетей, приводящее к негативным последствиям при реализации угроз безопасности информации или реализации новых угроз, может выполняться с использованием одной или более из перечисленных выше техник для повышения эффективности воздействия с точки зрения нарушителя или для реализации нескольких типов воздействия на атакуемую систему				

7.2.2. Актуальные тактики реализации угроз

Ввиду отсутствия на объектах защиты технологий, необходимых к реализации угроз, были признаны неактуальными следующие сценарии:

- Т1.1, Т1.2, Т1.7, Т1.8, Т1.14, Т1.16, Т1.20.
- Т2.1, Т2.7, Т2.9, Т2.12–Т2.14.
- Т3.1–Т3.16.
- Т4.1–Т4.4, Т4.6.
- Т5.1–Т5.4, Т5.11–Т5.13.
- Т6.1, Т6.4, Т6.5, Т6.9.
- Т7.1, Т7.12, Т7.14, Т7.18, Т7.26.
- Т8.1–Т8.4, Т8.7, Т8.8.
- Т9.1, Т9.2, Т9.4, Т9.6, Т9.10, Т9.11, Т9.12.
- Т10.11, Т10.15.

Также были исключены сценарии, для реализации которых отсутствует актуальный нарушитель.

Тактики и сценарии реализации УБИ определены в таблице 12.

Способы реализации УБИ представлены в графе «Способы реализации» таблицы 13.

Таблица 13 - Модель нарушителя

№	Вид нарушителя	Негативные последствия	Мотивация	Объекты воздействия	Способы реализации
1.	Авторизованные пользователи систем и сетей	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ухудшение состояния МНИ – Ошибка в использовании объекта защиты – Простой объекта защиты – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Негативное воздействие на репутацию правообладателя объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	– Получение финансовой или иной материальной выгоды – Любопытство или желание самореализации (подтверждение статуса) – Месть за ранее совершенные действия – Непреднамеренные, неосторожные или неквалифицированные действия	Уровень операторского управления	– Т1.3, Т1.4, Т1.5, Т1.6, Т1.9, Т1.10, Т1.11, Т1.12, Т1.13, Т1.15, Т1.17, Т1.18, Т1.19, – Т2.2, Т2.3, Т2.4, Т2.5, Т2.6, Т2.8, Т2.10, Т2.11, Т4.5. – Т4.7. – Т5.5, Т5.6, Т5.7, Т5.8, Т5.9, Т5.10, – Т6.2, Т6.3, Т6.6, Т6.7, Т6.8, – Т7.2, Т7.3, Т7.4, Т7.5, Т7.6, Т7.7, Т7.8, Т7.9, Т7.10, Т7.11, Т7.13, Т7.15, Т7.16, Т7.17, Т7.19, Т7.20, Т7.21, Т7.22, Т7.23, Т7.24, Т7.25, Т7.27, Т7.28, Т7.29, – Т8.5, Т8.6, – Т9.3, Т9.5, Т9.7, Т9.8, Т9.9, Т9.13, Т9.14, – Т10.1, Т10.2, Т10.3, Т10.4, Т10.5, Т10.6, Т10.7, Т10.8, Т10.9, Т10.10, Т10.12, Т10.13, Т10.14.
2.	Системные администраторы и администраторы безопасности	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ухудшение состояния МНИ – Ошибка в использовании объекта защиты – Простой объекта защиты – Нарушение обслуживания информационной системы – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Негативное воздействие на репутацию правообладателя объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса		Уровень ввода (вывода) данных Уровень автоматического управления Уровень операторского управления	– Т1.3, Т1.4, Т1.5, Т1.6, Т1.9, Т1.10, Т1.11, Т1.12, Т1.13, Т1.15, Т1.17, Т1.18, Т1.19, – Т2.2, Т2.3, Т2.4, Т2.5, Т2.6, Т2.8, Т2.10, Т2.11, Т4.5. – Т4.7. – Т5.5, Т5.6, Т5.7, Т5.8, Т5.9, Т5.10, – Т6.2, Т6.3, Т6.6, Т6.7, Т6.8, – Т7.2, Т7.3, Т7.4, Т7.5, Т7.6, Т7.7, Т7.8, Т7.9, Т7.10, Т7.11, Т7.13, Т7.15, Т7.16, Т7.17, Т7.19, Т7.20, Т7.21, Т7.22, Т7.23, Т7.24, Т7.25, Т7.27, Т7.28, Т7.29, – Т8.5, Т8.6, – Т9.3, Т9.5, Т9.7, Т9.8, Т9.9, Т9.13, Т9.14, – Т10.1, Т10.2, Т10.3, Т10.4, Т10.5, Т10.6, Т10.7, Т10.8, Т10.9, Т10.10, Т10.12, Т10.13, Т10.14.
3.	Отдельные физические лица (хакеры)	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ухудшение состояния МНИ – Ошибка в использовании объекта защиты – Простой объекта защиты	– Получение финансовой или иной материальной выгоды – Любопытство или желание самореализации (подтверждение статуса)	Уровень автоматического управления (средний уровень) Уровень операторского управления Каналы связи	– Т1.3, Т1.4, Т1.5, Т1.6, Т1.9, Т1.10, Т1.11, Т1.12, Т1.13, Т1.15, Т1.17, Т1.18, Т1.19, – Т2.2, Т2.3, Т2.4, Т2.5, Т2.6, Т2.8, Т2.10, Т2.11, Т4.5. – Т4.7. – Т5.5, Т5.6, Т5.7, Т5.8, Т5.9, Т5.10, – Т6.2, Т6.3, Т6.6, Т6.7, Т6.8,

№	Вид нарушителя	Негативные последствия	Мотивация	Объекты воздействия	Способы реализации
		– Нарушение обслуживания информационной системы – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Негативное воздействие на репутацию правообладателя объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса			– T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
4.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ухудшение состояния МНИ – Простой объекта защиты – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Уровень ввода (вывода) данных Уровень автоматического управления Уровень операторского управления Каналы связи	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
5.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы	– Нарушение законодательства Российской Федерации – Ухудшение состояния МНИ – Нарушение обслуживания информационной системы		Уровень операторского управления	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
6.	Разработчики программных, программно-аппаратных средств	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ошибка в использовании объекта защиты – Простой объекта защиты – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Негативное воздействие на репутацию правообладателя объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	– Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. – Получение финансовой или иной материальной выгоды. – Непреднамеренные, неосторожные или неквалифицированные действия	Уровень ввода (вывода) данных Уровень автоматического управления Уровень операторского управления	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
7.	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ухудшение состояния МНИ – Ошибка в использовании объекта защиты – Простой объекта защиты – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	– Получение финансовой или иной материальной выгоды. – Непреднамеренные, неосторожные или неквалифицированные действия.	Уровень ввода (вывода) данных Уровень автоматического управления Уровень операторского управления	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
8.	Поставщики вычислительных услуг, услуг связи	– Нарушение законодательства Российской Федерации – Ошибка в использовании объекта защиты – Простой объекта защиты – Нарушение обслуживания информационной системы – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты	– Получение финансовой или иной материальной выгоды. – Непреднамеренные, неосторожные или неквалифицированные действия.	Каналы связи	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16,

№	Вид нарушителя	Негативные последствия	Мотивация	Объекты воздействия	Способы реализации
		– Негативное воздействие на репутацию правообладателя объекта защиты			T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
9.	Преступные группы (криминальные структуры)	– Причинение ущерба жизни и здоровью людей – Нарушение законодательства Российской Федерации – Порча данных – Ухудшение состояния МНИ – Ошибка в использовании объекта защиты – Простой объекта защиты – Нарушение обслуживания информационной системы – Отказ оборудования – Затраты на восстановление работоспособности объекта защиты – Негативное воздействие на репутацию правообладателя объекта защиты – Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса	Совершение террористических актов, угроза жизни граждан	Уровень ввода (вывода) данных Уровень автоматического управления Уровень операторского управления Каналы связи	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.
10.	Террористические, экстремистские организации			Уровень ввода (вывода) данных Уровень автоматического управления Уровень операторского управления Каналы связи	– T1.3, T1.4, T1.5, T1.6, T1.9, T1.10, T1.11, T1.12, T1.13, T1.15, T1.17, T1.18, T1.19, – T2.2, T2.3, T2.4, T2.5, T2.6, T2.8, T2.10, T2.11, T4.5. – T4.7. – T5.5, T5.6, T5.7, T5.8, T5.9, T5.10, – T6.2, T6.3, T6.6, T6.7, T6.8, – T7.2, T7.3, T7.4, T7.5, T7.6, T7.7, T7.8, T7.9, T7.10, T7.11, T7.13, T7.15, T7.16, T7.17, T7.19, T7.20, T7.21, T7.22, T7.23, T7.24, T7.25, T7.27, T7.28, T7.29, – T8.5, T8.6, – T9.3, T9.5, T9.7, T9.8, T9.9, T9.13, T9.14, – T10.1, T10.2, T10.3, T10.4, T10.5, T10.6, T10.7, T10.8, T10.9, T10.10, T10.12, T10.13, T10.14.

7.3. Перечень актуальных угроз

В ходе оценки УБИ определены возможные УБИ и оценена их актуальность для объекта защиты – актуальные угрозы безопасности информации (таблица 14).

Таблица 14 - Актуальные УБИ

№	№ УБИ	Наименование угрозы
1.	УБИ.006	Угроза внедрения кода или данных
2.	УБИ.022	Угроза избыточного выделения оперативной памяти
3.	УБИ.025	Угроза изменения системных и глобальных переменных
4.	УБИ.069	Угроза неправомерных действий в каналах связи
5.	УБИ.074	Угроза несанкционированного доступа к аутентификационной информации
6.	УБИ.086	Угроза несанкционированного изменения аутентификационной информации
7.	УБИ.091	Угроза несанкционированного удаления защищаемой информации
8.	УБИ.098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб
9.	УБИ.099	Угроза обнаружения хостов
10.	УБИ.103	Угроза определения типов объектов защиты
11.	УБИ.104	Угроза определения топологии вычислительной сети
12.	УБИ.109	Угроза перебора всех настроек и параметров приложения
13.	УБИ.113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
14.	УБИ.116	Угроза перехвата данных, передаваемых по вычислительной сети
15.	УБИ.132	Угроза получения предварительной информации об объекте защиты
16.	УБИ.139	Угроза преодоления физической защиты
17.	УБИ.140	Угроза приведения системы в состояние «отказ в обслуживании»
18.	УБИ.157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
19.	УБИ.169	Угроза наличия механизмов разработчика
20.	УБИ.170	Угроза неправомерного шифрования информации
21.	УБИ.176	Угроза нарушения технологического/производственного процесса из-за временны□х задержек, вносимых средством защиты
22.	УБИ.183	Угроза перехвата управления автоматизированной системой управления технологическими процессами

№	№ УБИ	Наименование угрозы
23.	УБИ.185	Угроза несанкционированного изменения параметров настройки средств защиты информации
24.	УБИ.204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров (далее — ПЛК)
25.	УБИ.212	Угроза перехвата управления ИС

В результате разработки МУ был определен перечень из 25 актуальных угроз безопасности информации, обрабатываемой в АСУ ТП, не связанных с добыванием информации о СКЗИ или непосредственным воздействием на СКЗИ.

Каждая из УБИ, включенных в перечень актуальных УБИ, обрабатываемой в АСУ ТП, должна быть нейтрализована с помощью проведения мероприятий по созданию системы защиты информации.

Для АСУ ТП определены следующие требования по безопасности информации:

— СрЗИ не ниже 6 класса защиты;

— СВТ не ниже 5 класса.

8. Принятые термины, определения и сокращения

В настоящей модели угроз используются следующие термины и определения.

Таблица 15 - Термины и определения

Определение	Пояснение
Автоматизированная система	Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Архитектура систем и сетей	Совокупность основных структурно функциональных характеристик, свойств, компонентов систем и сетей, воплощенных в информационных ресурсах и компонентах, правилах их взаимодействия, режимах обработки информации
Базовый вектор уязвимости	Текстовая формализованная запись (строка), представляющая собой комбинированные данные о базовых метриках (критериях) уязвимости, на основании которой определяется численная базовая оценка уязвимости
Безопасность данных	Состояние защищенности данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность данных при их обработке в информационных системах
Взаимодействующая (смежная) система	Система или сеть, которая в рамках установленных функций имеет взаимодействие посредством сетевых интерфейсов с системой и сетью оператора и не включена им в границу процесса оценки угроз безопасности информации
Вирус (компьютерный, программный)	Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению
Возможности нарушителя	Мера усилий нарушителя для реализации угрозы безопасности информации, выраженная в показателях компетентности, оснащенности ресурсами и мотивации нарушителя
Вредоносная программа	Программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных
Граница оценки угроз безопасности информации	Совокупность информационных ресурсов и компонентов систем и сетей, в пределах которой обеспечивается защита информации (безопасность) в соответствии с едиными правилами и процедурами, а также контроль за реализованными мерами защиты информации (обеспечения безопасности)
Доступ к информации	Возможность получения информации, а также ее использования
Защищаемая информация	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Информационные ресурсы	Информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях. Компонент (системы, сети): программное, программно-аппаратное или техническое средство, входящее в состав систем и сетей
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
Источник угрозы безопасности информации	субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации
Межсетевой экран	Программное средство или аппаратно-программный комплекс, реализующие контроль информации, поступающей в информационную систему и (или) выходящей из информационной системы
Нарушитель безопасности	Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности данных при их обработке техническими средствами в информационных системах
Недекларированные возможности	Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации функциональным возможностям, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
Несанкционированный доступ	Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами
Обеспечивающие системы	Инженерные системы, включающие системы электроснабжения, вентиляции, охлаждения, кондиционирования, охраны и другие инженерные системы, а также средства, каналы и системы, предназначенные для оказания услуг связи, других услуг и сервисов, предоставляемых сторонними организациями, от которых зависит функционирование систем и сетей
Обладатель информации	Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам
Оператор	Лицо, осуществляющее деятельность по эксплуатации систем и сетей, в том числе по обработке содержащейся в них информации
Основные (критические) процессы (бизнес-процессы)	Управленческие, организационные, технологические, производственные, финансово-экономические и иные основные процессы (бизнес-процессы), выполняемые обладателем информации, оператором в рамках реализации функций (полномочий) или осуществления основных видов деятельности, нарушение и (или) прекращение которых может привести к возникновению рисков (ущербу)
Пользователь	Лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в системе или сети и использующее результаты ее функционирования
Программно-аппаратное средство	Устройство, состоящее из аппаратного обеспечения и функционирующего на нем программного обеспечения, участвующее в формировании, обработке, передаче или приеме информации
Программное (программно-математическое) воздействие	Несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ
Средства вычислительной техники	Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем
Средства шифрования	Аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении
Субъект доступа (субъект)	Лицо или процесс, действия которого регламентируются правилами разграничения доступа
Угроза безопасности информации	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. Уязвимость: недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(-ая) может быть использован(а) для реализации угроз безопасности информации

В настоящей МУ используются следующие сокращения.

Таблица 16 - Термины и сокращения

Сокращение	Термин
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АСТУ	Автоматизированная система телеконтроля и управления
АСУ	Автоматизированная система управления
АСУ	Автоматизированная система управления технологическими процессами

Сокращение	Термин
БД	База данных
БДУ	Банк данных угроз
ВПО	Вредоносное программное обеспечение (вредоносный код)
ДЦ	Диспетчерский центр
ЗИ	Защита информации
ЗРУ	Закрытое распределительное устройство
ИБ	Информационная безопасность
ИС	Информационная система
КЗ	Контролируемая зона
МНЭ	Машинный носитель информации
МСЭ	Межсетевой экран/Межсетевое экранирование
МУ	Модель угроз
НДВ	Недокументированные (недекларированные) возможности
НСД	Несанкционированный доступ
Общество	ПАО «Россети Московский Регион»
ОИК	Оперативно-информационный комплекс
ОС	Операционная система
ПЛК	Программируемый логический контроллер
ПО	Программное обеспечение
ПП	Переходной пункт
ПС	Подстанция электрическая
РЗА	Релейная защита и автоматика
СВТ	Средство вычислительной техники
СКЗИ	Средства криптографической информации
СрЗИ	Средства защиты информации
ТМ	Система сбора и передачи информации
ТИ	Телеизмерения
ТМ	Телемеханика
ТС	Телесигнализация
ТТ	(Измерительный) трансформатор тока
ТУ	Телеуправление
УБИ	Угрозы безопасности информации
ФСБ	Федеральная служба безопасности Российской Федерации
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации
ЦСПИ	Цифровая система передачи информации

Приложение 2 тому проектной документации
6350-25-ИОС5.3

Руководящие указания по риск-ориентированному управлению объектами информационной инфраструктуры (ИТТ активами), организации в рамках процесса эксплуатации установки критических обновлений ПО для объектов

Москва 2025 г.

Содержание

1. Назначение ... 3
2. Общие положения ... 4
3. Описание процесса эксплуатации установки критических обновлений ... 5
   3.1. Блок-схема процесса эксплуатации установки критических обновлений ... 5
   3.2. Определение доступных обновлений ПО ПС ... 7
   3.3. Создание резервной (архивной) копии информационной системы объекта ПС ... 7
   3.4. Работы по эксплуатации установки критических обновлений ПО ПС на тестовом стенде ... 7
   3.5. Установка критических обновлений на резервном устройстве ... 8
   3.6. Тестирование критических обновлений на совместимость на резервном устройстве, проверка работоспособности ... 8
   3.7. Анализ рисков влияния критических обновлений на бизнес-процессы ... 9
   3.8. Перевод резервного устройства системы в проектный режим работы ... 9
   3.9. Внесение изменений в рабочую (эксплуатационную) документацию ... 9
4. Термины и определения ... 10
5. Обозначения и сокращения ... 11

1. Назначение

Настоящий документ определяет указания по риск-ориентированному управлению объектами информационной инфраструктуры организации в рамках процесса эксплуатации установки критических обновлений программного обеспечения (далее — ПО) ПС 220 Кв Мельниково (далее — ПС).

Владельцем ПС является ПАО «Россети Московский регион», которое определяет участников процесса эксплуатации установки критических обновлений ПО, зоны их ответственности, типовые процедуры по установке критических обновлений ПО, выполняемые структурными подразделениями.

Настоящие руководящие указания предназначены для использования при разработке и реализации мероприятий по установке критических обновлений ПО на ПС ПАО «Россети Московский регион» в соответствие правовым нормативным актам, методическим документам, отраслевым стандартам в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, обеспечения безопасности объектов ТЭК, а также ЛНА ПАО «Россети Московский регион», определяющим процессы обеспечения безопасности информации, обрабатываемой в информационной инфраструктуре (далее — документы, устанавливающие требования по обеспечению безопасности к среде информационной безопасности).

Документ может являться основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности.

2. Общие положения

Установка критических обновлений ПО объектов ПС решает проблемы функциональности, стабильности и безопасности.

Необходимость установки критических обновлений ПО объектов ПС возникает при следующих обстоятельствах:

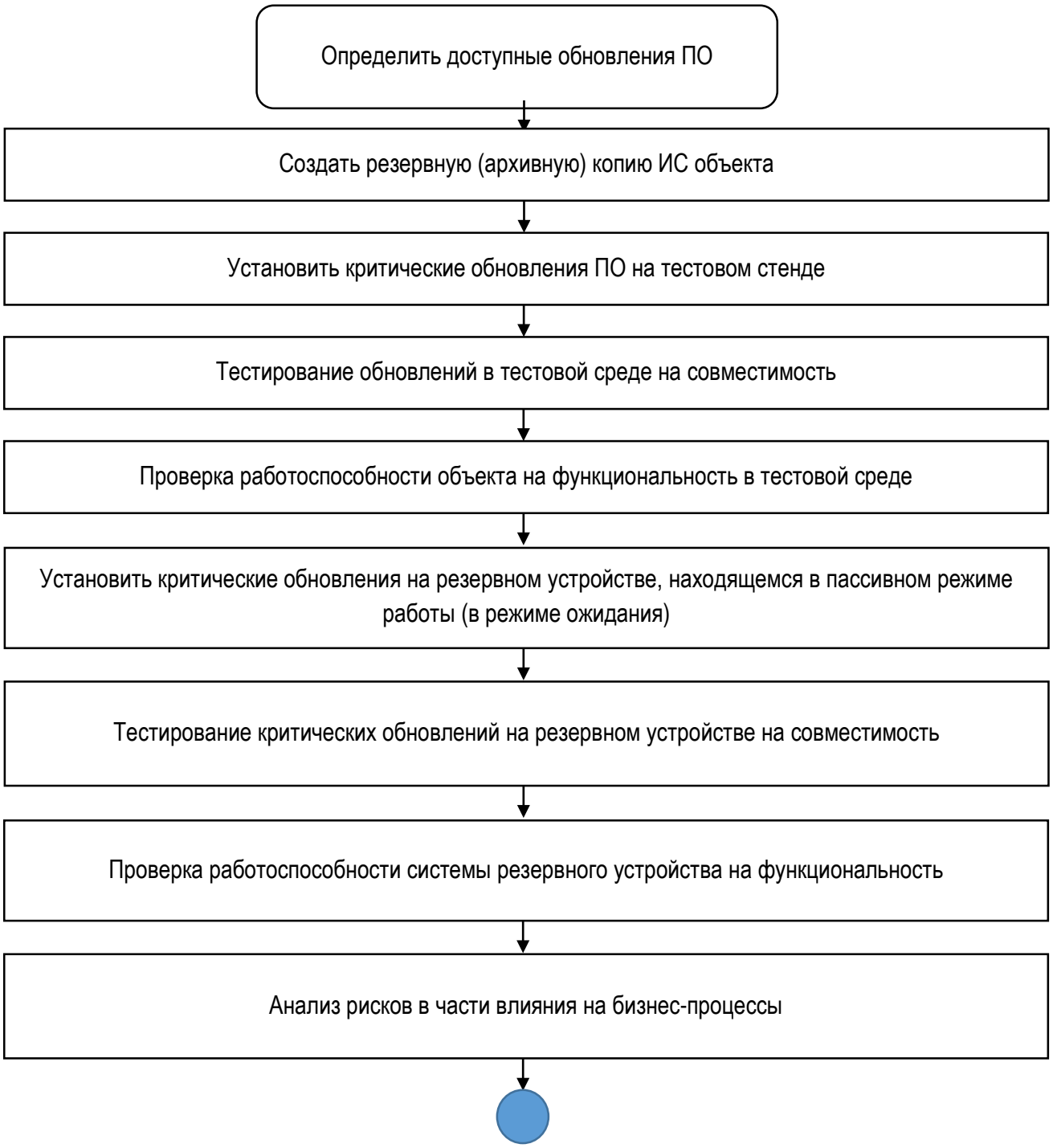
- Появились ошибки в ПО, негативно влияющие на работу объектов ПС в целом;
- Появились новые функциональные возможности применяемого ПО;
- Найдены уязвимости ПО объектов ПС, воспользовавшись которыми злоумышленник способен нанести вред.
- В процессе управления критическими обновлениями ПО объектов ПС могут возникнуть сложности, обусловленные следующими факторами:
- Необходимость непрерывности бизнес-процесса (для установки обновления может потребоваться перезагрузка/выключение объектов ПС);
- Недопустимость автоматического обновления и необходимость предварительного тестирования обновлений в силу критичности ПС;
- Зависимость от разработчика ПО объектов ПС.

Для того, чтобы правильно выстроить процесс эксплуатации установки критических обновлений ПО объектов ПС применяется риск-ориентированный подход.

3. Описание процесса эксплуатации установки критических обновлений

3.1. Блок-схема процесса эксплуатации установки критических обновлений

На рисунке ниже представлена блок-схема процесса эксплуатации установки критических обновлений ПО объектов ПС.



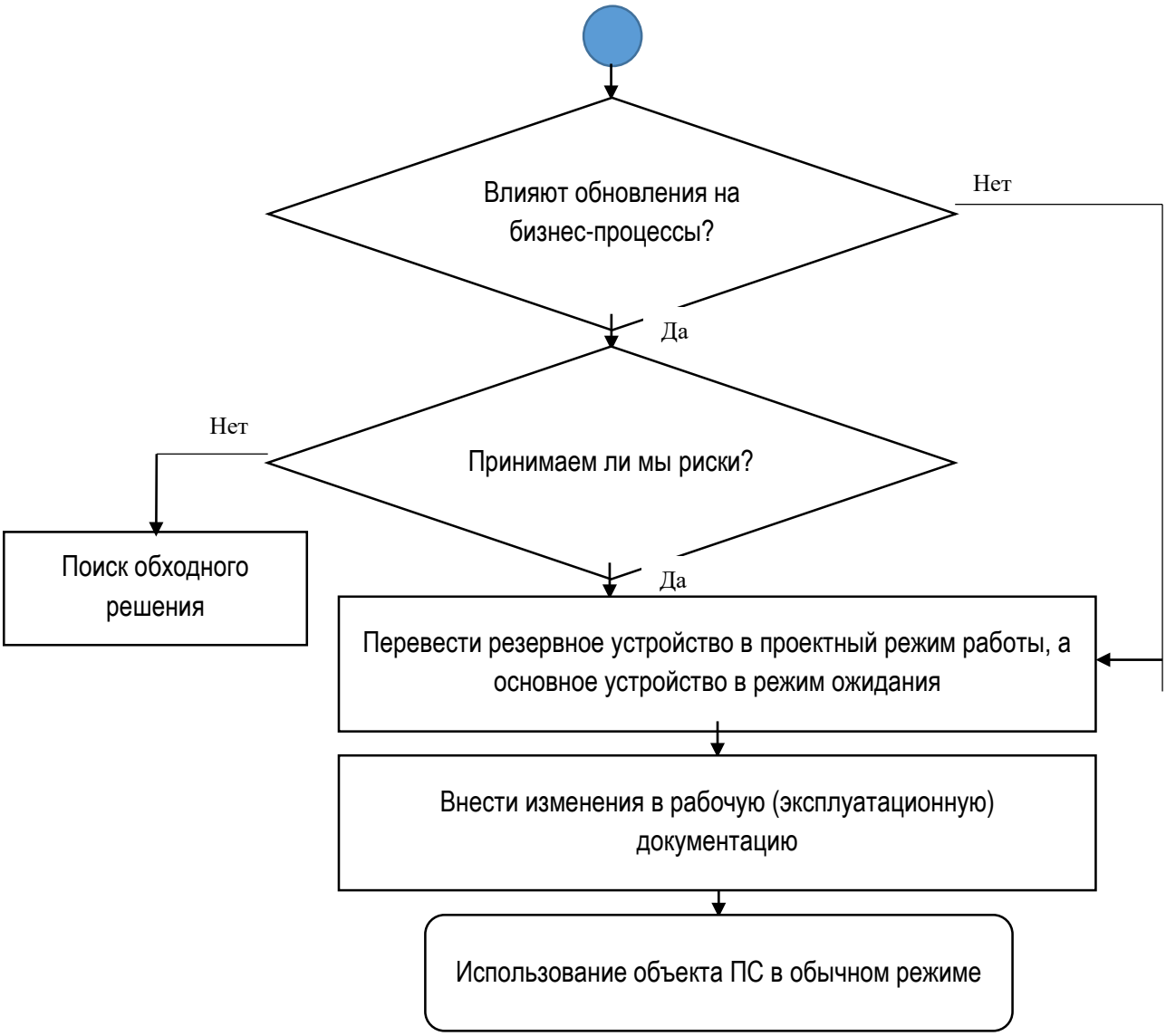


Рисунок 1. Блок-схема процесса эксплуатации установки критических обновлений ПО ПС

3.2. Определение доступных обновлений ПО ПС

При получении сведений о выпущенных обновлениях от производителей ПО объектов ПС (если лицензионное соглашение с производителем ПО предполагает подобное информационное обслуживание), либо сведений полученных самостоятельно путем регулярного мониторинга обновлений принимается решение об актуальности и применимости данных обновлений. Актуальность и применимость обновлений определяется с учетом характеристик программных и аппаратных компонент ПС, а также от степени критичности обновлений, которая присваивается производителем ПО.

В рамках настоящий руководящих указаний, рассматривается процесс управления критическими обновлениями ПО объектов ПС, но описанный подход также применим для установки некритичных обновлений безопасности, релизов накопленных функциональных обновлений ПО.

3.3. Создание резервной (архивной) копии информационной системы объекта ПС

После принятия решения об установке критических обновлений ПО объектов ПС в обязательном порядке создается текущая резервная копия (архив) ИС объекта ПС. Копия должна быть создана до любых действий по установке критических обновлений ПО и представлять собой последний образ функционирующей продуктивной системы соответствующего объекта ПС. Созданная копия ИС объекта ПС должна быть проверена на целостность средствами системы резервного копирования.

Для компонент ПС различаются четыре принципиально разных источника информации, подлежащей резервированию:

- Информация, хранимая и обрабатываемая в СУБД SQL. Объекты ПС: Сервер АСУТП нижнего уровня и сервер баз данных верхнего уровня;
- Информация, хранимая в файлах на серверах и АРМ. Объекты ПС: АРМ ОП, АРМ РЗА, сервера АСУТП, сервера ТМ, терминалы РЗА нижнего уровня;
- Конфигурации терминалов РЗА, сетевого оборудования, межсетевых экранов, систем обнаружения вторжений и иных средств защиты информации ПС;
- Копии виртуальных машин. Объекты ПС: виртуальные машины Сервера баз данных, Сервера приложений и БД АСМДП РЗА ЦОТУ WEB-Сервера, Коммуникационных серверов: коммуникационный сервер ПС; коммуникационный сервер ПС с СО ЕЭС.

Порядок создания резервной (архивной) копии ИС соответствующего объекта ПС в процессе эксплуатации установки критических обновлений ПО должен описываться в эксплуатационной документации или в плане резервного копирования и архивирования.

3.4. Работы по эксплуатации установки критических обновлений ПО ПС на тестовом стенде

В случае использования тестового стенда работы по установке и тестированию критических обновлений ПО ПС сначала проводятся в тестовой среде.

Основная функция тестового стенда заключается в снижении риска потери работоспособности системы до внесения изменений в операционную среду ПС. Дополнительным преимуществом испытательного стенда является возможность обучения оператора новым конфигурациям, разработки контрольных списков и оценки процедур перед развертыванием в производственных системах.

Работы по эксплуатации установки критических обновлений ПС на тестовом стенде проводятся в таком же порядке, что и на резервном устройстве объекта ПС (пп. 1.4, 1.5).

3.5. Установка критических обновлений на резервном устройстве

Установка и тестирование критических обновлений ПО на резервном устройстве объекта ПС является оптимальным вариантом для снижения рисков. Этот сценарий позволяет выполнять процесс установки критических обновлений ПО с незначительным влиянием на бизнес-процессы ПС.

Если определена критичность установки обновлений ПО объекта ПС и требуются незамедлительные действия, следует создать пошаговую процедуру установки критических обновлений (план установки критических обновлений ПО) и произвести установку критических обновлений ПО на резервное устройство объекта ПС. После установки критических обновлений объекта ПС необходимо перейти на этап тестирования, где объекта ПС с установленными критичными обновлениями проверяется на функциональность и совместимость с другими приложениями.

3.6. Тестирование критических обновлений на совместимость на резервном устройстве, проверка работоспособности

Тестирование процесса эксплуатации установки критических обновлений ПО объекта ПС имеет особое значение из-за необходимости поддержания высокой степени отказоустойчивости. Следующие рекомендации должны быть включены в тестирование процесса эксплуатации установки критических обновлений ПО:

- Должно быть выделено резервное устройство (тестовый стенд) для моделирования процесса эксплуатации установки критических обновлений ПО соответствующего объекта ПС;
- Должна быть создана среда тестирования, которая имитирует продуктивную среду и позволяет проводить тестирование на совместимость ПО;
- Должны проводиться плановые тесты, которые подтверждают, что процесс эксплуатации установки критических обновлений ПО устраняет проблемы, выявленные эксплуатирующим подразделением.
- Необходимо провести тесты, чтобы подтвердить, что процесс эксплуатации установки критических обновлений ПО не вызывает конфликтов с существующими приложениями в системе ПС;
- Должны быть разработаны один или несколько типов тестов, которые выполняют функциональные возможности системы (типа объектов ПС), наборы тестов должны храниться в базе знаний.
- Должны быть проведены тесты и написаны процедуры, чтобы убедиться, что установленные критические обновления ПО могут быть удалены без ущерба для операций и работы ПС (некоторые критические обновления ПО могут потребовать немедленного удаления, если тестирование было завершено неуспешно). Процедура отмены установленных критических обновлений ПО может быть довольно сложной, поэтому необходимо разработать план для восстановления критических систем;
- Необходимо провести тесты, чтобы убедиться, что приложение остается работоспособным после установки критических обновлений ПО. Это могут быть приемочные испытания системы, которые используются для проверки работоспособности до возврата в проектный режим работы;
- Контрольные списки и процедуры должны использоваться для процесса эксплуатации установки критических обновлений ПО объектов ПС, чтобы минимизировать риск ошибок работы и обеспечить повторяемость действий процесса эксплуатации установки критических обновлений ПО и его тестирования;
- Записи об установленных критических обновлениях ПО, тестах и изменениях конфигурации должны регистрироваться и документироваться.
- На этапе тестирования критических обновлений ПО на резервном устройстве объекта ПС должен производится мониторинг процессов ПС на наличие неисправностей, не выявленных во время

проведения тестов на тестовом стенде. Время эксплуатации установки критических обновлений ПО на резервном устройстве зависит от сложности бизнес-процессов ПС.

Всегда рекомендуется дублировать операционную среду ПС с абсолютной функциональной точностью, но проблемы, связанные со стоимостью компонент и местом для тестирования, могут ограничивать способность иметь полностью функциональную единицу тестирования. Для некоторых сценариев достаточно моделировать функции ПС без абсолютной точности репликации системы.

Несмотря на то, что рекомендуется иметь резервное устройство объекта ПС, тестирование некоторых компонент ПС может не потребоваться. В этих случаях, должно выполняться резервное копирование (архивирование) продуктивного объекта ПС, который должен быть проверен на возможность восстановления.

3.7. Анализ рисков влияния критических обновлений на бизнес-процессы

На этапе анализа рисков оценивается влияние критических обновлений на процесс функционирования ПС.

Риски определяются с учетом существующих моделей угроз безопасности ПС, при необходимости возможны внесения изменений в модель угроз.

После проведения анализа рисков определяется степень негативного воздействия на бизнес-процессы ПС, если установка критических обновлений приводят к существенным изменениям продуктивной среды ПС, то необходимо искать обходное решение. Это могут быть официальные рекомендации от производителей ПО и средств вычислительной техники, либо выпуск производителем новых версий обновлений, установка которых не повлияет на бизнес-процессы ПС.

В случае, когда принимается решение, что установка обновлений ПО не влияет на бизнес-процессы ПС или оказывает влияние в незначительной степени и отказ компонента ПС маловероятен, то процесс эксплуатации критических обновлений ПО может быть продолжен. Любые изменения конфигурации ПО объекта ПС должны вноситься в рабочую (эксплуатационную) документацию.

3.8. Перевод резервного устройства системы в проектный режим работы

При получении успешных результатов тестирования критических обновлений ПО на резервном устройстве объекта ПС необходимо перевести конфигурацию резервного устройства из пассивного режима работы (режима ожидания) на активный и сохранить состояние продуктивной системы без установленных критических обновлений для аварийного отката системы. Основное устройство при этом перевести в пассивный режим (режим ожидания). Возможные сценарии реагирования на аварийные события должны быть описаны в планах аварийного восстановления.

3.9. Внесение изменений в рабочую (эксплуатационную) документацию

Рабочая (эксплуатационная) документация ПС должна постоянно обновляться.

4. Термины и определения

Активный режим работы	Состояние оборудования, которое включено и подсоединено к телекоммуникационной сети для осуществления обмена информацией.
Операционная среда	Совокупность инструментов, методов их интеграции и приемов работы с ними, позволяющая решать любые задачи в инструментальной области и большинство задач в прикладных областях.
Пассивный режим работы (режим ожидания)	Состояние оборудования, которое включено и подсоединено к телекоммуникационной сети, но не осуществляет обмен информацией.
Приемочные испытания:	Испытания, проводимые с целью окончательной проверки и подтверждения соответствия опытного образца продукции требованиям ТЗ и принятия решения о готовности результатов ОКР к предъявлениям приемочной комиссии для их приемки.
Продуктивная среда	Управляемая среда, содержащая конфигурационные единицы в режиме продуктивной эксплуатации, используемые для предоставления услуг.
Проектный режим работы:	Работа, которая осуществляется, согласно плану, описанию и графику, проектной документацией.
Рабочая (эксплуатационная) документация:	Документация, содержащая сведения, необходимые для выполнения ввода в эксплуатацию и эксплуатации ПС.
Тестирование совместимости:	Тип тестирования, который измеряет степень того, насколько удовлетворительно элемент тестирования может функционировать параллельно с другими независимыми продуктами в общей среде (сосуществование) и, по мере необходимости, обменивается информацией с другими системами или компонентами (функциональная совместимость).
Тестовая среда:	Контролируемая среда, используемая для тестирования конфигурационных единиц, сборок, процессов и т.п.

5. Обозначения и сокращения

ГК:	Группа компаний.
ИБ:	Информационная безопасность.
ИС:	Информационная система.
ИТ:	Информационные технологии.
ЛНА:	Локальные нормативные акты.
ПО:	Программное обеспечение.
СВТ:	Средства вычислительной техники.
ТЗ:	Техническое задание.
ТЭК:	Топливно-энергетический комплекс.

Приложение 3 к тому проектной документации
6350-25-ИОС5.3

Программа информирования и обучения персонала объекта информационной инфраструктуры в области информационной безопасности

Москва 2025 г.

Содержание

1. Цели и правила обучения и подготовки персонала 3
2. Критерии подготовки персонала 4
3. Подготовка и обучение персонала 5
4. Развитие культуры информационной безопасности 6
5. Обучение информационной безопасности персонала организаций, участвующих в стадиях жизненного цикла АСУ ТП ПС 7

1. Цели и правила обучения и подготовки персонала

Цели обучения и подготовка персонала в области информационной безопасности:

- поддержание информированности персонала об угрозах информационной безопасности;
- обеспечение выполнения мер информационной безопасности персоналом ПС.

Правила обучения подготовки персонала ПС в области информационной безопасности таковы:

- для подразделений должна быть разработаны программы обучения и информирования в области информационной безопасности, основанные на функциях и процедурах, выполняемых этими подразделениями;
- программы обучения и информирования должны быть согласованы с группой информационной безопасности, руководителями обучаемых подразделений и утверждены руководством ПС;
- должны быть разработаны программы обучения новых сотрудников в области информационной безопасности;
- сотрудники ПС должен обучаться и информироваться только в той области реализации мер информационной безопасности, в который они непосредственно участвуют;
- знания персонала в области информационной безопасности должны проверяться по итогам проведенного обучения, а также периодически. Сотрудники, показавшие низкие результаты по итогам проверки знаний могут быть отстранены от работы по решению руководителя соответствующего подразделения;
- соответствие мерам информационной безопасности (например, административным мерам, политике чистого стола и т.д.) должно проверяться в ходе аудита учебных курсов.

2. Критерии подготовки персонала

Глубина обучения персонала ПС в области информационной безопасности должна соответствовать категории персонала:

- для сотрудников в области информационной безопасности должно проводиться детальное обучение в области реализации мер информационной безопасности с последующей их практической отработкой на реальном оборудовании на предприятии-изготовителе оборудования, тестовой конфигурации оборудования или с применением виртуальных машин;
- для сотрудников ПС, взаимодействующих с АС (включая комплексы регистрации аварийных процессов, далее — КРАП), должно проводиться обучение по реализации мер информационной безопасности в их зоне ответственности, а также общее информирование об актуальных угрозах информационной безопасности АС;
- для руководства и прочего персонала ПС должно проводиться общее информирование об актуальных угрозах информационной безопасности и мерах их предотвращения.

3. Подготовка и обучение персонала

Таблица 1 показывает формы обучения и информирования руководства и персонала.

Таблица 1 Критерии подготовки персонала

Категория персонала ПС	Формат обучения	Темы обучения
Руководство	– Лекции (информирование). – Симуляции на электронных платформах, практические упражнения	– Актуальные угрозы информационной безопасности АС – Реализация мер информационной безопасности
Группа информационной безопасности	– Лекции (информирование). – Практическое обучение с применением оборудования и ПО. Симуляции на электронных платформах, практические упражнения	– Реализация отдельных мер информационной безопасности в зоне своей ответственности. – Работа с используемыми средствами информационной безопасности, их настройка и администрирование.
Персонал ПС	– Лекции (информирование). – Практическая отработка мер информационной безопасности.	– Актуальные угрозы информационной безопасности АС – Реализация отдельных мер информационной безопасности в зоне своей ответственности. – Действия в случае вербовки.
Прочий персонал ПС	Лекции (информирование)	Актуальные угрозы информационной безопасности АС

4. Развитие культуры информационной безопасности

В связи с тем, что внутренний нарушитель обладает большими возможностями по причинению ущерба АС как намеренного, так и ненамеренного, культура информационной безопасности должна поддерживаться на всех этапах работы персонала на ПС, начиная с приема на работу и заканчивая увольнением или переводом. Каждый сотрудник ПС, взаимодействующий с АС должен обеспечивать компьютерную безопасность АС в рамках своих должностных обязанностей.

5. Обучение информационной безопасности персонала организаций, участвующих в стадиях жизненного цикла АС ПС

Организации, вовлеченные в этапы жизненного цикла АС ПС должны тренировать персонал в области информационной безопасности для:

- поддержания информированности персонала об угрозах информационной безопасности;
- обеспечения выполнения мер информационной безопасности персоналом;
- обеспечение информационной безопасности подсистем и компонентов АС ПС на этапах жизненного цикла.

Программы обучения и информирования в области информационной безопасности должны быть разработаны для групп персонала, основываясь на их функциях и выполняемых ими процедурах.

Должны быть разработаны программы обучения для новых сотрудников.

Знания персонала в области информационной безопасности и результаты обучения должны периодически оцениваться. Сотрудники, показавшие слабые результаты при проверке знаний могут быть отстранены от работы решением руководителя соответствующего подразделения.

Приложение 4 к тому проектной документации
6350-25-ИОС5.3

Расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности, управление средствами защиты информации, управление обновлениями программных и программно-аппаратных средств защиты информации, с учетом особенностей функционирования значимого объекта, мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее — события безопасности), сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документах по безопасности значимого объекта

Москва 2025 г.

Содержание

1. Список сокращений 3
2. Расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности 4
3. Функциональные обязанности 5

1. Список сокращений

ИБ — информационная безопасность

КИИ — критическая информационная инфраструктура

Организация — ПАО «Россети Московский регион»

Система — автоматизированные системы (АС) ПС 220/20 кВ Мельниково.

2. Расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности

Для непрерывного функционирования подсистемы информационной безопасности комплекса необходимо обеспечение подсистемы квалифицированным персоналом в области информационной безопасности.

Также на привлекаемый персонал СОИБ возлагаются функции по исполнению Федерального закона «О безопасности КИИ Российской Федерации» от 26.07.2017 г. №187-ФЗ

В ходе анализа предполагаемых трудозатрат и опроса экспертов по информационным технологиям и информационной безопасности был сформирован базовый состав персонала СОИБ:

- Администратор технических средств — 2 человека;
- Администратор информационной безопасности — 2 человека.

3. Функциональные обязанности

Администратор технических средств:

- Управление (администрирование) СОИБ;
- Обеспечение непрерывного функционирования СОИБ;
- Техническое регламентное обслуживание компонентов СОИБ;
- Обновление компонентов СОИБ;
- Развертывание компонентов СОИБ и их настройка;
- Проведение работ по восстановлению функционирования компонентов СОИБ после сбоев;
- Проведение профилактических работ нацеленных на профилактику сбоев компонентов СОИБ;
- Участие в расследовании инцидентов информационной безопасности;
- Планирование и контроль мероприятий по обеспечению безопасности;
- Проведение работ нацеленных на профилактику инцидентов ИБ;
- Анализ угроз безопасности информации в отношении компонентов Системы и выявление уязвимостей в них;
- Участие в испытаниях Системы и его подсистемы безопасности;
- Участие в категорировании объектов КИИ;

Администратор информационной безопасности:

- Управление (администрирование) СОИБ;
- Мониторинг функционирования компонентов СОИБ;
- Мониторинг событий в СОИБ;
- Добавление объектов мониторинга в СОИБ;
- Добавление источников событий в подсистему регистрации событий информационной безопасности;
- Написание правил корреляции для подсистемы регистрации информационной безопасности;
- Выявление и реагирование на инциденты ИБ;
- Проведение расследований инцидентов;
- Планирование и контроль мероприятий по обеспечению безопасности;
- Проведение работ нацеленных на профилактику инцидентов ИБ;
- Анализ угроз безопасности информации в отношении компонентов Системы и выявление уязвимостей в них;
- Участие в проведении оценки соответствия компонентов Системы требованиям по безопасности;
- Участие в категорировании объектов КИИ.

Приложение 5 к тому проектной
документации 6350-25-ИОС5.3

План мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций

Москва 2025 г.

Содержание

1. Список сокращений 3
2. Общие положения 4
3. Общий порядок действий при возникновении нештатных ситуаций 5
4. Особенности действий при возникновении наиболее распространенных нештатных ситуаций 7
5. Меры против возникновения нештатных ситуаций 10

1. Список сокращений

АС — автоматизированная система

ДП — диспетчерский пункт

ДУ — дистанционное управление

ЛВС — локальная вычислительная сеть

ПО — программное обеспечение

Организация — ПАО «Россети Московский регион»

Система — автоматизированные системы ПС 220 кВ Мельниково.

2. Общие положения

Настоящий План мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций (далее – План) разработан в соответствии с требованиями:

- Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. n 60)».

План мероприятий определяет порядок действий пользователя при возникновении нештатной ситуации при работе с Системой и по реагированию на нештатные ситуации, связанные с работой данной Системы.

В Организации действует «Регламент реагирования на критические угрозы информационной безопасности автоматизированных систем технологического управления ПАО «Россети Московский регион», в случае совпадения ситуаций при которых одновременно должны применяться пункты Регламента и Плана, следует руководствоваться Регламентом.

- Пользователем АС (далее — Пользователь) являются диспетчерский персонал и персонал службы РЗА, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и управления АС, для выполнения своих должностных обязанностей.
- Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под роспись. Пользователь должен быть предупрежден о возможной ответственности за ее нарушение.

3. Общий порядок действий при возникновении нештатных ситуаций

В настоящем документе под нештатной ситуацией понимается происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС, а также с вероятностью потери защищаемой информации.

К нештатным ситуациям относятся следующие ситуации:

- сбой в работе программного обеспечения («зависание» компьютера, сервера, медленная скорость работы программы, ошибки в работе программы и т.п.);
- отключение электричества;
- пожар;
- потоп;
- пандемия;
- сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);
- выход из строя сервера;
- потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);
- обнаружен компьютерный вирус;
- обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);
- взлом системы (web-сервера, файл-сервера и др.) или несанкционированный доступ;
- попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);
- компрометация ключей (утеря носителя ключевой информации (Rutoken, E-token и т. п.), несанкционированный доступ постороннего лица в место физического хранения носителя информации, к устройству хранения информации, визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место, взлом учётной записи пользователя);
- компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);
- физическое повреждение ЛВС или ПЭВМ (не включается ПЭВМ, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);
- стихийное бедствие;
- иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов АС и возможность потери защищаемой информации, и названные таковыми пользователем АС или администратором информационной безопасности ИС.

При возникновении нештатных ситуаций во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно поставить в известность администратора информационной

безопасности. В случае, если поставить в известность администратора не представляется возможным (администратор информационной безопасности отсутствует на рабочем месте), пользователем, обнаружившим нештатную ситуацию, составляется служебная записка в свободной форме с описанием нештатной ситуации, и передается руководителю подразделения.

Администратор безопасности проводит предварительный анализ ситуации и, в случае невозможности исправить положение, ставит в известность своего непосредственного начальника для определения дальнейших действий. Здесь и далее — в случае отсутствия администратора информационной безопасности, все действия и меры в отношении нештатной ситуации, описанные в настоящей инструкции, выполняет сотрудник отдела, временно назначенный начальником отдела, либо сам начальник.

По факту возникновения и устранения нештатной ситуации заносится запись в «Журнал учета нештатных ситуаций ИС, выполнения профилактических работ, установки и модификации программных средств на рабочих станциях и серверах».

При необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

4. Особенности действий при возникновении наиболее распространенных нештатных ситуаций

4.1. Сбой программного обеспечения.

Администратор безопасности совместно с сотрудником отдела, у которого произошла нештатная ситуация, выясняют причину сбоя. Если исправить ошибку своими силами не удалось, разработчику ПО направляется информационное сообщение с сопроводительными материалами о возникшей ситуации.

4.2. Отключение электричества.

Администратор безопасности совместно с сотрудником отдела, у которого произошла нештатная ситуация, проводят анализ на наличие потерь и (или) разрушения данных и ПО, а также проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

4.3. Сбой в работе шифрованных каналов связи.

Администратор безопасности проводит анализ неисправности, работы по восстановлению канала связи, если в ходе анализа устанавливается, что сбой вызван не средствами организации шифрованных каналов связи,

Администратор безопасности информирует дежурного ЦУДОС управления эксплуатации Департамента ИТСиС о неполадках.

4.4. Выход из строя сервера.

Администратор безопасности, ответственный за эксплуатацию сервера, проводит меры по немедленному вводу в действие резервного сервера (если есть) для обеспечения непрерывной работы системы обеспечения информационной безопасности.

При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

4.5. Потеря данных.

При обнаружении потери данных Администратор безопасности проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.

4.6. Обнаружен вирус.

При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области сотрудником. Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны.

После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса.

При обнаружении вируса следует руководствоваться локально-нормативными актами ПАО «Россети Московский регион», инструкцией по эксплуатации применяемого антивирусного ПО.

После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ЭВМ, участвующих в информационном обмене с компонентами Системой с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС). По факту инцидента проводится служебное расследование, данные об инциденте передаются в НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

4.7. Обнаружена утечка информации.

При обнаружении утечки информации ставится в известность Администратор безопасности. Если утечка информации произошла по техническим причинам, проводится анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

По факту инцидента проводится служебное расследование, данные об инциденте передаются в НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

4.8. Взлом системы (Web-сервера, файл-сервера, гипервизора и др.) или несанкционированный доступ (НСД).

При обнаружении взлома сервера ставится в известность Администратор безопасности. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянских закладок. Возможен временный переход на резервный сервер.

Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов-скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий. По результатам анализа ситуации следует проверить вероятность проникновения несанкционированных программ в ЛВС, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ. По факту взлома сервера проводится служебное расследование, данные об инциденте передаются в НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

4.9. Попытка несанкционированного доступа (НСД).

При обнаружении утечки информации ставится в известность Администратор безопасности. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД (данный журнал ведется автоматизированным способом средствами защиты информации от несанкционированного доступа).

По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

По факту инцидента проводится служебное расследование, данные об инциденте передаются НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

4.10. Компрометация ключей.

При обнаружении утечки информации ставится в известность Администратор безопасности и начальник подразделения.

При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

4.11. Компрометация пароля.

При обнаружении утечки информации ставится в известность Администратор безопасности и начальник отдела информационной безопасности ПАО «Россети Московский регион».

При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т.д.).

По факту инцидента проводится служебное расследование, данные об инциденте передаются в НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

4.12. Физическое повреждение ЛВС или ПЭВМ.

Ставится в известность Администратор безопасности, Служба безопасности Организации. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий. Данные об инциденте передаются в НКЦКИ (Национальный координационный центр по компьютерным инцидентам).

4.13. Стихийное бедствие.

При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в учреждении.

5. Меры против возникновения нештатных ситуаций

Администратором безопасности периодически, не реже 1 раза в год, должен проводиться анализ зарегистрированных нештатных ситуаций для выработки мероприятий по их предотвращению.

В общем случае, для предотвращения нештатных ситуаций необходимо четкое соблюдение требований нормативных документов Организации и инструкций по эксплуатации оборудования и ПО.

Рекомендации по предотвращению некоторых типичных нештатных ситуаций:

- Сбой программного обеспечения – применять лицензионное ПО, регулярно проводить антивирусный контроль и профилактические работы на ЭВМ (проверка диска и др.).
- Отключение электричества – использовать источники бесперебойного питания на критически важных технологических участках Министерства.
- Сбой ЛВС – обеспечение бесперебойной работы ЛВС путем применения надежных сетевых технологий и резервных систем.
- Выход из строя серверов – применять надежные программно-технические средства. Допускать к работе с серверным оборудованием только квалифицированных специалистов.
- Потеря данных – периодически проводить анализ системных журналов работы ПО с целью выяснения «узких» мест в технологии и возможной утечки (или потери) информации. Проводить с администраторами информационной безопасности (и сотрудниками) разъяснительные и обучающие собрания. Обеспечить резервное копирование данных.
- Обнаружение вируса – соблюдать требования локально-нормативных актов ПАО «Россети Московский регион».
- Утечка информации – применять средства защиты от НСД. Регулярно проводить анализ журналов попыток НСД и работы по совершенствованию системы защиты информации.
- Попытка несанкционированного доступа (НСД) – по возможности, установить регистрацию попыток НСД на всех технологических участках, где возможен несанкционированный доступ, с оповещением Администратора информационной безопасности о попытках НСД.
- Компрометация паролей – соблюдать требования «Инструкции по организации парольной защиты».
- Физическое повреждение ЛВС или ПЭВМ – физическая защита компонентов сети (серверов, маршрутизаторов и др.), ограничение доступа к ним.
- Стихийное бедствие – проводить обучающие собрания и тренировки персонала по вопросам гражданской обороны.

Приложение 6 к тому проектной документации
6350-25-ИОС5.3

Руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры, в том числе по обеспечению безопасного удаленного мониторинга объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сети субъекта электроэнергетики

Москва 2025 г.

Содержание

1. Обнаружение вторжений 3
1.1. Подсистема обнаружения вторжений 3
1.2. Начальной установка (инсталляция) Подключить аппаратную платформу к сети электропитания. 3
1.3. Настройка сетевого взаимодействия 3
1.4. Настройка общих параметров 5
1.5. Настройка оповещений 6
1.6. Режим IDS (обнаружения вторжений) 8
1.7. Создание учетных записей 9
1.8. Описание процесса настройки 10

1. Обнаружение вторжений

1.1. Подсистема обнаружения вторжений

Настройка СОВ представляет собой интерактивный процесс, в ходе которого производится настройка оборудования и задаются необходимые параметры для нормального функционирования средства в информационной системе.

СОВ обладает интуитивно понятным, структурированным графическим интерфейсом.

Настройка СОВ производится посредством Web-интерфейса при обращении к изделию по его IP-адресу.

1.2. Начальной установка (инсталляция) Подключить аппаратную платформу к сети электропитания.

- Включить тумблер питания на корпусе изделия (при наличии тумблера, зависит от аппаратного исполнения).
- Осуществить подключение сетевого коммутационного кабеля одним концом к коммутатору или компьютеру, используемого для управления СОВ, вторым концом — к устройству, в порт управления (можно выбрать любой из доступных).
- Осуществить назначение сетевого адреса для интерфейса управления.

1.3. Настройка сетевого взаимодействия

При подключении с использованием консольного кабеля (при наличии аппаратной возможности):

- Выполнить вход с систему с реквизитами: имя пользователя: admin, пароль: admin (по умолчанию).

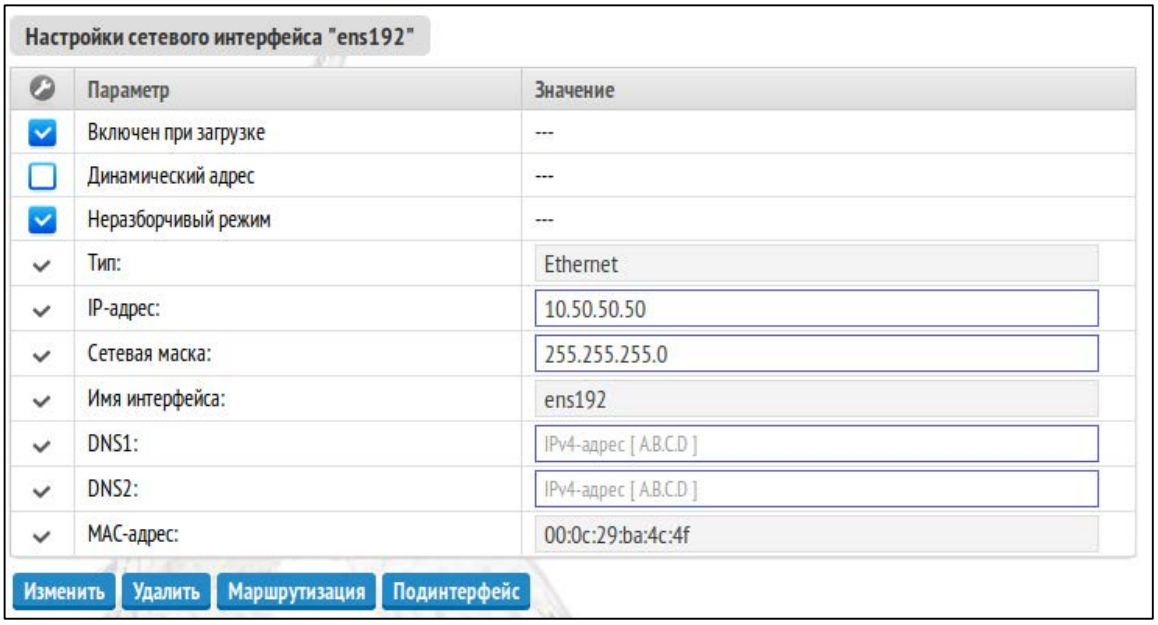
```
IDS-VM-CERT login: admin
Password:
Last login: Fri Oct 19 15:15:00 from 192.168.0.20
KRECHET ADMINISTARTIVE SHELL:
IDS-VM-CERT# _
```

- Выполнить команду: sh.
- Выполнить команду: link.
- В консоль будет выдан перечень сетевых адаптеров, используемых в аппаратной платформе. Определить имя сетевого интерфейса, используемого в последующем в качестве интерфейса управления. При активном соединении в свойствах адаптера будет указан признак "UP". Вернуться в интерфейс командной строки можно по клавише "q".
- Перейти в корень меню, выполнив команду: exit.
- Выполнить команду: conf.
- Выполнить команду: if.
- Выполнить команду: add.
- В строку: "Enter interface:" ввести имя выбранного интерфейса.
- В строку: "Enter IP address to add:" ввести устанавливаемый сетевой адрес в формате: X.X.X.X/YY.

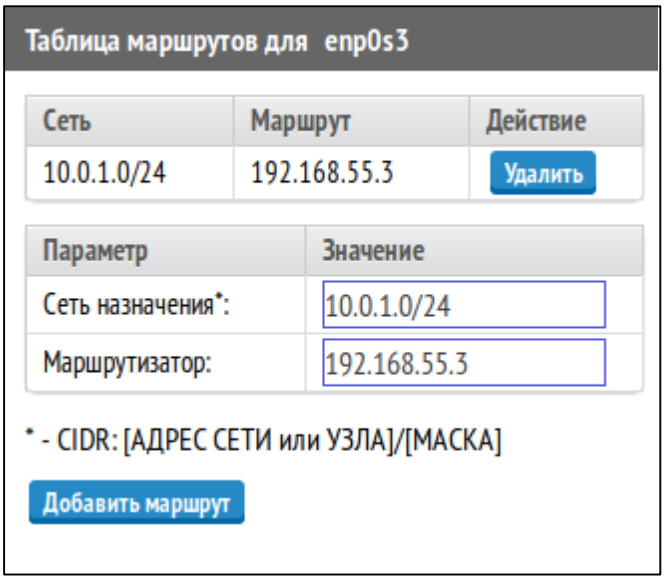
При подключении с использованием предустановленных параметров, в качестве порта управления необходимо выбрать первый сетевой порт устройства.

- Для сетевого адреса, заданного по умолчанию, использовать строку запроса.
- Осуществить вход в систему с использованием имени: admin и пароля: admin.

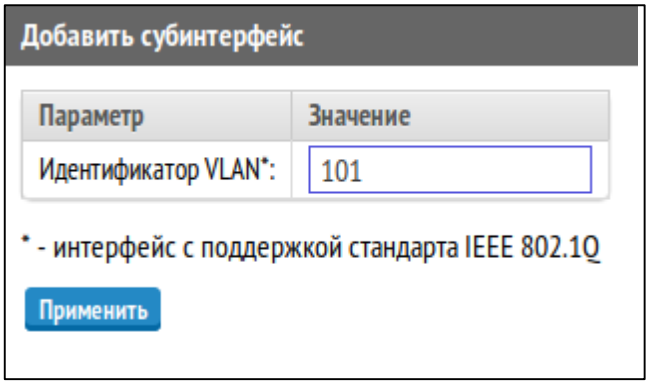
- Утвердить (изменить) настройки интерфейса управления. Перейти на страницу "Администрирование" > "Настройки" > "Общие настройки" > "Сетевые интерфейсы" > [интерфейс управления].
- Выполнить команду "Создать файл конфигурации"
- Осуществить настройку сетевых параметров интерфейса управления, согласно утвержденной адресации:
- Выполнить команду "Изменить". Настройки вступят в силу незамедлительно.
- Определить схему использования Изделия. Осуществить настройку Изделия в соответствии с выбранной схемой. Настройка типовых схем:



На странице настройки сетевого интерфейса прописать статические маршруты для корректной работы в сетях с различной конфигурацией

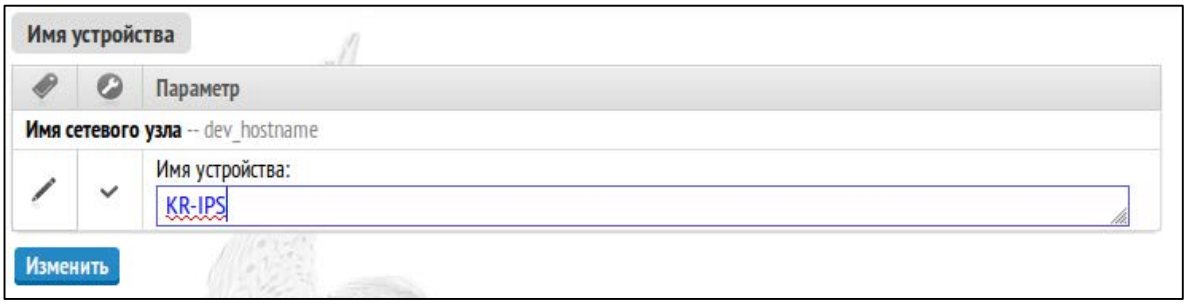


При добавлении к сетевому интерфейсу субинтерфейса (кнопка "Субинтерфейс"), создается программный интерфейс, осуществляющий селекцию по идентификатору VLAN.

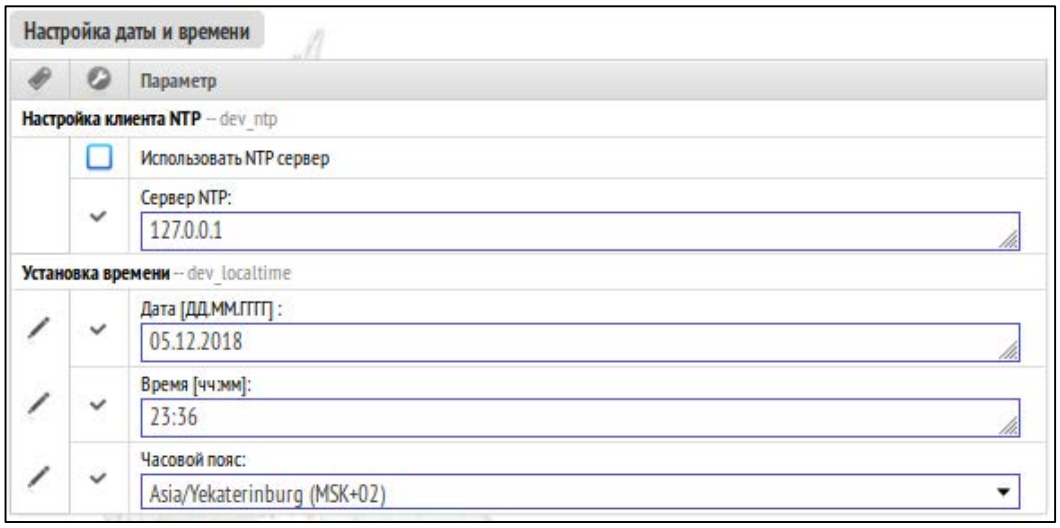


1.4. Настройка общих параметров

Необходимо задать сетевое имя устройства



В пункте «Дата и время» настроить синхронизацию с сервером времени



1.5. Настройка оповещений

Пункт дополнительного меню "Оповещение".

Пункт меню открывает страницу "Оповещение" (см. рисунок 10). На странице можно определить параметры хранения или экспорта регистрируемых событий, а также прочие параметры оповещения уполномоченных лиц о событиях системы, включая звуковую сигнализацию.

Изделие "Кречет" позволяет размещать события, фиксируемые системой, в формате внутренней базы данных и (или) передавать их на внешние хранилища.

Основным форматом экспорта событий системы является формат сообщений syslog. Оператор может определить сетевой адрес, протокол (TCP или UDP) и номер порта, используемые целевым сервером событий. Системные события и события обнаружения анализатора СОВ имеют независимые настройки и могут отличаться.

К системным событиям относятся события, не связанные с функционированием компонентов обнаружения и предотвращения вторжений.

Дополнительно к указанию параметров подключения к серверу событий (syslog-сервер, SIEM-сервер и пр.) оператор должен определить идентификатор, указываемый в каждом сообщении syslog, позволяющий идентифицировать источник событий на приёмной стороне.

Включение и отключение механизма оповещения для всех категорий событий осуществляется посредством изменяемого параметра "Состояние".

Параметр "Время в UTC" определяет формат метки времени, передаваемой совместно с событием. Состояние "включено" для параметра "Время в UTC" задает форматирование метки времени, соответствующее всемирному координированному времени, в противном случае, время в сообщениях указывается по местному времени (с учетом часового пояса), заданному на устройстве.

Параметр "Отправка событий по e-mail" задает конечного адресата и тему сообщения. Отправка электронных сообщений осуществляется в соответствии с задачей "Отправка событий СОВ по электронной почте", определяющей расписание отправки.

Параметр "Звуковая сигнализация" обеспечивает звуковое сопровождение обнаружения сетевой аномалии, угроз, вторжений (требуется аппаратная поддержка: встроенный динамик).

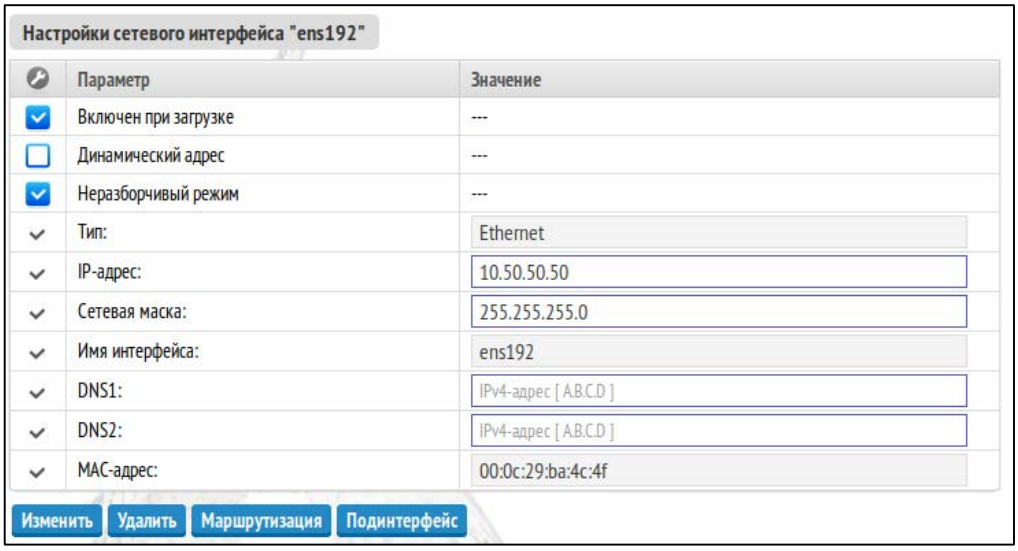
Сохранение событий обнаружения вторжений по умолчанию сохраняется в локальную базу данных. При необходимости, возможно организовать сохранение событий во внешнюю (совместимую) БД. Параметр "Хранить события только локально" раздела "База данных хранения событий анализатора" обеспечивает игнорирование изделием параметров, определяющих адрес и параметры подключения к внешнему серверу БД (не влияет на настройки раздела "Оповещение на события анализатора" и "Передача системных событий по протоколу syslog").

Настройка оповещения

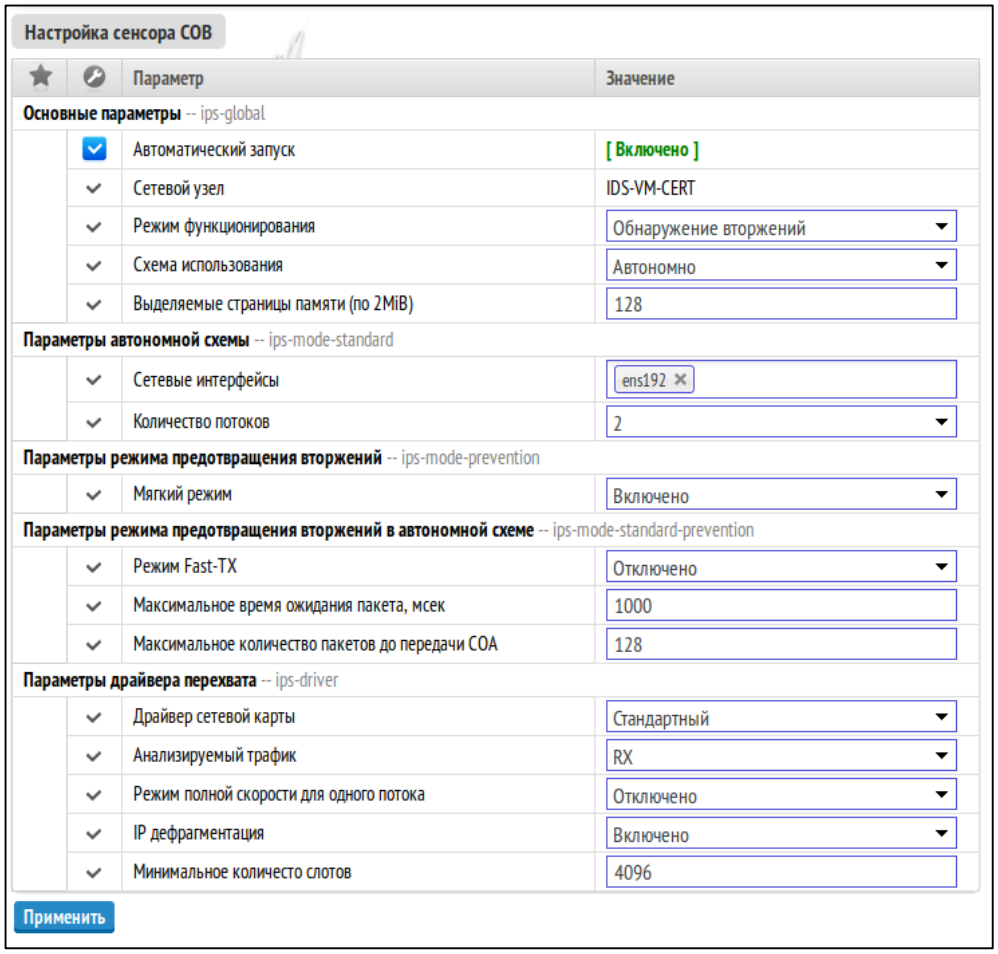
	Параметр
Передача системных событий по протоколу syslog -- log_sys_syslog	
☐	Состояние
✓	Адрес сервера syslog: 172.22.0.100
✓	Порт (UDP/TCP): 514
✓	Идентификатор: krechet-ids
☐	Использовать протокол TCP для syslog
☐	Время в UTC
Оповещение на события анализатора -- log_ids_alert	
☐	Состояние
☐	Передача событий по протоколу syslog
✓	Адрес сервера syslog: 172.22.0.100
✓	Порт (UDP/TCP): 514
✓	Идентификатор: krechet-ids
☐	Использовать протокол TCP для syslog
☐	Звуковая сигнализация
☐	Отправка событий по e-mail (периодичность определяется задачей "Отправка событий СОВ по электронной почте")
✓	Электронный адрес назначения (e-mail): ms@mail.local
✓	Тема письма: События анализатора
☐	Время в UTC
База данных хранения событий анализатора -- log_ids_db	
☑	Состояние
☑	Хранить события только локально
✓	Адрес сервера БД: 127.0.0.1
✓	Порт (TCP): 5432
✓	Имя базы: krechet-ids
✓	Пользователь: admin

1.6. Режим IDS (обнаружения вторжений)

- Осуществить подключение сетевого коммутационного кабеля одним концом к коммутатору в порт, на котором реализовано зеркалирование исследуемого сетевого трафика, другим концом к выбранному свободному порту.
- Настроить порт мониторинг. Установить неразборчивый режим.



Настроить режим работы. Перейти на страницу "Администрирование" > "Настройка" > "СОВ" > "Сенсор" > "Общие параметры".



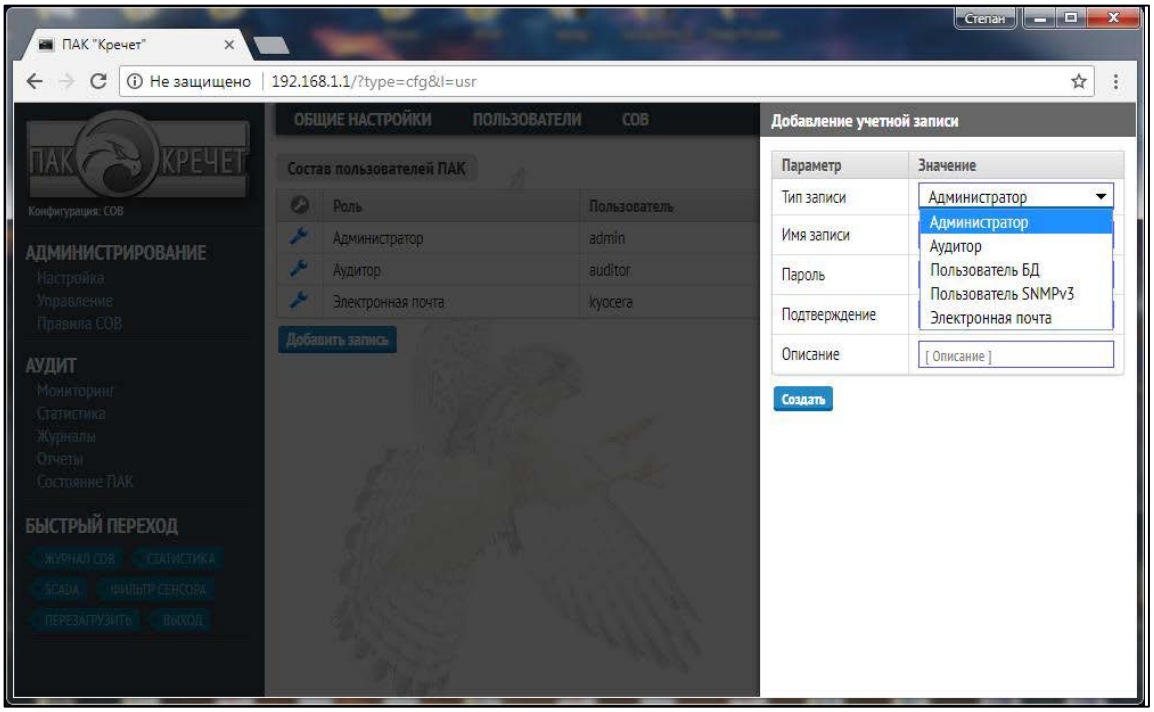
- Задать нужный режим функционирования: Обнаружение вторжений.

- Задать схему использования: Автономно.
- Выбрать интерфейс мониторинга.
- Определить и установить количество потоков обработки (максимальное количество зависит от аппаратного исполнения).
- Установить параметр: "Автоматический запуск".
- Выполнить команду: "Применить".

1.7. Создание учетных записей

Пункт меню открывает страницу "Пользователи" (рисунок 13). На странице существует возможность управления учетными записями пользователей в изделии "Кречет". В системе существуют пять типов (ролей) учетных записей пользователей: Администратор, Аудитор, Пользователь БД, Пользователь SNMPv3, Электронная почта.

- Учетная запись "Администратор" позволяет получить привилегированные полномочия в системе, из-под этой учетной записи производятся все настройки изделия, а так же просматриваются любые журналы регистрируемых событий.
- Учетная запись "Аудитор" позволяет просматривать все регистрируемые события, но не имеет возможности настройки изделия.
- Учетная запись "Пользователь БД" используется для работы с удаленной базой данных на сервере консолидации.
- Учетная запись "Пользователь SNMPv3" используется для аутентификации в рамках реализации протокола SNMPv3.
- Учетная запись "Электронная почта" используется для возможности отправки оповещений по электронной почте.



- Произвести настройку пользователей согласно утвержденных нормативов и стандартов Организации.

1.8. Описание процесса настройки

Дальнейшие действия, связанные с:

- обновлением
- изменение правил
- добавлением дополнительных интерфейсов мониторинга
- работа с журналами и статистикой

Осуществляются согласно руководства администратора, руководства пользователя, принятых нормативных актов Организации.

Экз. № 1

ФЕДЕРАЛЬНАЯ
СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(ФСБ России)
Центр по лицензированию, сертификации и
защите государственной тайны

20.04.2021 № 8/ЛЗ/2/2/1295

107031, г. Москва, ул.Большая Лубянка, д. 2

Генеральному директору
ООО «ИСС»

В.Н.ЗАЙЦЕВУ

117246, г. Москва, Научный проезд, д. 17

О предоставлении лицензии
ООО «ИСС»

Уважаемый Владимир Николаевич!

Уведомляем, что приказом ЦЛСЗ ФСБ России от 16.04.2021 № 218 принято решение о предоставлении лицензии № 18381 Н от 16.04.2021 ООО «ИСС».

Заместитель начальника Центра Д.А. Круглов

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ (ФСТЭК России)

Старая Басманная, д. 17, Москва, 105066
Тел., факс: (495) 696-49-04
E-mail: postin@fstec.ru

04.06.2021 № 240/13/2742

На №_____

Генеральному директору
ООО «Интеллектуальные сети и системы»
В.Н.ЗАЙЦЕВУ
Научный проезд, д. 17, г. Москва, 117246

Уведомление

В соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, приказом ФСТЭК России от 25 декабря 2020 г. № 160дсп и на основании заявления ООО «Интеллектуальные сети и системы» приказом ФСТЭК России от 4 июня 2021 г. № 130-л предоставлена ООО «Интеллектуальные сети и системы» (ИНН 7707754710) лицензия на деятельность по технической защите конфиденциальной информации, регистрационный номер 3916 от 4 июня 2021 г.

Сведения об указанной лицензии размещены на официальном сайте ФСТЭК России в сети Интернет в разделе «Лицензирование», «Техническая защита информации», «Реестры».

Исполняющий обязанности
начальника 1 управления

О.Кузнеченков

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4770

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
2 февраля 2024 г.

Выдан: 2 февраля 2024 г.
Действителен до: 2 февраля 2029 г.

Настоящий сертификат удостоверяет, что **программное средство системы обнаружения вторжений (СОВ) «Кречет»**, разработанное Екатеринбургским НТЦ ФГУП «НПП «Гамма» и производимое ФГУП «НПП «Гамма», является средством обнаружения вторжений уровня сети, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012), при выполнении указаний по эксплуатации, приведенных в формуляре БЮЛИ.00068-02 30 01.

Сертификат выдан на основании технического заключения от 20.12.2023, оформленного по результатам сертификационных испытаний испытательной лабораторией АО «НПО «Эшелон» (аттестат аккредитации от 18.04.2017 № СЗИ RU.0001.01БИ00.Б018), и экспертного заключения от 12.01.2024, оформленного органом по сертификации АО «БИТК» (аттестат аккредитации от 23.05.2016 № СЗИ RU.0001.01БИ00.А003).

Заявитель: ФГУП «НПП «Гамма»
Адрес: 117393, г. Москва, ул. Профсоюзная, д. 78, стр. 4
Телефон: (495) 514-0274

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия,
на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре
средств защиты информации по требованиям безопасности информации

ЗАКЛЮЧЕНИЕ О СОВМЕСТИМОСТИ

Промышленные контроллеры TOPAZ серии MX681 - программное средство системы обнаружения вторжений (СОВ) "Кречет" (далее СОВ "Кречет").

Настоящим заключением компании ООО "ПиЭлСи Технолоджи" и ФГУП "НПП "Гамма", как разработчики и владельцы торговых марок, подтверждают совместимость и работоспособность СОВ "Кречет" производства ФГУП "НПП "Гамма" и промышленных контроллеров TOPAZ серии MX681 производства ООО "ПиЭлСи Технолоджи".

СОВ "Кречет" может быть быть использовано в качестве системы обнаружения вторжений на основе промышленных контроллеров TOPAZ серии MX681. Процедура установки СОВ "Кречет" в промышленные контроллеры TOPAZ серии MX681 производится в соответствии с документацией.

СОВ "Кречет" может применяться при решении задач информационной безопасности автоматизированных систем управления, построенных на основе промышленных контроллеров TOPAZ серии MX681.

Москва / 21 апреля 2021

Генеральный директор
ООО "ПиЭлСи Технолоджи"

_____/Крутских И.В.

Директор Екатеринбургского НТЦ
ФГУП "НПП "Гамма"

_____/Худеньких А.С.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4379

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
22 марта 2021 г.

Выдан: 22 марта 2021 г.
Действителен до: 22 марта 2026 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс ViPNet Coordinator IG 4**, разработанный АО «ИнфоТеКС», производимый АО «ИнфоТеКС» и ООО «Линза», является межсетевым экраном, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа А четвертого класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа Д четвертого класса защиты. ИТ.МЭ.Д4.ПЗ» (ФСТЭК России, 2016) при выполнении указаний по эксплуатации, приведенных в формуляре ФРКЕ.467759.001ФО.

Сертификат выдан на основании технического заключения от 28.12.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 18.02.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-4823*** от "***03***" ***апреля*** 2024 г.

Действителен до "***03***" ***апреля*** 2027 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что **Программно-аппаратный комплекс ViPNet Coordinator IG 4** на аппаратных платформах IG10 I1, IG10 I2, IG100 I1 в комплектации согласно формуляру ФРКЕ.467759.001ФО с учётом извещения об изменении № 2 ФРКЕ.467759.001.FB.2-2021

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 925-000501, 925-000502, 925-000503, 925-000504, 925-000505, 925-000506.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.467759.001ТУ с учётом извещения об изменении № 2 ФРКЕ.467759.001.FB.2-2021, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.467759.001ФО с учётом извещения об изменении № 2 ФРКЕ.467759.001.FB.2-2021.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

ЗАКЛЮЧЕНИЕ О СОВМЕСТИМОСТИ

Промышленные контроллеры TOPAZ серии MX 240, MX 681/ SCADA "TOPAZ SCADA" - продукты ПК ViPNet Client 4, ПАК ViPNet Coordinator HW4, ПАК ViPNet Coordinator IG4

Настоящим заключением компании ООО «ПиЭлСи Технолоджи» и ОАО «ИнфоТеКС», как разработчики и владельцы торговых марок, подтверждают совместимость и работоспособность средств криптографической защиты информации ПК ViPNet Client 4, ПАК ViPNet Coordinator HW4, ПАК ViPNet Coordinator IG4 производства ОАО «ИнфоТеКС» и промышленных контроллеров TOPAZ серии MX 240, MX 681 и SCADA «TOPAZ SCADA» производства ООО «ПиЭлСи Технолоджи».

Программный комплекс ViPNet Client 4 может быть использован в качестве средства криптографической защиты информации при создании шлюзов безопасности и контроллеров в защищенном исполнении на основе промышленных контроллеров TOPAZ серии MX 240, MX 681. Процедура установки в промышленные контроллеры TOPAZ серии MX 240 и MX 681 программного комплекса ViPNet Client 4 производится в соответствии с документацией.

Программно-аппаратные комплексы ПАК ViPNet Coordinator HW4 и ПАК ViPNet Coordinator IG4 могут использоваться в качестве средств криптографической защиты информации и межсетевого экранирования при решении задач информационной безопасности автоматизированных систем управления, построенных на основе промышленных контроллеров TOPAZ серии MX 240, MX 681 и/ или SCADA «TOPAZ SCADA».

Москва / 01 октября 2019

Генеральный директор
ООО "ПиЭлСи Технолоджи"

_____ / Крутских И.В.

Генеральный директор
ОАО "ИнфоТеКС"

_____ / Чапчаев А.А.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер ***СФ/124-5079*** от "***27***" ***декабря*** 2024 г.

Действителен до "***31***" ***декабря*** 2025 г.

Выдан Обществу с ограниченной ответственностью «ТСС».

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) **«Dcrypt 1.0 v.2»** (исполнения: 24, 29, 30) в комплектации согласно формуляру 4012-006-61649217-18 02 30

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 24), класса КС2 (для исполнения 29), класса КС3 (для исполнения 30) и может использоваться для криптографической защиты (шифрование данных, содержащихся в областях оперативной памяти, и сетевого трафика, вычисление имитовставки для данных, содержащихся в областях оперативной памяти, и сетевого трафика, вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «Центр сертификационных исследований»

сертификационных испытаний образцов продукции № 852Н1-000501 (для исполнения 24), № 852П1-000501 (для исполнения 29), № 852Р1-000501 (для исполнения 30).

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру 4012-006-61649217-18 02 30.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

105187, г. Москва,
ул. Борисовская, д.1, офис 900.
Тел., факс: +7 (495) 120-12-84.
E-mail: info@tssltd.ru.

Юр. адрес: 117449, г. Москва,
ул. Винокурова, д.3.
Факт. адрес: 117246, г. Москва,
Научный проезд, д.17.
Тел. (495)139-04-05,
(495)139-04-06.
E-mail: sales@tpz.ru

04.04.2023 г.

ЗАКЛЮЧЕНИЕ О СОВМЕСТИМОСТИ

Настоящим заключением компании ООО «ТСС» и ООО «ПиЭлСи Технолоджи», как разработчики и владельцы торговых марок, подтверждают совместимость и работоспособность средств криптографической защиты информации (далее – СКЗИ) продуктов серий «Dcrypt», «Diamond VPN/FW» производства ООО «ТСС», и промышленных контроллеров TOPAZ и SCADA «TOPAZ SCADA», производства ООО «ПиЭлСи Технолоджи».

Продукты серии «Dcrypt» могут быть использованы в качестве СКЗИ при создании шлюзов безопасности и промышленных контроллеров в защищенном исполнении на основе промышленных контроллеров TOPAZ. Процедура установки в промышленные контроллеры TOPAZ СКЗИ серии «Dcrypt» производится в соответствии с документацией на изделие и не требует проведения дополнительных проверок корректности встраивания.

Программно-аппаратные комплексы «Diamond VPN/FW» могут использоваться в качестве средств криптографической защиты информации для автоматизированных систем управления, построенных на основе промышленных контроллеров TOPAZ и/или SCADA «TOPAZ SCADA».

Генеральный директор
ООО «ТСС»

Шарапов И.М.

Генеральный директор
ООО «ПиЭлСи Технолоджи»

Крутских И.В.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4541

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
6 мая 2022 г.

Выдан: 6 мая 2022 г.
Действителен до: 6 мая 2027 г.

Настоящий сертификат удостоверяет, что **программное обеспечение «Технологическая операционная система «Topaz Linux»**, разработанное и производимое ООО «ПиЭлСи Технолоджи», является операционной системой, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016), «Профиль защиты операционных систем типа Б четвертого класса защиты. ИТ.ОС.Б4.ПЗ» (ФСТЭК России, 2017) и задании по безопасности 643.89466010.00001-01 ЗБ 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.89466010.00001-01 30 01.

Сертификат выдан на основании технического заключения от 03.11.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), и экспертного заключения от 21.12.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: ООО «ПиЭлСи Технолоджи»
Адрес: Научный проезд, д. 17, г. Москва, 117246
Телефон: 495 510-4961

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия,
на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре
средств защиты информации по требованиям безопасности информации

РОССИЙСКАЯ ФЕДЕРАЦИЯ

СВИДЕТЕЛЬСТВО

о государственной регистрации программы для ЭВМ

№ 2012619552

TOPAZ

Правообладатель(ли): ***Общество с ограниченной ответственностью «ПиЭлСи Технолоджи» (RU)***

Автор(ы): ***Не указаны***

Заявка № **2012617143**

Дата поступления **23 августа 2012 г.**

Зарегистрировано в Реестре программ для ЭВМ

22 октября 2012 г.

Руководитель Федеральной службы по интеллектуальной собственности

Б.П. Симонов

СОГЛАСОВАНО
Первый заместитель директора –
главный диспетчер
Филиала АО «СО ЕЭС» Московское РДУ

_____ **А.С. Куделин**
(подпись) (ФИО)

16.08.2024

УТВЕРЖДАЮ
Первый заместитель генерального
директора – главный инженер ПАО
«Россети Московский регион»

_____ **Д.Б. Гвоздев**
(подпись) (ФИО)

Идентификационный номер специалиста

П	**И**	**-**	**1**	**2**	**2**	**5**	**1**	**8**

№153-13/ГД/02/ВН-1454 от 19.08.2024

Задание на проектирование

по титулу «Строительство ПС 220/20 кВ Мельниково»

АДРЕС на территории ПС 220 кВ Молжаниновка
(г. Москва, Новосходненское шоссе, д.80)

ПРОЕКТНАЯ ОРГАНИЗАЦИЯ

_____
(наименование организации)

_____
(должность)

_____
(Ф.И.О.)

_____
(подпись)

«_____»_____ 20__ г.

М.П.

ГИП _____ _____
(Ф.И.О.) (подпись)

Идентификационный номер специалиста

Москва 2024 г.

1. Основание для проектирования

1.1. Инвестиционная программа ПАО «Россети Московский регион», утвержденная приказом МЭ РФ от 22.12.2023 года №31@ «Об утверждении изменений, вносимых в инвестиционную программу ПАО «Россети Московский регион» на 2023 – 2027 годы, утвержденную приказом Минэнерго России от 24.11.2022 № 30@», а также текущий проект ее корректировки.

1.2. Регламент подготовки, согласования и утверждения ТУ, ЗП и ПСД на сооружение, техническое перевооружение и реконструкцию объектов ПАО «Россети Московский регион» и объектов сторонних организаций, связанных с объектами ПАО «Россети Московский регион» (далее – регламент) в действующей редакции.

1.3. Технические условия на технологическое присоединение к электрическим сетям ПАО «Россети Московский регион» энергопринимающих устройств ОАО «РЖД» № И-24-00-223309/125 к договору о технологическом присоединении от 15.06.2023 № ИА-23-302-15007(624621).

2. Нормативно-технические документы, определяющие требования к оформлению и содержанию проектной документации.

НТД указаны в приложении 1 к типовому заданию на проектирование ПАО «Россети», утвержденного распоряжением ПАО «Россети» от 17.11.2017 № 628р. Также необходимо учесть следующие НТД:

- «Правила технологического функционирования электроэнергетических систем» утвержденные постановлением Правительства РФ от 13.08.2018 №937.
- ПНСТ 283-2018 «Трансформаторы измерительные. Часть 2. Технические условия на трансформаторы тока», утвержденный и введенный в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30.10.2018 №51-пнст.
- ГОСТ Р 58669-2019 «Единая энергетическая система и изолированно работающие энергосистемы. Релейная защита. Трансформаторы тока измерительные индуктивные с замкнутым магнитопроводом для защиты. Методические указания по определению времени до насыщения при коротких замыканиях».
- Требования к обеспечению надежности электроэнергетических систем, надежности и безопасности объектов электроэнергетики и энергопринимающих установок «Методические указания по устойчивости энергосистем», утвержденные Приказом Министерства энергетики РФ от 03.08.2018 №630.
- Методические указания по проектированию энергосистем, утвержденные приказом Минэнерго России от 06.12.2022 № 1286 «Об утверждении Методических указаний по проектированию развития энергосистем и о внесении изменений в приказ Минэнерго России от 28 декабря 2020 г. № 1195.
- ГОСТ Р 71170-2023 «Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Проверка соответствия номинального тока отключения выключателей 110 кВ и выше расчетным уровням токов короткого замыкания. Нормы и требования».
- Приказ Министерства Энергетики Российской Федерации от 13.02.2019 №101 «Об утверждении требований к оснащению линий электропередачи и оборудования объектов электроэнергетики классом напряжения 110 кВ и выше устройствами и комплексами релейной защиты и автоматики, а также к принципам функционирования устройств и комплексов релейной защиты и автоматики».

− Приказ Министерства Энергетики Российской Федерации от 13.02.2019 №97 «Об утверждении требований к каналам связи для функционирования релейной защиты и автоматики».

− Приказ Министерства Энергетики Российской Федерации от 13.02.2019 №100 «Об утверждении правил взаимодействия субъектов электроэнергетики, потребителей электрической энергии при подготовке, выдаче и выполнении заданий по настройке устройств релейной защиты и автоматики».

− «Порядок раскрытия цифровых информационных моделей электроэнергетических систем и предоставления системным оператором иным субъектам электроэнергетики, потребителям электрической энергии и проектным организациям перспективных расчетных моделей электроэнергетических систем или фрагментов таких моделей для целей перспективного развития электроэнергетики», утвержденный приказом Министерства энергетики Российской Федерации от 17.02.2023 № 82.

При проектировании необходимо руководствоваться последними редакциями документов, необходимых и действующих на момент разработки документации, в том числе не указанных в данном приложении.

3. Заказчик

«Московские высоковольтные сети» – филиал ПАО «Россети Московский регион».

4. Проектная организация (генеральный проектировщик)

Определяется по итогам конкурса (торгово-закупочных процедур по выбору подрядной организации на выполнение ПИР).

5. Сроки начала и окончания проектирования

Начало - с момента заключения договора на выполнение ПИР.

Окончание – сроки окончания договора ПИР.

6. Вид строительства и этапы разработки проектной документации.

6.1. Вид строительства: реконструкция.

6.2. До начала разработки проектной документации Проектировщик разрабатывает и согласовывает с Заказчиком состав проекта, в соответствии с которым осуществляется дальнейшее проектирование и приемка выполненных работ.

6.3. Этапы разработки документации:

− **Выбор оптимального варианта проектирования** – разработка и рассмотрение 2-3 вариантов проектирования на соответствие объемов реконструкции объемам, указанным в задании на проектирование, на корректность и реализуемость предлагаемых технических решений, на применимость выбранного оборудования, а также анализ технико-экономического сопоставления предложенных вариантов проектирования.

− **ОТР** - разработка, обоснование и согласование с ПАО «Россети Московский регион», собственниками объектов, технологически связанных с объектом проектирования и Филиалом АО «СО ЕЭС» Московское РДУ (далее – Московское РДУ) основных технических решений (ОТР) по проектируемому объекту (в сроки, установленные соответствующим договором).

− **ПД** - разработка, согласование с ПАО «Россети Московский регион»,

собственниками объектов, технологически связанных с объектом проектирования, Московским РДУ и сопровождение подрядчиком прохождения экспертизы проектной документации в соответствии с требованиями нормативно-технических документов; обеспечение подрядчиком получения положительного заключения государственной/негосударственной экспертизы проектной документации (ПД), результатов инженерных изысканий и заключения о достоверности определения сметной стоимости объекта.

− **РД** - разработка и согласование с ПАО «Россети Московский регион», собственниками объектов, технологически связанных с объектом проектирования и Московским РДУ рабочей документации (РД) в соответствии с требованиями нормативно-технических документов.

Основные технико-экономические показатели

Принять по утверждённым прогрессивным технико-экономическим показателям, нормам и аналогам. Предусмотреть мероприятия по снижению материалов и энергоёмкости, трудовых и финансовых затрат.

Проектно-сметная документация должна быть разделена на мероприятия, учтенные и не учтенные укрупненными нормативами цен.

Объем финансовых потребностей мероприятий, учтенных укрупненными нормативами цен, необходимых для выполнения работ по строительству (реконструкции) в сводно-сметном расчете, не должен превышать объема финансовых потребностей для данных мероприятий, рассчитанных в соответствии с Приказом Министерства энергетики Российской Федерации от 17.01.2019 №10 «Об утверждении укрупненных нормативов цены типовых технологических решений капитального строительства объектов электроэнергетики в части объектов электросетевого хозяйства».

7. Основные характеристики проектируемого объекта.

7.1. В части ПС:

Наименование мероприятия	**Технологические решения**
Номинальные напряжения (высший класс напряжения), кВ	220 кВ
Количество резервных ячеек по каждому РУ	0 резервных ячеек 220 кВ 0 резервных ячеек 20 кВ
Выделение этапов реконструкции	Без этапов
Общие требования к оборудованию ПС	1. Применяемое оборудование должно быть аттестовано в ПАО «Россети», соответствовать требованиям технической политики ПАО «Россети», Приказа ПАО «Россети» от 29.03.2019 №64 «Об утверждении стандартов организации», Распоряжения ПАО «Россети» от 19.03.2018 №106р «Об утверждении технических требований к компонентам цифровой

Наименование мероприятия	Технологические решения
	сети» и Методических указаний ПАО «Россети Московский регион», Российским стандартам и быть сертифицированными в установленном порядке. 2. Выключатели 20 кВ: 2.1. привод выключателей должен быть энергонезависимым и запитан от СОПТ; 2.2. выключатели 20 кВ должны быть вакуумные; 2.3. рассмотреть возможность оснащения автоматизированной системой мониторинга и диагностики (коммутационный ресурс и др.). 3. Силовые трансформаторы: 3.1. Установка трансформаторов должна быть с применением поворотных катков с ребордой. 3.2. Уклон крышки бака должен быть заложен в конструкцию трансформатора. 3.3. Конструкция трансформатора должна обеспечить отсутствие необходимости подпрессовки обмоток и магнитопровода на весь срок службы трансформатора. 3.4. При изготовлении трансформатора применять технологии и материалы, влияющие на потери в сторону уменьшения; 3.5. Трансформатор должен быть оборудован: 3.5.1. необслуживаемыми воздухоосушителями; 3.5.2. автоматическими предохранительными клапанами с контактным устройством сигнализации срабатывания; 3.5.3. переключателем РПН вакуумного исполнения обладающим повышенным коммутационным ресурсом до первой ревизии не менее 300 000 переключений. 3.5.4. приводом РПН на виброгасителях; 3.5.5. пластинчатыми радиаторами системы охлаждения с противокоррозионным покрытием; 3.5.6. уплотняющей резиной со сроком службы не менее 30 лет; 3.5.7. газовым реле типа BF80 (или аналог) с двумя парами сигнальных и отключающих контактов; 3.5.8. струйным реле типа RS 2001 (или аналог) с двумя парами отключающих контактов; 3.5.9. высоковольтными вводами с твердой изоляцией; 3.5.10. Фланцевые соединения (за исключением разъёма бака) и люки должны иметь проточки под кольцевую резину для улучшения герметичности; 3.5.11. болтовым соединением разъёма бака; 3.5.12. устройством постоянной очистки масла - термосифонным фильтром; 3.5.13. устройством отбора газа из газового реле с уровня

Наименование мероприятия	Технологические решения
	установки трансформатора; 3.5.14. табличкой-шильдиком, закрепляемой на баке трансформатора, с указанием основных параметров: - тип трансформатора; - номинальная мощность по обмоткам; - номинальные токи и напряжения по обмоткам; - напряжения короткого замыкания между обмотками; - ток холостого хода; - потери холостого хода и короткого замыкания; - схема соединения обмоток; - количество фаз; - номинальная частота; - массово-габаритные параметры; - таблица напряжений по положениям переключателя и соответствующего положению тока; - диапазон регулировки напряжения; - заводской номер; - год выпуска; - завод-изготовитель. 3.5.15. измерителями-сигнализаторами температуры и уровня масла с преобразователями по стандарту МЭК 61850-8.1. 4. Применять стационарные лестницы с использованием средств защиты ползункового типа в качестве страховочной системы при подъеме на оборудование, стационарных анкерных точек (анкерных столбов), либо с предустановкой анкерной линии и использования средства защиты втягивающего типа, либо с применением телескопических анкерных столбов для работы на оборудовании ПС 35 кВ и выше, где есть риск падения с высоты более 1,8 м (выключатели, трансформаторы (автотрансформаторы) и т.д.). Места установки и типы стационарных средств защиты от падения с высоты определить проектом. 5. Блокировка ПС: 5.1. питание блокировки ПС должно осуществляться от ЩПТ через шкаф питания оперативной блокировки разъединителей предусматривающий электрическое разделение цепей с применением не менее 3х работающих параллельно преобразователей DC/DC. 6. Применить в зданиях и сооружениях распределительных устройств 20 кВ устройства отпугивания животных. 7. Применять в качестве опорно-стержневых изоляторов и на разъединителях полимерные изоляторы, в основе опорного элемента которых используется стеклопластиковый стержень. В качестве подвесной изоляции на ПС применять стеклянную или полимерную изоляцию в соответствии с требованием

Наименование мероприятия	Технологические решения
	Распоряжения ПАО «МОЭСК» от 13.05.2019 №429р. 8. Обеспечить наличие на ПС информационных и предупреждающих знаков в соответствии с требованиями Приказа ПАО «Россети» от 05.12.2019 №330 и Приказа ПАО «Россети Московский регион» от 04.12.2020 №1225 «О размещении на информационных знаках и плакатах идентификационных QR-кодов». 9. Величина наибольшего рабочего напряжения электросетевого оборудования 20 кВ и 220 кВ должна соответствовать требованиям ГОСТ Р 57382-2017 и составлять не менее 24 кВ и 252 кВ соответственно.
Количество и мощность силовых трансформаторов	2х40 МВА (220/20 кВ)
Реконструкция и технологические решения	Установить два трансформатора напряжением 220/20 кВ, мощностью 40 МВА каждый, оснащенных устройством РПН. Тип РПН и параметры устанавливаемого оборудования уточнить проектом. Мощность устанавливаемых трансформаторов уточнить проектом в соответствии с пунктом 196, 198 «Методических указаний по проектированию развития энергосистем», утвержденных приказом Минэнерго России от 06.12.2022 № 1286. Выполнить модернизацию линейных ячеек 220 кВ ГТ-1А (резерв) и ГТ-1Б (резерв). Объём работы определить проектом. Выполнить строительство кабельных перемычек 220 кВ от линейных ячеек ГТ – 1А (резерв), ГТ – 1Б (резерв) КРУЭ 220 кВ ПС 220 кВ Молжаниновка до вновь устанавливаемых силовых трансформаторов 220 кВ. Параметры сооружаемых КЛ 220 кВ уточнить при проектировании. Выполнить установку токоограничивающих реакторов 20 кВ, обеспечивающих ограничение токов КЗ на шинах РУ 20 кВ тяговой ПС 20 кВ Молжаниново до величины не более 16 кА (тип, количество, место установки и параметры токоограничивающих реакторов определить проектом). Выполнить строительство КЛ-20 кВ, 2 шт. от выводов 20 кВ трансформатора 220/20 кВ мощностью 40 МВА до РУ-20 кВ ТП-10/20 кВ №1 нов. Выполнить строительство КЛ-20 кВ, 2 шт. от выводов 20 кВ трансформатора 220/20 кВ мощностью 40 МВА до РУ-20 кВ ТП-10/20 кВ №2 нов. Схему фазировки цепей первичной и вторичной коммутации выполнить в соответствии с указанием Мосэнерго №41-24/93 от

Наименование мероприятия	Технологические решения
	20.07.1981 г. «Об упорядочении расцветки фаз оборудования и схем включения трансформаторов».
Система собственных нужд	Необходимость реконструкции системы собственных нужд определить проектом. Проектом предусмотреть установку 3 резервного источника собственных нужд (ДГУ).
Система оперативного тока (СОТ, СОПТ)	Необходимость реконструкции системы собственных нужд определить проектом.
Расчет электроэнергетических режимов и токов короткого замыкания	1. В разделе должны быть приведены результаты анализа прогнозных балансов мощности энергосистемы г. Москвы и Московской области на год завершения каждого этапа реконструкции объекта электроэнергетики и на Расчетный период[1], для характерных режимов, указанных в пункте 2. 2. В разделе должны быть приведены описание и результаты расчетов установившихся электроэнергетических режимов для нормальной и основных ремонтных схем, а также при нормативных возмущениях в указанных схемах в соответствии с требованиями Методических указаний по устойчивости энергосистем, характеризующихся максимальной токовой нагрузкой на год завершения каждого этапа реконструкции объекта и на Расчетный период с учетом этапности реконструкции существующих и ввода/вывода электросетевых объектов, объектов генерации и динамики изменения электрических нагрузок. При анализе перспективных режимов работы электрической сети 20 кВ и выше, прилегающей к объектам проектирования, необходимо рассматривать режимы зимних максимальных нагрузок рабочего дня, зимних минимальных нагрузок рабочего дня, летних минимальных нагрузок выходного дня, летних максимальных нагрузок рабочего дня. Результаты расчетов должны включать в себя токовые нагрузки ЛЭП, (авто-)трансформаторов ПС, потокораспределение активной и реактивной мощности, уровни напряжения в сети 20 кВ и выше, представленные в табличном виде и нанесенные на однолинейную схему замещения сети. На основании результатов расчетов должен быть проведен выбор оборудования ПС 220 кВ Мельниково и ЛЭП, оценен объем необходимого электросетевого строительства,

[1] Последний год периода, на который разработана схема и программа развития электроэнергетических систем России (далее – СиПР ЭЭС России), актуальные на момент разработки проектной документации.

Если пятилетний период, начинающийся с планируемой даты ввода в работу объекта электроэнергетики, не превышает расчетный период СиПР ЭЭС России, актуальных на момент разработки проектной документации, то под Расчетным периодом понимается перспектива 5 лет, начиная с планируемой даты реализации последнего этапа реконструкции объектов электроэнергетики.

Наименование мероприятия	Технологические решения
	очередность ввода элементов электрической сети, определены мероприятия по обеспечению допустимых параметров электроэнергетического режима. В случае превышения расчетными величинами допустимых значений параметров существующего оборудования электрической сети (провода ЛЭП, выключатели, разъединители, ТТ, ВЧ-заградители, ошиновка и т.д.) предусмотреть усиление сети, а также замену оборудования вне зависимости от принадлежности объектов. 3. В составе раздела должен быть выполнен анализ баланса реактивной мощности и определены вид, количество, номинальные параметры и точки подключения СКРМ в районе размещения объекта проектирования на год завершения каждого этапа реконструкции объекта и на Расчетный период, необходимость регулирования напряжения в сети с использованием РПН трансформаторов (автотрансформаторов), включая автоматическое изменение их коэффициента трансформации. При необходимости установки регулируемых СКРМ должны быть представлены соответствующие обосновывающие расчеты. В разделе должна быть произведена проверка БСК (иных СКРМ, имеющих в своем составе БСК) на возможную перегрузку токами высших гармоник и отсутствие условий для возникновения резонансных явлений при исходных фактических значениях, гармонических составляющих напряжения на шинах подстанции, к которой присоединяется БСК. Информация о фактических значениях показателей качества электроэнергии предоставляется Заказчиком. 4. В составе раздела должны быть выполнены расчеты токов КЗ на шинах объекта проектирования, а также на шинах энергообъектов прилегающей сети 20 кВ и выше на год завершения каждого этапа реконструкции объекта электроэнергетики и на Расчетный период. По результатам расчетов должны быть определены требования к отключающей способности устанавливаемых выключателей (в том числе с учетом параметров восстанавливающегося напряжения на контактах выключателя), термической и динамической стойкости выключателей и иного оборудования, выполнена проверка соответствия существующего оборудования расчетным токам КЗ (в том числе оборудования кабельных систем 20 кВ и выше по термической стойкости и напряжению на экране кабеля), обеспечения требуемой погрешности измерительных трансформаторов тока по условиям надежной работы устройств РЗ и СИ и, при необходимости, разработаны рекомендации по замене

Наименование мероприятия	Технологические решения
	оборудования на объекте проектирования и объектах прилегающей сети 20 кВ и выше и/или разработаны мероприятия по ограничению токов КЗ (секционирование, применение токоограничивающих реакторов, разземление нейтрали части трансформаторов, опережающее деление сети и т.д.). 5. Величина наибольшего рабочего напряжения кабеля и электросетевого оборудования 20 кВ и 220 кВ должна соответствовать требованиям ГОСТ Р 57382-2017 и составлять не менее 24 кВ и 252 кВ соответственно. 6. Расчет электроэнергетических режимов и токов короткого замыкания выполнить с учетом актуальной СиПР ЭЭС России. 7. При применении схемно-режимных мероприятий по вводу параметров электроэнергетического режима в область допустимых значений, данные мероприятия должны быть проверены на допустимость их выполнения с учетом требований Методических указаний по устойчивости энергосистем и исходя из обеспечения соответствия отключающей способности выключателей уровням токов короткого замыкания. Расчетные результаты проверки должны быть представлены в дополнение к прочим результатам расчетов. Применение схемно-режимных мероприятий, приводящих к переводу электроснабжения потребителей в «тупиковом режиме», должно быть проверено на допустимость применения с учетом требований к категории электроснабжения. 8. Предоставить на рассмотрение и согласование в ПАО «Россети Московский регион» том, содержащий раздел «Расчет электроэнергетических режимов и токов короткого замыкания», принципиальную схему электрических соединений объекта реконструкции (сооружения) для каждого этапа реконструкции (сооружения) на бумажном носителе и в электронном виде в формате *.pdf (Adobe Acrobat Reader) с поясняющими рисунками и схемами без защиты содержимого с возможностью работы с текстом (поиск, копирование, печать). Не допускается передача документации в формате Adobe Acrobat Reader с пофайловым разделением страниц.
Расчетные модели	1. Расчеты установившихся электроэнергетических режимов и расчеты действующего значения основной гармоники периодической составляющей тока в начальный момент короткого замыкания, выполняемые в соответствии с требованиями раздела «Расчет электроэнергетических режимов и токов короткого замыкания» настоящего задания на проектирование, должны осуществляться с использованием расчетных моделей, сформированных на основании перспективных расчетных моделей электроэнергетической

Наименование мероприятия	Технологические решения
	системы или их фрагментов, полученных от АО «СО ЕЭС» в соответствии с Порядком раскрытия цифровых информационных моделей электроэнергетических систем и предоставления системным оператором иным субъектам электроэнергетики, потребителям электрической энергии и проектным организациям перспективных расчетных моделей электроэнергетических систем или фрагментов таких моделей для целей перспективного развития электроэнергетики, утвержденным приказом Министерства энергетики Российской Федерации от 17.02.2023 №82 (далее – расчетные модели). 2. Расчетные модели формируются для каждого этапа строительства ПС 220 кВ Мельниково и на Расчетный период. 3. К томам с результатами расчетов установившихся электроэнергетических режимов и расчетов действующего значения основной гармоники периодической составляющей тока в начальный момент короткого замыкания, направляемым на согласование в адрес Московского РДУ, должны быть приложены расчетные модели с учетом определенных в проектной документации технических решений по развитию электрических сетей (при первичном направлении результатов расчетов и при внесении изменений в направленные ранее расчетные модели).
КЛ 220 кВ	1. Для кабельных перемычек применить кабель на номинальное напряжение 220 кВ с полиэтиленовой изоляцией и медной жилой, с продольной герметизацией жилы кабеля, продольной и поперечной герметизацией экрана, с усиленной оболочкой толщиной 6 мм и с покрытием из экструдированного электропроводящего слоя. Кабельные перемычки прокладывать одной строительной длиной. 2. Сечение жилы кабеля выбрать исходя из обеспечения необходимой пропускной способности и согласовать на стадии проектирования с Московским РДУ и МВС - филиалом ПАО «Россети Московский регион». 3. Сечение экрана кабелей определить исходя из термической стойкости к току короткого замыкания для КЛ/КВЛ 220 кВ. Величину тока короткого замыкания определить проектом, подтвердить расчетом и согласовать с Московским РДУ и МВС – филиалом ПАО «Россети Московский регион». Проектом обеспечить потенциал на экране кабеля не выше 110 вольт при применении транспозиции экранов или их одностороннем заземлении в случае протекания длительно допустимого тока. Схему соединений экранов кабелей определить проектом, исходя из требуемой пропускной способности.

Наименование мероприятия	Технологические решения
	4. Для КЛ/КВЛ 220 кВ применить концевые муфты с полимерными изоляторами. При использовании металлоконструкций для установки концевых муфт, выполнить их с цинковым антикоррозионным покрытием методом горячего заводского цинкования, остальные металлоконструкции, а также места сварки - загрунтовать и покрасить. Для крепления кабеля к стойкам концевых муфт использовать полимерные хомуты. Обеспечить защиту кабелей от механических повреждений в месте выхода из земли к концевым муфтам полиэтиленовыми трубами на высоту 0,5 м под и над землей. Выход кабеля из земли на стойки концевых муфт обеспечить под прямым углом относительно земли с его центровкой и герметизацией в трубе ПНД. Обеспечить установку сплайс боксов на расстоянии не менее 1,4 м от земли. 5. При использовании элегазовых вводов на стадии проектирования обеспечить возможность их стыковки/расстыковки с переключательными пунктами без проведения земляных работ. Обеспечить возможность проведения высоковольтных испытаний постоянным напряжением и испытаний оболочек кабелей без расстыковки элегазовых вводов с переключательными пунктами. Обеспечить расстояние от прижимного фланца элегазового ввода до фундамента не менее 500 мм. Предусмотреть возможность перемещения кабеля при расстыковке элегазового ввода в незасыпном кабельном сооружении. Требования к сооружению определить в ходе проектирования. Выполнить контур заземления элегазовых вводов медными шинами. Предусмотреть в межэтажных перекрытиях подстанции противопожарные мероприятия при заходе кабеля на этаж с КРУЭ (противопожарные подушки и т.д.). 6. Конструкцию, тип кабеля и кабельной арматуры дополнительно согласовать с МВС - филиалом ПАО «Россети Московский регион» и управлением эксплуатации высоковольтных ЛЭП исполнительного аппарата ПАО «Россети Московский регион» с учётом выбора поставщика кабеля, муфт и других материалов и оборудования. Применяемая кабельная продукция должна быть аттестована в ПАО «Россети». 7. Трассу прохождения КП выбрать проектом вне проезжих частей автодорог и зоны зеленых насаждений. Согласовать трассу с МВС - филиалом ПАО «Россети Московский регион».

Наименование мероприятия	Технологические решения
	Предусмотреть меры по сохранности новых кабелей на период строительства. 8. Охранную зону КП обозначить информационными знаками установленного образца в соответствии с требованиями ПУЭ. Места установки знаков согласовать с МВС - филиалом ПАО «Россети Московский регион». 9. Засыпку кабеля произвести стабилизированным грунтом с тепловым сопротивлением, обеспечивающим требуемую пропускную способность кабельных линий. Тип грунта согласовать с МВС - филиалом ПАО «Россети Московский регион». 10. Для защиты кабелей от механических повреждений установить защитные железобетонные плиты сбоку и сверху над кабелями. 11. На открытых участках выполнить влагостойкое огнезащитное покрытие кабелей толщиной не менее 1 мм. 12. В случае прокладки кабелей в здании ПС необходимо выполнить следующие технические требования ПАО «Россети Московский регион»: - При заходе/выходе кабеля в сооружение обеспечить расположение по центру трубы в месте выхода из нее кабеля и загерметизировать выход. При расстоянии между трубами более 200 мм выполнить герметизацию термоусаживаемыми трубками; - Шаг крепления кабеля обеспечивать не более 1 м; - Заход кабеля в сооружение обеспечивать треугольником; - Кабели проложить треугольником в соответствии с требованиями ПУЭ (2006 издания) п.п. 2.3.112 - 2.3.133 (расстояние между креплениями кабеля в свету); - Исключать замкнутый металлический контур при прокладке кабеля; - В случае отсутствия противопожарной системы на объекте, предусмотреть асбестоцементные листы при пересечении кабельных перемычек и кабельных линий. 13. Проектные решения по организации заходов кабелей во все кабельные сооружения согласовать с МВС и управлением эксплуатации высоковольтных ЛЭП исполнительного аппарата ПАО «Россети Московский регион». Проект сооружения КП должен быть выполнен специализированной организацией. Получить письменное подтверждение завода-изготовителя кабеля: об обеспечении требуемой пропускной способности кабельных линий, при соблюдении предусмотренных проектами условий прокладки; о технологическом соответствии кабеля и кабельной арматуры различных производителей. Согласовать

Наименование мероприятия	Технологические решения
	проект с заводом производителем кабеля. Согласовать проект с МВС - филиалом ПАО «Россети Московский регион» и другими заинтересованными организациями. Предусмотреть проектом и выполнить мероприятия по охране окружающей среды (почва, воздух, вода) согласно требованиям законодательства РФ «Об охране окружающей среды» и Экологической политики ПАО «Россети Московский регион». 14. Для всех реконструируемых и вновь вводимых кабельных сооружений оформить технический паспорт согласно Приложению №1 и Приложению №2 к приказу ОАО «МОЭСК» №185 от 05.03.2013. 15. В сметах к рабочему проекту предусмотреть расходы на: - шеф-надзор завода-изготовителя кабельной продукции за прокладкой и монтажом КП; - изготовление хомутов пластиковых, бирок на основе технологии ламинирования; - услуги по испытанию оболочек и изоляции кабелей; - измерение частичных разрядов; - настройку системы мониторинга частичных разрядов; - выполнение электрических измерений и фазировки; - выполнение входного контроля кабелей 220 кВ с обязательным проведением испытаний на водонепроницаемость кабеля; - отбор проб и контроль качества изоляционной жидкости при монтаже концевых муфт; - проектирование и устройство временного электроснабжения объекта на время строительства; - поставку комплекта резервных материалов, оборудования; 16. Для КП 220 кВ предусмотреть в сметах затраты на приобретение резервного оборудования: 1-й концевой муфты и/или 1-го элегазового ввода (в зависимости от применения соответствующего оборудования); комплекта инструмента и оборудования для монтажа кабельной арматуры. 17. Работы по прокладке и монтажу кабелей должны выполняться специализированной строительно-монтажной организацией. Специализированный персонал строительно-монтажной организации должен иметь группу по электробезопасности (соответствующую выполняемым типам работ) и быть аттестован поставщиком кабеля и кабельной арматуры. 18. Комиссия для приемки законченных строительно-монтажных и наладочных работ назначается после предъявления технической и исполнительной документации в МВС - филиал ПАО «Россети Московский регион».

Наименование мероприятия	Технологические решения
	19. Все работы должны проводиться с получением уведомлений и согласованием ППР. 20. Все решения по данному технологическому заданию должны соответствовать требованиям действующих нормативных документов по пожарной безопасности, ПУЭ, ПТЭ электрических станций и сетей и должны быть согласованы с МВС – филиалом ПАО «Россети Московский регион» и заводом-производителем кабельной продукции. Сроки и объемы проведения работ по огнезащитной обработке кабельных линий для вновь строящихся и реконструируемых объектов определить заданием на проектирование. 21. Один экземпляр проектно-сметной документации должен быть передан в МВС - филиал ПАО «Россети Московский регион» до начала строительства для ведения технического надзора. Предоставить в МВС - филиал ПАО «Россети Московский регион»: - исполнительную документацию в бумажном виде и на электронном носителе; - исполнительные чертежи трассы КП (выполненные на инженерно-топографическом плане М 1:500 МГГТ) в бумажном виде и на электронном носителе в формате *.dwg (AutoCAD); - руководство (инструкцию) по эксплуатации кабельных линий.
КЛ 20 кВ	1. Применить кабель на номинальное напряжение 20 кВ с изоляцией сшитый полиэтилен (СПЭ) и алюминиевой жилой – марки АПвПуг. Кабельную линию прокладывать одной строительной длиной. 2. Сечение жилы кабеля выбрать исходя из обеспечения необходимой пропускной способности и согласовать на стадии проектирования с МКС - филиала ПАО «Россети Московский регион». 3. Сечение экрана кабелей определить исходя из термической стойкости к току короткого замыкания для КЛ-20 кВ. Величину тока короткого замыкания определить проектом, подтвердить расчетом и согласовать с МКС – филиалом ПАО «Россети Московский регион». 4. Для КЛ 20 кВ применить концевые муфты марки ПКВтО (для внутренней установки в РУ-20 кВ). При условии применения малогабаритных ячеек РУ-20 кВ, предусмотреть установку изолирующих адаптеров на концевую муфту. Для крепления кабеля к металлоконструкциям использовать хомуты из немагнитных материалов.

Наименование мероприятия	Технологические решения
	5. В РУ-20 кВ обеспечить возможность проведения высоковольтных испытаний постоянным напряжением и испытаний оболочек кабелей без отбалчивания. 6. Конструкцию, тип кабеля и кабельной арматуры дополнительно согласовать с 21 РЭР УКС СО МКС - филиала ПАО «Россети Московский регион» и управлением УТЭВКЛ филиала МКС ПАО «Россети Московский регион» Применяемая кабельная продукция должна быть аттестована в ПАО «Россети». 7. При прохождении КЛ в земле, трассу КЛ выбрать проектом вне проезжих частей автодорог и зоны зеленых насаждений. Согласовать трассу с 21 РЭР УКС СО МКС - филиалом ПАО «Россети Московский регион». Предусмотреть меры по сохранности новых кабелей на период строительства. Для защиты кабелей от механических повреждений установить сверху над кабелями несгораемую плитку ПЗК (или полнотелого кирпича, или бетонные плитки). 8. При прохождении сложных участков трассы КЛ (пересечения с инженерными коммуникациями, дорогами, ненормативное расстояние и пр.) необходимо производить прокладку кабеля в термостойких полимерных трубах, прошедших аттестацию в ПАО «Россети», с закладкой резерва 30 %. При заходе/выходе кабеля в сооружение обеспечить расположение по центру трубы в месте выхода из нее кабеля и загерметизировать выход. При расстоянии между трубами более 200 мм выполнить герметизацию термоусаживаемыми трубками, для трубных вводов предусмотреть шамотные карманы. 9. На открытых участках (в техподпольях, приямках) выполнить влагостойкое огнезащитное покрытие кабелей толщиной не менее 1 мм. 10. В случае прокладки кабелей в здании ПС необходимо выполнить следующие технические требования ПАО «Россети Московский регион»: - шаг крепления кабеля обеспечивать не более 1 м; - заход кабеля в сооружение обеспечивать треугольником; - кабели проложить треугольником в соответствии с требованиями ПУЭ (2006 г. издания) п.п. 2.3.112 - 2.3.133 (расстояние между креплениями кабеля в свету); - исключать замкнутый металлический контур при прокладке кабеля; 11. Проектные решения по организации заходов кабелей во все кабельные сооружения согласовать с 21 РЭР УКС СО филиала.

Наименование мероприятия	Технологические решения
	Проект сооружения КЛ должен быть выполнен специализированной организацией. Согласовать проект с МКС - филиалом ПАО «Россети Московский регион» и другими заинтересованными организациями. Предусмотреть проектом и выполнить мероприятия по охране окружающей среды (почва, воздух, вода) согласно требованиям законодательства РФ «Об охране окружающей среды» и Экологической политики ПАО «Россети Московский регион». 12. В сметах к рабочему проекту предусмотреть расходы на: - технический надзор персоналом филиала МКС за прокладкой и монтажом КЛ; - услуги по испытанию оболочек и изоляции кабелей; - получение ТУ по сохранности существующих КЛ филиала в случае проведения земляных работ в охранных зонах - выполнение входного контроля кабелей 20 кВ и полимерных труб. 13. Работы по прокладке и монтажу кабелей должны выполняться специализированной строительно-монтажной организацией. Специализированный персонал строительно-монтажной организации должен иметь группу по электробезопасности (соответствующую выполняемым типам работ) и быть аттестован поставщиком кабеля и кабельной арматуры. 14. Все работы должны проводиться с получением уведомлений и согласованием ППР. 15. Все решения по данному технологическому заданию должны соответствовать требованиям действующих нормативных документов по пожарной безопасности, ПУЭ, ПТЭ электрических станций и сетей и должны быть согласованы с МКС – филиалом ПАО «Россети Московский регион». Предоставить в МКС - филиал ПАО «Россети Московский регион»: - исполнительную документацию в бумажном виде и на электронном носителе; - исполнительные чертежи трассы КЛ (выполненные на инженерно-топографическом плане М 1:500 МГГТ) в бумажном виде.
Изоляция, защита от перенапряжений и заземление	<u>По ПС:</u> 1. Применить для защиты от перенапряжений взрывобезопасные необслуживаемые ОПН 220, 20 кВ с полимерной (силиконовой) изоляцией. Предусмотреть оснащение ОПН 220 кВ датчиками тока утечки. 2. Предусмотреть в проекте: - выполнение предпусковой диагностики (с учетом

Наименование мероприятия	Технологические решения
	требований электромагнитной совместимости) заземляющего устройства ПС заземляющего устройства ПС с выдачей паспорта ЗУ; - выполнение проверки электромагнитной обстановки (ЭМО) перед включением оборудования в работу. <u>По КЛ:</u> 1. После завершения работ по монтажу КЛ 220 кВ провести высоковольтные испытания кабеля с измерением частичных разрядов (ЧР). Затраты на указанные работы учесть в смете по монтажу КЛ.
Автоматизированная система мониторинга и диагностика	1. Технические решения по АСМД оформить отдельным томом документации. 2. Оснастить автоматизированной системой мониторинга и диагностики (АСМД) силовые трансформаторы напряжением 220 кВ. 3. АСМД должны осуществлять оперативное диагностирование текущего технического состояния оборудования, своевременное выявление возникающих дефектов и прогнозирование их развития. 4. АСМД должна выполнять: - формирование сигналов предупредительной и аварийной сигнализации по контролируемым параметрам; - самодиагностику собственных программно-технических средств; - формирование архивов долговременного хранения диагностической информации. - формировать заключение о техническом состоянии контролируемого оборудования; - вычисление отработанного ресурса и прогнозирование срока службы трансформатора в режиме реального времени. 5. Порядок оснащения и особенности конструктивной подготовки силовых трансформаторов для монтажа датчиков первого уровня АСМД должен соответствовать требованиям СТО «Технические требования по оснащению силовых трансформаторов 35 кВ и выше первичными датчиками контроля автоматизированных систем мониторинга и технического диагностирования», утвержденного распоряжением ПАО «Россети» от 06.10.20 г. №298р. 6. Выбора объема и номенклатуры датчиков первого уровня АСМД, в зависимости от мощности контролируемого оборудования, должны выполняться в соответствии с Положением ПАО «Россети» «О единой технической политике в электросетевом комплексе». 7. Полный перечень контролируемых параметров определяется на этапе проектирования с учётом особенностей

Наименование мероприятия	Технологические решения
	конкретного оборудования. 8. Оснастить автоматизированной системой мониторинга и диагностики (АСМД) частичных разрядов концевые кабельные муфты 220 кВ. 9. АСМД должна соответствовать следующим общим требованиям: - обеспечивать измерение интенсивности частичных разрядов в изоляции; - обеспечивать определение места нахождения дефекта; - формировать заключение о техническом состоянии контролируемого оборудования. 10. Система мониторинга и диагностики (АСМД) частичных разрядов концевых кабельных муфт 110 кВ должна контролировать ЧР электрическим и акустическим способами. 11. Должен осуществляться непрерывный контроль с применением АСМД под рабочим напряжением в объеме контроля уровня ЧР концевых муфт по показателям: регулярность ЧР, опасный кажущийся заряд ЧР, длительность одного цикла регистрации ЧР. 12. АСМД должна формировать заключение о техническом состоянии контролируемого оборудования. 13. Сбор и анализ полученной информации от всех подсистем мониторинга и диагностики оборудования должен проводиться на едином АРМ системы мониторинга и диагностики подстанции. Система мониторинга и диагностики должна передавать в полном объёме в режиме реального времени данные в профильные подразделения филиала и Центральную службу диагностики исполнительного аппарата ПАО «Россети Московский регион» (ЦСД). На стороне профильных служб филиала и ЦСД информация от АСМД подстанции должна выводиться (быть интегрирована) в единое существующее (при наличии) программное обеспечение (мнемосхему). Объём работ по настройке программного обеспечения со стороны подразделений учесть в пояснительной записке на тома АСМД. 14. Предусмотреть в томе по АСМД программу приемо-сдаточных испытаний единой АСМД подстанции или на отдельные её компоненты. Программа должна включать проверку передачи и получения данных с удалённых АРМ профильных подразделений.
Электромагнитная совместимость	На ПС должны быть выполнены следующие требования инструкций и методических указаний по ЭМС: - Инструкция по устройству молниезащиты зданий, сооружений и промышленных коммуникаций» СО-153-34.21.122-2003, утвержденной приказом Минэнерго России 30.06.2003 №280, Москва, изд-во МЭИ, 2004

Наименование мероприятия	Технологические решения
	- «Методические указания по контролю состояния заземляющих устройств электроустановок» РД 153-34.0-20.525-00, Москва, СПО ОРГРЭС, 2000 г. - «Методические указания по определению электромагнитной обстановки и совместимости на электрических станциях и подстанциях» СО 34.35.311-2004, утвержденными заместителем правления РАО ЕЭС «России» В.П. Ворониным 03.02.2004 г., Москва, изд-во МЭИ, 2004 г. Для обеспечения ЭМС необходимо: - выполнить в составе проекта отдельный том по обеспечению ЭМС; - в соответствии с актом обследования электромагнитной обстановки на подстанции выполнить необходимый объем работ по обеспечению ЭМС; - проводить повторную проверку электромагнитной обстановки после завершения работ по обеспечению ЭМС, предписанных актом; - по открытой части ПС кабели вторичной коммутации должны прокладываться в лотках, соответствующих всем требованиям по электромагнитной совместимости (ЭМС); - в составе тома по ЭМС представить отчёт о выполнении требований инструкций по ЭМС по результатам повторной проверки электромагнитной обстановки и расчёт допустимости протекания по экранам кабелей токов КЗ; - применять микропроцессорные терминалы защит успешно прошедшие испытания на электромагнитную совместимость в соответствии с ГОСТ Р 51317.6.5-2006 «Требования к помехоустойчивости технических средств, установленных на электрических станциях и подстанциях», а также требованиям стандарта МЭС 61850 раздел 3; - в проекте предусматривать финансирование работ по проверке электромагнитной обстановки на подстанции и устранение выявленных недочётов.
Релейная защита и автоматика (РЗА)	1. Проектирование релейной защиты и автоматики и последующие строительно-монтажные и пусконаладочные работы по РЗиА выполнить с учётом следующих нормативно-технических документов: - Приказ Минэнерго России от 13.02.2019 №100 «Об утверждении Правил взаимодействия субъектов электроэнергетики, потребителей электрической энергии при подготовке, выдаче и выполнении заданий по настройке устройств релейной защиты и автоматики»; - Приказ Минэнерго России от 13.02.2019 №101 «Об утверждении требований к оснащению линий электропередачи и оборудования объектов электроэнергетики классом

Наименование мероприятия	Технологические решения
	напряжения 110 кВ и выше устройствами и комплексами релейной защиты и автоматики, а также к принципам функционирования устройств и комплексов релейной защиты и автоматики»; - Приказ Минэнерго России от 10.07.2020 №546 «Об утверждении требований к релейной защите и автоматике различных видов и ее функционированию в составе энергосистемы и о внесении изменений в приказы Минэнерго России от 8.02.2019 №80, от 13.02.2019 №100, от 13.02.2019 №101»; - Приказ Минэнерго России от 13.02.2019 №97 «Об утверждении требований к каналам связи для функционирования релейной защиты и автоматики»; - «Рекомендации по модернизации, реконструкции и замене длительно эксплуатирующихся устройств релейной защиты и автоматики энергосистем» (СТО 34.01-4.1-011-2020); - Распоряжение ОАО «МОЭСК» №203р от 20.03.2014 года «Об утверждении альбома типовых функциональных схем взаимодействия устройств релейной защиты и автоматики»; - Распоряжение ОАО «МОЭСК» №385р от 09.06.2014 года «Об утверждении требований к оформлению схем размещения защит». 2. Релейную защиту и автоматику вновь вводимого оборудования на ПС 220 кВ Мельниково в соответствии с п. 1.12-1.20 ТУ на ТП, выполнить в соответствии с требованиями СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ». 3. Микропроцессорные устройства РЗА, устанавливаемые на объекте проектирования, объектах, технологически связанных с объектом проектирования, и объектах, на которых предусматривается выполнение работ, должны обеспечивать свою работу при частоте 45,0 – 55,0 Гц. 4. Построение систем релейной защиты и противоаварийной автоматики выполнить с применением микропроцессорных устройств, позволяющих осуществлять их дистанционную настройку и мониторинг состояния. 5. Технические характеристики устанавливаемых/заменяемых ТТ и подключенных к ним устройств РЗА в совокупности должны обеспечивать правильную работу устройств РЗА, в том числе в переходных режимах КЗ с учётом требований изготовителей устройств РЗА и приложения Б ПНСТ 283-2018 «Трансформаторы измерительные. Часть 2. Технические условия на

Наименование мероприятия	Технологические решения
	трансформаторы тока». 6. Выполнить проектирование и построение шины процесса в соответствии с требованиями МЭК 61850, в частности МЭК 61850-8-1 (MMS, GOOSE) и МЭК 61850-9-2 (SV). 7. Объем функций РЗА, реализуемых ПАК ЦПС (Программный аппаратный комплекс цифровая подстанция), должен полностью соответствовать функциям РЗА, реализуемых МП средствами, согласно распоряжению ОАО «МОЭСК» №203 от 20.03.14 года «Об утверждении альбома типовых функциональных схем взаимодействия устройств релейной защиты и автоматики». 8. Терминалы РЗА, IED, цифровые счетчики и устройства сопряжения должны иметь: декларацию соответствия реализации протокола (PICS), декларацию соответствия реализации информационной модели (MICS), дополнительную информацию по реализации протокола для испытаний (PIXIT), декларацию соответствия утвержденному перечню технических недочетов (TICS) и ICD файл с описанием возможностей устройства. 9. Для вновь вводимого оборудования на ПС 220 кВ Мельниково в соответствии с п. 1.12-1.20 ТУ на ТП, применить цифровые измерительные трансформаторы тока и напряжения, при применении аналоговых измерительных трансформаторов тока и напряжения оснастить их устройствами, осуществляющими аналогово-цифровое преобразование измерений и сигналов (АЦП). 10. На каждом выключателе КРУЭ 220 кВ в ячейках ГТ-1А и ГТ-1Б предусмотреть установку микропроцессорного терминала автоматики управления выключателем. 11. На каждом силовом трансформаторе напряжением 220/20 кВ мощностью 40 МВА должны быть установлены по два комплекта ДЗТ на базе МПТ. 12. Для защиты резисторов 20 кВ должно быть установлены комплекты дифференциальных токовых защит резисторов (ДЗР) с действием на группы выходных цепей основных защит трансформаторов, выполненные на базе МПТ. Комплекты должны быть независимыми по токовым и оперативным цепям. 13. Для защиты реакторов 20 кВ должно быть установлено по два комплекта дифференциальных токовых защит реакторов (ДЗО) с действием на группы выходных цепей основных защит трансформаторов, выполненные на базе МПТ. 14. В составе комплектов ДЗО 20 кВ выполнить МТЗ вводов 20 кВ. 15. На отходящих КЛ 20 кВ предусмотреть установку микропроцессорных терминалов.

Наименование мероприятия	Технологические решения
	16. На каждом СВ 20 кВ предусмотреть установку микропроцессорных терминалов защит. 17. Оптическую дуговую защиту шин 20 кВ на каждой секции 20 кВ выполнить в соответствии с распоряжением ОАО «МОЭСК№ №745р от 29.10.2012. 18. Для защиты секций шин 20 кВ предусмотреть применение централизованной цифровой дифференциальной защиты шин с обменом данными в соответствии с требованиями МЭК 61850-8-1, МЭК 61850-9-2. 19. Управление выключателями 220 кВ (20 кВ) организовать с использованием дискретных устройств сопряжения с шиной процесса (преобразователей дискретных сигналов), интегрированных в единую шину процесса. Передачу сигналов отключения от терминалов РЗА к дискретным устройствам сопряжения с шиной процесса (преобразователям дискретных сигналов), а также передачу сигналов РПО/РПВ от последних к терминалам РЗА выполнить с применением протокола GOOSE. Шина процесса в части передачи Sampled Values (IEC 61850-9-2LE)/GOOSE сообщений должна быть резервированной на базе протокола PRP. Передача всей информации осуществляется с контролем времени доставки по меткам времени. Устройства, подключаемые к шине процесса (терминалы РЗА, контроллеры телемеханики и т.д.) также должны поддерживать протокол резервирования PRP. 20. Непосредственное управление электрооборудованием реализовать с помощью управляющих контроллеров. Команды на отключение поступают одновременно от нескольких (интеллектуальные электронные устройства) IED (каждый из дублирующих IED работает независимо от резервирующего) через 2 контроллера на 2 катушки отключения выключателя. 21. Модельный ряд цифровых устройств, сопрягаемых с шиной процесса, должен включать в себя: преобразователь аналоговых сигналов (аналоговые измерения → Sampled Values), преобразователь дискретных сигналов (дискретные сигналы → GOOSE, GOOSE → «сухие» контакты реле), датчики технологических величин с цифровым интерфейсом, управляющий контроллер (управление выключателем, отсечным клапаном, разъединителями, ЗН, РПН, ЛРТ, УКРМ, пускателями ЭВ и ЭН в системе охлаждения тр-ра), устройства среднего уровня (IED), коммутаторы шины процесса. 22. Проектом предусмотреть применение комплекса регистрации аварийных событий по протоколам стандарта IEC 61850, в том числе с пуском по мета-данным, передаваемым в цифровых сообщениях (качества информация, признаки синхронизации времени и др.).

Наименование мероприятия	Технологические решения
	23. Проектом предусмотреть применение системы диагностики исправности цифровых коммуникаций по протоколам стандарта IEC 61850 в режиме реального времени. 24. В состав рабочей документации по РЗА должны входить: 24.1. Пояснительная записка, включающая расчет параметров настройки (уставок) и алгоритмов функционирования устройств РЗА, устанавливаемых на объектах электроэнергетики и существующих устройств РЗА, в том числе в прилегающей сети, в связи с включением нового оборудования, а также бланки уставок, содержащие параметры настройки (уставки) и алгоритмы функционирования, предусмотренные производителем устройства РЗА, и их значения, выбранные по результатам расчета. 24.2. Схемы распределения по трансформаторам тока и напряжения устройств РЗА, информационно-измерительных систем (автоматизированных систем управления технологическим процессом, автоматизированных информационно-измерительных систем коммерческого учета электроэнергии). 24.3. Принципиальные и функционально-логические схемы (алгоритмы функционирования) устройств РЗА и внешних связей с другими устройствами РЗА, коммутационными аппаратами, устройствами высокочастотной связи, устройствами передачи аварийных сигналов и команд. 24.4. Схемы организации каналов связи для функционирования устройств РЗА. 24.5. Заказные спецификации на устройства РЗА с указанием версии программного обеспечения для микропроцессорных устройств РЗА. 24.6. Схемы организации цепей оперативного тока устройств РЗА. 24.7. Схемы организации цепей напряжения устройств РЗА. 24.8. Принципиальные схемы управления и автоматики (алгоритмы функционирования) выключателей. 24.9. Технические решения по интеграции устанавливаемых устройств РЗА в создаваемые (модернизируемые) объектовые автоматизированные системы управления технологическим процессом, системы сбора и передачи информации. 25. Определение времени до насыщения устанавливаемых/заменяемых ТТ должны производиться в соответствии с ГОСТ Р 58669-2019 «Единая энергетическая система и изолированно работающие энергосистемы. Релейная защита. Трансформаторы тока измерительные индуктивные с замкнутым магнитопроводом для защиты. Методические указания по определению времени до насыщения при коротких

Наименование мероприятия	Технологические решения
	замыканиях». 26. Количественный и качественный состав РЗА на ПС 220 кВ Мельниково определить проектом; 27. Проектирование средств регистрации аварийных событий должно вестись в соответствии с ГОСТ Р 58601-2019 Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Релейная защита и автоматика. Автономные регистраторы аварийных событий. Нормы и требования. 28. В состав проектной документации по РЗА должна входить пояснительная записка, включающая проектный расчет параметров настройки (уставок) и алгоритмов функционирования устройств РЗА, устанавливаемых на объектах электроэнергетики и существующих устройств РЗА, в том числе в прилегающей сети, в связи с включением нового оборудования, а также для подтверждения принципов выполнения и уточнения качественного и количественного состава существующих устройств РЗА в прилегающей сети, а также устройств РЗА предусмотренных к установке. 29. Проектом должно быть предусмотрено применение специализированного программного обеспечения и проверочных устройств для вновь устанавливаемого комплекса РЗА с применением обмена данными по протоколу МЭК 61850. 30. Проектом предусмотреть установку на ПС 220 кВ Молжаниновка независимого регистратора аварийных событий (РАС), в том числе передаваемых в соответствии с МЭК 61850, с формированием осциллограмм в формате comtrade. 31. На этапе разработки проектной документации должна быть выполнена разработка файла SSD (System Specification Description), включающим в себя описание однолинейной схемы, требования к используемым логическим узлам и их объектам данных для моделирования функций РЗА и АСУ ТП. Файл SSD также должен включать описание распределение логических узлов по физическим (виртуальным) устройствам комплекса РЗА и АСУ ТП. На этапе разработки рабочей документации должен быть разработан файл SCD (System Configuration Description), описывающий коммуникации в формате коммуникационных сервисов стандарта IEC 61850 между устройствами комплексов РЗА и АСУ ТП. 32. Устанавливаемый комплекс РЗА должен обеспечивать возможность работы с цифровыми измерительными трансформаторами тока и напряжения, подтвержденную протоколом совместных предварительных испытаний. 33. Терминалы РЗА, IED, цифровые счетчики и устройства сопряжения должны иметь: декларацию соответствия

Наименование мероприятия	Технологические решения
	реализации протокола (PICS), декларацию соответствия реализации информационной модели (MICS), дополнительную информацию по реализации протокола для испытаний (PIXIT), декларацию соответствия утвержденному перечню технических недочетов (TICS) и ICD файл с описанием возможностей устройства. 34. Связное оборудование (коммутаторы, патч-панели, и т.п.), через которое обеспечивается связь AMU/DMU с терминалами РЗА (передача команд на отключение и SV) должно быть включено в проект РЗА и не иметь пересечений со связным оборудованием, устанавливаемым по проекту АСУТП. Для синхронизации времени между терминалами РЗА и AMU\DMU в проекте РЗА должен быть предусмотрен резервируемый сервер времени. Для присоединений, на которых предусматривается установка оптических трансформаторов тока и напряжения, и соответствующая реконструкция в части РЗА, предусмотреть проектом РЗА установку контроллеров присоединений (IED), принимающих данные от устройств полевого уровня (MU) по протоколу МЭК61850-9.2(LE), передающих команды управления выключателями, разъединителями и заземляющими ножами по протоколу GOOSE MMS и связанных с серверами АСУ ТП и ТМ по протоколу МЭК61850-8.1. Отследить согласование этих требований с требованиями в части АСУТП. 35. Обеспечить привлечение производителя оборудования РЗА на инженерное сопровождение проекта, включающий контроль стадии проектирования, приемку из наладки и один цикл технического обслуживания. 36. Предоставить в Московское РДУ не позднее, чем за шесть месяцев до намечаемого ввода объекта, параметры вновь включаемого (реконструируемого) оборудования, согласованную схему размещения устройств РЗА, схему организации каналов связи для функционирования устройств РЗА, рабочую документацию по РЗА и принципиальные проектные схемы основных и резервных защит оборудования (ЛЭП, шин) напряжения 110 кВ и 220 кВ в соответствии с пунктом 23 Правил взаимодействия субъектов электроэнергетики, потребителей электрической энергии при подготовке, выдаче и выполнении заданий по настройке устройств релейной защиты и автоматики, утвержденных приказом Министерства энергетики России от 13.02.2019 №100.
Противоаварийная, режимная и сетевая автоматика	1. На основании разработанного тома, содержащего раздел «Расчет электроэнергетических режимов и токов короткого замыкания»: а) определить виды необходимых для установки устройств

Наименование мероприятия	Технологические решения
	противоаварийной автоматики (ПА) и сетевой автоматики (СА) на ПС и в прилегающей сети; б) определить объемы управляющих воздействий, а также перечень токоприемников, подключаемых под действие АОПО и АОСН (состав фидеров и возможности их отключения); в) разработать алгоритмы функционирования устройств АОПО, АОСН и АВР; г) разработать принципиальные и функционально-логические схемы устройств АОПО, АОСН и АВР. 2. Подтвердить достаточность объемов управляющих воздействий АОПО и АОСН на основании расчетов электроэнергетических режимов для нормальной и ремонтных схем, требующих включения нормально отключенного коммутационного оборудования в прилегающей сети, при характерном максимальном и минимальном потреблении района с учетом этапов и подэтапов реконструкции (сооружения) ПС, на год окончания реконструкции (сооружения) объекта и на Расчетный период. 3. Определить настройку и режимы работы устройств автоматического повторного включения (АПВ). 4. Выполнить установку комплектов АЧР, позволяющих подключить под действие АЧР предполагаемую нагрузку ПС в полном объеме с учетом задания отдельной группы уставок на каждое присоединение (фидер). 5. Выполнить установку устройств автоматики регулирования напряжения трансформаторов под нагрузкой (АРНТ), обеспечивающих уровни напряжения в соответствии с ГОСТ 32144-2013. 6. Определить тип и количество устройств, уставки ПА и СА (уставки устройств АОПО, АОСН, АВР на основании пп. а), б), в), г) п.1). 7. При разработке технических решений по установке устройств ПА и СА: а) определить возможность использования существующих устройств ПА и СА; б) определить списки сигналов, передаваемых к/от устройств ПА и СА из/в РДП филиала ПАО «Россети Московский регион» и ДП Московского РДУ; в) списки передаваемых сигналов, технические решения, обеспечивающие передачу информации между объектами, на которых расположены устройства ПА и СА, и схемы распределения по трансформаторам тока и напряжения устройств информационно-технологических систем согласовать с подразделениями информационно-технологических систем и связи ПАО «Россети Московский регион» и филиалами

Наименование мероприятия	Технологические решения
	ПАО «Россети Московский регион», на объектах которых проектом предусмотрена установка устройств ПА и СА; г) предусмотреть возможность подключения проектируемых устройств ПА и СА к информационно-аналитическому модулю ПТК оперативно-технологического управления в РДП филиала ПАО «Россети Московский регион» с обеспечением функций мониторинга и управления. 8. Предоставить на рассмотрение и согласование в ПАО «Россети Московский регион» том, содержащий раздел «Противоаварийная, режимная и сетевая автоматика» на бумажном носителе и в электронном виде в формате *.pdf (Adobe Acrobat Reader) с поясняющими рисунками и схемами без защиты содержимого с возможностью работы с текстом (поиск, копирование, печать). Не допускается передача документации в формате Adobe Acrobat Reader с пофайловым разделением страниц.
Организация цифровой системы связи	Проектирование средств связи должно вестись согласно «Нормам технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ» СТО 56947007-29.240.10.248-2017 и Требованиям к каналам связи для функционирования релейной защиты и автоматики, утвержденным приказом Министерства энергетики Российской Федерации от 13.02.2019 №97. 1. Получить в ООО «Инфраструктура Молжаниново» технические условия на заходы волоконно-оптических кабелей связи и размещение оборудования связи на ПС 220 кВ Молжаниновка (при необходимости). 2. На участке от ПС 220 кВ Мельниково до ПС 220 кВ Молжаниновка совместно с КЛ 220 кВ выполнить устройство двух географически разнесённых волоконно-оптических линий связи с использованием волоконно-оптических кабелей связи емкостью по 48 оптических волокон каждый. 3. При устройстве волоконно-оптических линий связи применить волоконно-оптические кабели с оптическими волокнами, произведенными в странах ЕАЭС. 4. Способ устройства, трассы и марки волоконно-оптических кабелей связи определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион», управлением развития ИТСиСС ПАО «Россети Московский регион» и всеми заинтересованными организациями. 5. Выполнить разварку оптических волокон на оптических кроссах. 6. Построить цифровую систему передачи ПС 220 кВ Мельниково – ПС 220 кВ Молжаниновка – Центральный узел

Наименование мероприятия	Технологические решения
	связи ПАО «Россети Московский регион» с установкой оборудования связи: ПС 220 кВ Мельниково: - мультиплексор СЦИ с базовым пакетом лицензии для подключения сетевого элемента к серверу (1 к-т). ПС 220 кВ Молжаниновка: - доукомплектовать мультиплексор СЦИ, в случае невозможности доукомплектования – установить мультиплексор СЦИ с базовым пакетом лицензии для подключения сетевого элемента к серверу (1 к-т). Центральный узел связи ПАО «Россети Московский регион»: - при необходимости доукомплектовать мультиплексор СЦИ, в случае невозможности доукомплектования – установить мультиплексор СЦИ с базовым пакетом лицензии для подключения сетевого элемента к серверу (1 к-т). 7. Создаваемая цифровая система передачи должна быть включена в систему управления с Центрального узла связи ПАО «Россети Московский регион». 8. Разработать схему тактовой синхронизации мультиплексоров СЦИ создаваемой цифровой системы передачи, взаимоувязанную с существующей тактовой системой синхронизации ПАО «Россети Московский регион». 9. На ПС 220 кВ Мельниково установить оборудование узла доступа технологической сети передачи данных ПАО «Россети Московский регион» в составе резервируемого маршрутизатора и резервируемого коммутатора. Обеспечить резервируемое присоединение проектируемых коммутаторов к проектируемым маршрутизаторам, а также проектируемого оборудования узла доступа к узлам агрегации технологической сети передачи данных ПАО «Россети Московский регион». Тип и комплектацию оборудования определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион». 10. Организовать каналы связи для передачи команд релейной защиты и автоматики в соответствии со схемой включения защит. В случае принятия решения о применении для защит ЛЭП дифференциальных защит линий (ДЗЛ), плановый или аварийный вывод из работы любого элемента цифровой системы передачи или волоконно-оптической линии связи не должен приводить к отключению двух ДЗЛ одной линии. 11. В соответствии с разделом «Противоаварийная и режимная автоматика» проектной документации по данному титулу и ГОСТ Р 55105-2012 для передачи информации, обеспечивающей функционирование противоаварийной автоматики, организовать не менее двух независимых (по

Наименование мероприятия	Технологические решения
	географически разнесённым трассам) каналов связи в каждом направлении передачи информации. 12. Организовать основные и резервные (по географически разнесённым трассам) каналы диспетчерской телефонной связи на информационных направлениях: - ПС 220 кВ Мельниково – Центр управления сетями ПАО «Россети Московский регион». 13. Организовать основной и резервный (по географически разнесённым трассам) каналы связи для передачи технологической информации из АСУ ТП ПС 220 кВ Мельниково в АСДУ МВС – филиала ПАО «Россети Московский регион» в соответствии с требованиями раздела «По автоматизированной системе телеконтроля и управления». Адреса опорных узлов сети сбора и передачи технологической информации согласовать с управлениями эксплуатации ИТСиСС ПАО «Россети Московский регион» и развития ИТСиСС ПАО «Россети Московский регион» на этапе проектирования. 14. Организовать каналы связи для передачи информации автоматизированной системы мониторинга и диагностики высоковольтного оборудования на информационных направлениях: - ПС 220 кВ Мельниково – ДП МВС – филиала ПАО «Россети Московский регион»; - ПС 220 кВ Мельниково – центральная служба диагностики ПАО «Россети Московский регион». 15. Организовать основной и резервный (по географически разнесённым трассам) каналы связи для передачи телеинформации о технологических режимах работы КЛ 220 кВ на информационном направлении ПС 220 кВ Мельниково – ДП МВС – филиала ПАО «Россети Московский регион». 16. Организовать выделенный канал связи для передачи температурных профилей кабельных участков и удаленной настройки устройства мониторинга температуры кабелей КЛ 220 кВ с сервера мониторинга температуры ДП МВС на информационном направлении ПС 220 кВ Мельниково – ДП МВС – филиала ПАО «Россети Московский регион». 17. Организовать каналы связи передачи информации по ЧР и удаленной настройки устройства мониторинга ЧР КЛ на информационных направлениях: - ПС 220 кВ Мельниково – ДП МВС – филиала ПАО «Россети Московский регион»; - ПС 220 кВ Мельниково – центральная служба диагностики ПАО «Россети Московский регион». 18. Организовать основной и резервный (по географически

Наименование мероприятия	Технологические решения
	разнесённым трассам) каналы связи для системы учёта электроэнергии АИИС КУЭ на информационном направлении ПС 220 кВ Мельниково – сервер АИИС КУЭ филиала ПАО «Россети Московский регион» – «Энергоучет». Адрес расположения сервера АИИС КУЭ согласовать с филиалом ПАО «Россети Московский регион» – «Энергоучет», службой СДТУ МВС – филиала ПАО «Россети Московский регион» и управлением развития ИТСиСС ПАО «Россети Московский регион» на этапе проектирования. 19. В соответствии с требованиями разделов «Системы технологического видеонаблюдения» и «Охранные мероприятия» организовать каналы связи для передачи информации видеонаблюдения на информационном направлении ПС 220 кВ Мельниково – пункт управления системами видеонаблюдения. Адреса пунктов управления системами видеонаблюдения согласовать с соответствующими подразделениями ПАО «Россети Московский регион», а также управлениями эксплуатации ИТСиСС ПАО «Россети Московский регион» и развития ИТСиСС ПАО «Россети Московский регион» на этапе проектирования. 20. При необходимости разработать технические решения по сохранению действующих каналов связи и согласовать их со службой СДТУ МВС – филиала ПАО «Россети Московский регион», управлением развития ИТСиСС ПАО «Россети Московский регион», а также всеми заинтересованными организациями. 21. Схему организации связи согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион», управлением развития ИТСиСС ПАО «Россети Московский регион», а также всеми заинтересованными организациями. 22. В случае принятия решения об организации или реконструкции высокочастотных каналов связи, РЗ и ПА необходимо: - на стадии «Проектная документация» представить расчет максимальной частоты для ВЧ каналов и предварительное заключение о наличии свободных участков в рассматриваемом диапазоне частот, в которых обеспечивается работа каналов связи без взаимных помех; - на стадии «Рабочая документация» представить решение о назначении рабочих частот для ВЧ каналов, выпущенное проектным институтом, отвечающим за ведение частотного диапазона в регионе (при необходимости согласованное со смежными энергосистемами). 23. Построить СКС и ЛВС ПС 220 кВ Мельниково. Объем

Наименование мероприятия	Технологические решения
	сооружения СКС и ЛВС определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион». 24. На ПС 220 кВ Мельниково установить диспетчерский коммутатор. Тип и комплектацию оборудования определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион». 25. На ПС 220 кВ Мельниково обеспечить звукозапись диспетчерских переговоров. Тип и комплектацию оборудования определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион». 26. На ПС 220 кВ Мельниково обеспечить связь оповещения с установкой громкоговорителей, включенных в радиотрансляционную и радиопоисковую сеть подстанции. Тип и комплектацию оборудования определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион». 27. Электропитание оборудования комплекса средств связи должно осуществляться от системы гарантированного и бесперебойного электропитания ГОСТ 5237-83 и соответствовать в отношении надежности энергоснабжения – первой категории. Оборудование связи, имеющее возможность электропитания от нескольких источников, должно быть запитано от двух независимых вводов. Оборудование связи оснастить собственной системой бесперебойного электропитания. Емкость аккумуляторных батарей собственной системы бесперебойного электропитания должна обеспечивать питание нагрузки в течение 6 часов. Устройства системы электропитания: выпрямители, преобразователи, герметичные аккумуляторы (в специальных шкафах) разместить в аппаратной связи, негерметичные аккумуляторы в специальном помещении. Схемы электропитания оборудования связи должны быть разработаны в соответствии с «Руководящими указаниями по проектированию электропитания технических средств диспетчерского и технологического управления» №11619тм-т1. Схемы электропитания оборудования связи для каждого объекта, на котором устанавливается оборудование связи, а также тип и комплектацию оборудования определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион», а также всеми заинтересованными организациями. 28. Все интерфейсные окончания трибутарных модулей

Наименование мероприятия	Технологические решения
	цифровых систем передачи, систем коммутации, ТМиТИ и другого оконечного оборудования должны быть выведены на пассивное кроссовое оборудование для их оперативной коммутации с помощью съемных перемычек или шнуров с возможностью параллельного контроля сигналов передаваемых по этим цепям. 29. Применяемые кабели связи, оборудование, изделия, материалы и программное обеспечение должны быть включены в Единый реестр российских программ для электронных вычислительных машин и баз данных (Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановление Правительства Российской Федерации от 16.11.2015 г. № 1236, https://reestr.digital.gov.ru) и Единый реестр российской радиоэлектронной продукции (постановление Правительства Российской Федерации от 10.07.2019 г. № 878, https://gisp.gov.ru/pprf/marketplace/#/). Применяемые кабели связи, оборудование, изделия и материалы должны быть аттестованы в ПАО «Россети» и иметь действующее положительное заключение аттестационной комиссии ПАО «Россети». Применяемые кабели связи, оборудование, изделия и материалы должны быть включены в Перечень оборудования, материалов и систем, допущенных к применению на объектах ДЗО ПАО «Россети», размещенного на электронном ресурсе общего доступа сайта ПАО «Россети», применяться на сети связи ПАО «Россети Московский регион» и не иметь отрицательного опыта эксплуатации в ПАО «Россети Московский регион». В случаях отсутствия возможности применения аттестованных кабелей связи, оборудования, изделий и материалов необходимо получить положительное решение комиссии ПАО «Россети Московский регион» по допуску оборудования, материалов и систем (КДО) о возможности применения неаттестованных кабелей связи, оборудования, материалов и систем на объектах Общества согласно действующему Регламенту работы КДО ПАО «Россети Московский регион». Комплектацию оборудования связи определить в процессе проектирования и согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион», управлением развития ИТСиСС ПАО «Россети Московский регион» и всеми заинтересованными организациями. 30. Оборудование связи на объектах ПАО «Россети Московский регион» должно располагаться в телекоммуникационных шкафах двухстороннего обслуживания. 31. Помещения для размещения оборудования связи должны

Наименование мероприятия	Технологические решения
	быть оборудованы охранной сигнализацией, а также системами вентиляции и кондиционирования. Для ввода кабелей связи в здания и сооружения выполнить кабельные вводы с учетом допустимых радиусов изгиба кабелей и запасных кабельных каналов (на развитие). 32. В смете и спецификации предусмотреть: - комплект ЗИП для ремонта станционного и линейного оборудования связи; - эксплуатационный (аварийный) запас волоконно-оптического кабеля согласно распоряжению ПАО «МОЭСК» №409-1097р от 06.12.2007; - затраты на проведение технического надзора при проектировании и строительстве волоконно-оптических линий связи. Тип, количество и комплектацию ЗИП согласовать со службой СДТУ МВС – филиала ПАО «Россети Московский регион», управлением развития ИТСиСС ПАО «Россети Московский регион», а также всеми заинтересованными организациями. 33. Исполнитель, при выполнении работ на оборудовании связи ПАО «Россети Московский регион» должен руководствоваться Регламентом по организации производства работ на оборудовании и линиях связи ПАО «МОЭСК» от 25.10.2010 34. При сдаче в эксплуатацию каналов связи необходимо руководствоваться «Инструкцией по проведению измерений и составлению паспортов технической документации на станционные и линейные сооружения волоконно-оптических линий передачи, законченные строительством», введенной приказом ПАО «МОЭСК» №941 от 17.08.2017. 35. Проект по организации цифровой системы связи ПС 220 кВ Мельниково выполнить в виде отдельного тома. Проект по организации цифровой системы связи ПС 220 кВ Мельниково должен быть согласован со службой СДТУ МВС – филиала ПАО «Россети Московский регион», управлением развития ИТСиСС ПАО «Россети Московский регион», а также всеми заинтересованными организациями. Электронную копию проектной документации по организации цифровой системы связи ПС 220 кВ Мельниково в формате *.pdf (со всеми подписями уполномоченных должностных лиц) и в формате *.dwg (AutoCAD) представить в управление развития ИТСиСС ПАО «Россети Московский регион». 36. По завершению работ по организации цифровой системы связи ПС 220 кВ Мельниково представить исполнительную документацию в бумажном виде, а также на электронном

Наименование мероприятия	Технологические решения
	носителе в формате *.pdf (со всеми подписями уполномоченных должностных лиц) и в формате *.dwg (AutoCAD) в службу СДТУ МВС – филиала ПАО «Россети Московский регион».
Автоматизированная система телеконтроля и управления	На ПС 220/20 кВ установить систему автоматизации подстанции по архитектуре МЭК61850 с созданием шины процесса и шины подстанции. Система автоматизации должна соответствовать требованиям «Методических указаний по применению в ПАО «Россети Московский регион» основных технических решений по эксплуатации, реконструкции и новому строительству электросетевых объектов» с учетом требований Приложения 3, требованиям СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ» и требованиям Положения о Единой технической политике ПАО Россети. **1. Общие требования к системе:** 1.1. Система автоматизации должна обеспечивать: - оперативное управление (технологическое и диспетчерское); - информационную поддержка и контроль систем РЗА и других специализированных систем автоматического управления/регулирования устанавливаемых/реконструируемых на ПС; - мониторинг состояния и эксплуатации основного технологического оборудования с интеграцией устанавливаемых на ПС систем мониторига и диагностики; - синхронизацию времени для всех устанавливаемых на ПС автоматизированных систем; - обеспечение информационной безопасности. 1.2. Построить шину подстанции и шину процесса в соответствии с требованиями МЭК 61850, в частности МЭК 61850-8-1 (MMS, GOOSE) и МЭК 61850-9-2 (SV). 1.3. Разработать и включить при проектировании цифровой ПС в состав электронной документации ПС файлы электронной конфигурации SSD и SCD (и другие файлы SCL при необходимости) с учетом следующего: - SSD и SCD файлы должны быть разработаны на базе языка SCL в соответствии с актуальной схемой, определенной в МЭК 61850; - в SSD файле должны быть описаны однолинейная схема ЦПС и логические узлы с привязкой к элементам однолинейной схемы; - в SCD файле должны содержаться описание подстанции (однолинейной схемы), описание коммуникаций между

Наименование мероприятия	Технологические решения
	устройствами, описание интеллектуальных электронных устройств и описание шаблонов типов данных. 1.4. Оснастить нецифровые измерительные трансформаторы тока и напряжения устройствами, осуществляющими аналогово-цифровое преобразование измерений и сигналов. 1.5. Предусмотреть возможность расширения системы автоматизации по количеству данных до 20%. 1.6. Обеспечить резервирование электропитания оборудования системы автоматизации. Предусмотреть подключение системы бесперебойного питания к независимым секциям ЩСН и к ЩПТ. 1.7. Определить ЗИП необходимый для эксплуатации системы автоматизации по ГОСТ 27.507-2015, включить ЗИП в комплект поставки оборудования. Состав ЗИП согласовать на этапе проектирования со службой АСТУ и ТМ филиала ПАО «Россети Московский регион». **2. Требования к организации оперативно-технологического управления** 2.1. Для оперативного контроля состояния и режимов работы обеспечить передачу от ПС до узла доступа на ДП филиала ПАО «Россети Московский регион» и ЦУС ПАО «Россети Московский регион» телеинформации в соответствии с требованиями: - п.3 «Технических требований по организации каналов связи для оперативных переговоров и передачи телеметрической информации при выполнении ЦУС операционных функций в отношении объектов диспетчеризации», утвержденных ПАО «Россети» 29.12.2017 с учетом требований п. 3.8. - Приложения 4 к Соглашению о технологическом взаимодействии между АО «СО ЕЭС» и ПАО «Россети Московский регион» в целях обеспечения надежности функционирования ЕЭС России. - Типовому составу телеинформации, подлежащей передаче с объектов электроэнергетики в диспетчерские центры АО «СО ЕЭС». - Составу аварийно-предупредительной сигнализации, подлежащей передаче с объектов электроэнергетики в Московское РДУ. 2.2. Организовать сбор и передачу на ДП филиала ПАО «Россети Московский регион» АПТС и телеизмерений от МП РЗА, ОМП, СОПТ, ЩСН, ОПС. Объем телеинформации уточнить на этапе проектирования и, включая адресную часть, согласовать со службой АСТУ и ТМ филиала ПАО «Россети Московский регион», Управлением эксплуатации ИТС и СС и Управлением развития ИТС и СС Исполнительного Аппарата

Наименование мероприятия	Технологические решения
	ПАО «Россети Московский регион». 2.3. На этапе проектирования разработать перечни телеинформации для передачи на ДП филиала ПАО «Россети Московский регион». Перечни, включая адресную часть, согласовать с ПАО «Россети Московский регион» и Московским РДУ. 2.4. Передача телеинформации от ПС на ДП филиала ПАО «Россети Московский регион» должна производиться в протоколе МЭК-60870-104 и МЭК61850 с возможностью выбора протокола передачи данных путем изменения программных настроек головного устройства системы автоматизации на ПС. 3. Реализовать передачу информации с обособленных автоматизированных подсистем на АРМ подразделений ПАО «Россети Московский регион», занимающихся их эксплуатацией. Направления передачи, протоколы передачи данных и формы отображения информации согласовать с соответствующими подразделениями ПАО «Россети Московский регион» 4. Проектом предусмотреть комплекс мероприятий по обеспечению информационной безопасности системы автоматизации и каналов передачи телеинформации. **5. Разработка документации для согласования проекта с АО «СО ЕЭС».** 5.1. Разработать и согласовать с ПАО «Россети Московский регион» и Московским РДУ схемы организации каналов передачи телеинформации, логическую схему передачи телеинформации и матрицу распределения информационных потоков. 5.2. Проектную документацию согласовать с ПАО «Россети Московский регион» и Московским РДУ. 5.3. Разработать программу-методику комплексных испытаний системы автоматизации согласовать её с Московским РДУ и ПАО «Россети Московский регион».
Учет электроэнергии	1. Требования к проектированию. 1.1. Разработка и проектирование автоматизированной информационно-измерительной системы коммерческого учета (АИИС КУЭ) ПС 220 кВ Мельниково должны выполняться в соответствии с требованиями действующих отраслевых нормативных, директивных и методических документов, требований Типового стандарта «Техническая политика. Системы учета электрической энергии с удаленным сбором данных оптового и розничных рынков электрической энергии на объектах дочерних и зависимых обществ ПАО «Россети». 1.2. Разработке проектной документации на АИИС КУЭ ПС

Наименование мероприятия	Технологические решения
	220 кВ Мельниково должно предшествовать проведение ППО ПС: 1.2.1. До проведения ППО необходимо собрать техническую документацию (копии документов должны быть получены в соответствующем электросетевом филиале ПАО «Россети Московский регион», филиале «Энергоучет» или оформлены до начала проведения ППО сетевой организацией), в соответствии с п.4.3. распоряжения ПАО «Россети» №355 от 20.07.2015 1.2.2. Отчет ППО должен быть утверждён в ПАО «Россети Московский регион». 1.2.3. Отчет ППО должен содержать: а) перечень существующих точек учета с указанием состава измерительных комплексов: - однолинейная схема подстанции с указанием расположения измерительных комплексов, в т.ч. на уровне напряжения 0,4/0,23 кВ. - перечень оборудования на подстанции, используемого для учета. - наличие на подстанции приборов учёта, принадлежащих ПАО «Россети Московский регион», потребителю. б) перечень измерительных комплексов, не соответствующих требованиям НТД по следующим критериям: - несоответствие класса точности ТТ, ТН, счетчиков действующим НТД (подтверждает организацией, проводящей ППО). - несоответствие нагрузок на ТТ по току (согласно требованиям п. 1.5.17 ПУЭ, ГОСТ 7746-2015) (для ИИК с не подлежащими замене измерительным ТТ). - наличие совмещенных вторичных цепей учета с цепями измерений и РЗА (для ИИК с не подлежащими замене измерительным ТТ, ТН). - несоответствие нагрузок вторичных цепей измерительных трансформаторов (для ИИК с ТТ, ТН, не подлежащими замене). - несоответствие падений напряжения в цепях учета (для ИИК с ТН, не подлежащими замене). - несоответствие срока службы (для ИИК с ТТ, ТН, не подлежащими замене). 1.2.4. Отчет ППО должен быть согласован с «Энергоучет» - филиалом ПАО «Россети Московский регион» в части перечня точек учета, наличия и состояния, балансовой принадлежности приборов учета. 1.3. До выполнения строительно-монтажных работ необходимо разработать дополнение к проектной документации на автоматизированную информационно-измерительную систему коммерческого учета электроэнергии (АИИС КУЭ) ПС

Наименование мероприятия	Технологические решения
	220 кВ Молжаниновка. Проект выполнить отдельным томом, электронную копию представить в «Энергоучёт» - филиал ПАО «Россети Московский регион» и ДМиККЭ ИА ПАО «Россети Московский регион». 1.4. Измерительные комплексы (ИК) должны быть установлены/модернизированы на ПС 220 кВ Молжаниновка: 1.4.1. В РУ-220 кВ на вновь устанавливаемых присоединениях: - линейных (ГТ-1А, ГТ-1Б); - вводах трансформаторов; - ремонтной перемычки (при наличии), - обходного выключателя (при наличии). 1.4.2. В РУ-20 кВ на вновь устанавливаемых присоединениях: - вводах трансформаторов; 1.4.3. В РУ-20 кВ на вновь устанавливаемых присоединениях: - отходящих линий; - присоединениях ДГК (при наличии). 1.4.4. ЩСН-0,4 кВ (Собственные нужды ПС) - на вновь устанавливаемых присоединениях: - присоединениях ТСН/ДГУ, в т.ч. резервного ТСН (при наличии), - присоединений хознужд (при наличии). 1.5. В качестве приборов учета для реконструируемых/вновь вводимых присоединений, указанных в п. 1.4.1, 1.4.2 использовать цифровые многофункциональные счетчики электроэнергии, класса точности не ниже 0,2S/0,5. На присоединениях, указанных в п. 1.4.3, 1.4.4 использовать статические интервальные счетчики электроэнергии, класса точности 0,2S/0,5. Применяемые приборы учета должны соответствовать требованиям СТО 34.01-5.1-009-2021. 1.6. Для ПС 220 кВ Молжаниновка установить УСПД соответствующее требованиям СТО 34.01-5.1-010-2021. Схему сбора и передачи данных по учету электроэнергии, применяемое оборудование в случае построения шины процесса и шины подстанции в соответствии с МЭК 61850 и применения цифровых многофункциональных счетчиков электроэнергии с использованием МЭК 61850-9-2 (SV) определить проектом. Количество узлов учета электроэнергии в АИИС КУЭ ПС 220 кВ Молжаниновка должно обеспечивать получение баланса электроэнергии по шинам и по подстанции в целом. Конкретные типы и модификации счетчиков и УСПД согласовать с «Энергоучёт» - филиалом ПАО «Россети Московский регион». 1.7. Предусмотреть этапность/последовательность

Наименование мероприятия	Технологические решения
	выполнения работ по модернизации системы АИИС КУЭ, согласно этапам/последовательности выполнения реконструкции ПС. 1.8. Все средства измерений должны иметь действующие сертификаты об утверждении типа средств измерений, выданные Федеральным агентством по техническому регулированию и метрологии (с информацией о занесении СИ в Госреестр СИ РФ). Выполнение измерений должно осуществляться в соответствии с аттестованными в установленном порядке методиками. 1.9. Проектная и эксплуатационная документация должна выполняться в соответствии с требованиями: - Единой системы конструкторской документации ЕСКД; - ГОСТ 34.201-89, ГОСТ 34.602-89, ГОСТ 34.601-90, ГОСТ 34.603-92 - Комплекс стандартов на автоматизированные системы; - ГОСТ 24.104-85, ГОСТ 24.701-86 – Система технической документации; - ГОСТ 19.101-77, ГОСТ 19.201-78 - Единая система программной документации. Проектные и эксплуатационные документы должны быть согласованы в электросетевом филиале, филиале ПАО «Россети Московский регион» - «Энергоучёт» и утверждены в ПАО «Россети Московский регион». 1.10. На этапе проектирования измерительных комплексов, расчеты и выбор компонентов должен соответствовать требованиям ПУЭ (1.5), типовых инструкций СО 153- 34.09.101-94, СО 34.11.321-96, СО 34.11.114-95, СО 34.11.209-99, МЭК 61850. 1.11. Для измерительных каналов необходимо: - на присоединениях РУ-220, 20 кВ, указанных в 1.4.1, 1.4.2 раздела «Учет электроэнергии», установить измерительные трансформаторы тока и напряжения (в трех фазах) с отдельными используемыми для учета вторичными обмотками (кернами) и/или цифровыми выходами класса точности 0,2S и 0,2 соответственно; при использовании измерительных ТТ и ТН с аналоговыми выходами рассмотреть возможность применения устройств, осуществляющих аналого-цифровое преобразование измерений (АЦП); - на присоединениях РУ-20 кВ, указанных в п. 1.4.3 установить измерительные трансформаторы тока в трех фазах с отдельной вторичной обмоткой для цепей учета с классом точности 0,2S и измерительной обмоткой с классом точности 0,5; установить трансформаторы напряжения, которые должны иметь отдельную вторичную обмотку для цепей учета;

Наименование мероприятия	Технологические решения
	необходимо обеспечить работу данной вторичной обмотки трансформаторов напряжения в классе точности 0,2. - на присоединениях 0,4 кВ (присоединения ТСН), указанных в п.1.4 раздела «Учет электроэнергии», установить отдельные измерительные трансформаторы тока в трех фазах для учета с классом точности не ниже 0,2S - для всех измерительных каналов применять измерительные трансформаторы, приборы учета, соответствующие ГОСТ 7746-2015, ГОСТ 1983-2015, ГОСТ 31818.11-2012, ГОСТ 31819.22-2012, ГОСТ 31819.23-2012, требований Типового стандарта «Техническая политика. Системы учета электрической энергии с удаленным сбором данных оптового и розничных рынков электрической энергии на объектах дочерних и зависимых обществ ПАО «Россети», ГОСТ Р МЭК 60044-8-2010, ГОСТ Р МЭК 60044-7-2010, СТО 34.01-5.1-009-2021, МЭК 61850, в частности МЭК 61850-9-2 (SV); - средства измерений, поставляемые для оснащения подстанции, входящие в состав измерительных комплексов, должны иметь на момент ввода в эксплуатацию действующие оттиски клейм о поверке или свидетельства о поверке (Приказ Минпромторга России от 02.07.2015 №1815). 1.12. В проекте предусмотреть основной и резервные каналы передачи данных между УСПД на ПС 220 кВ Молжаниновка и сервером АИИС КУЭ ПАО «Россети Московский регион». Подключение каналов связи к УСПД осуществить по интерфейсу Ethernet. Произвести параметрирование УСПД ПС и сервера АИИС КУЭ ПАО «Россети Московский регион» в соответствии с объёмами выполняемых работ по этапам реконструкции ПС. Провести работы по полной интеграции счетчиков электроэнергии и УСПД ПС в существующий ИВК верхнего уровня системы учета электроэнергии ПАО «Россети Московский регион» (ПО «АльфаЦЕНТР»). Возможность интеграции счетчиков и УСПД с ИВК ВУ должна быть подтверждена протоколом совместных предварительных испытаний. При этом ИВКЭ должен обеспечивать предоставление доступа ИВК к результатам измерений, данным о состоянии средств измерений и состоянии объектов измерений, в том числе параметры электрической сети. 1.13. Аппаратная часть ИК должна быть защищена от воздействия электромагнитных полей и механических повреждений. 1.14. Все компоненты ИК должны иметь возможность функционировать в существующем электромагнитном

Наименование мероприятия	Технологические решения
	окружении, не влияя на это окружение недопустимым образом. При этом ко всем компонентам системы должны предъявляться требования действующих нормативных, отраслевых директивных и методических документов в части электромагнитной совместимости (ЭМС). 1.15. Средства коммерческого учета и данные коммерческого учета об энергопотреблении на всех уровнях должны быть защищены от несанкционированного доступа для исключения возможности искажения результатов измерений. 1.16. Необходимо обеспечить резервирование питания технических средств коммерческого учета электроэнергии, устанавливаемых на подстанции (предусмотреть в проектной документации шинки/клеммы резервного питания счетчиков, шкаф АВР для резервного питания счетчиков и питания шкафа УСПД). Необходимо обеспечить подключение к источнику бесперебойного питания технических средств коммерческого учета электроэнергии уровня ИВКЭ, устанавливаемых на подстанции. 1.17. В проекте отдельным разделом выполнить расчет численности персонала, выполняющего техническое обслуживание АИИС КУЭ ПС 220 кВ Молжаниновка в ччас/год. 2. Требования к монтажу. 2.1. Строительно-монтажные и пуско-наладочные работы выполнить организацией, отвечающей требованиям установленным законодательством Российской Федерации для выполнения данного вида работ, в соответствии с согласованной проектной документацией. 2.2. Счетчики должны устанавливаться на панелях, щитах, в нишах, на стенах, имеющих жесткую конструкцию (ПУЭ, п.1.5.29.). 2.2.1. Счетчики, предусмотренные в п.п. 1.4.1 раздела «Учет электроэнергии», установить в отдельных панелях/шкафах учета. 2.2.2. Счетчики, предусмотренные в п.п. 1.4.2, 1.4.3, 1.4.4, раздела «Учет электроэнергии», установить на дверях ячеек. 2.3. Предусмотреть резервирование ТН, используемых для учета. 2.4. Информационные цепи выполнять контрольным экранированным кабелем с необходимым количеством жил; прокладку информационных цепей на территории ПС выполнять морозоустойчивым кабелем в броневой оболочке; исключить совместную прокладку информационных и силовых кабелей. *В случае применения измерительных ТТ, ТН с отдельным аналоговым выходом для учета:*

Наименование мероприятия	Технологические решения
	2.5. Производить подключение электросчетчиков к измерительным трансформаторам тока и напряжения отдельным кабелем. 2.6. Вывести вторичные измерительные цепи тока и напряжения на специальные испытательные блоки, (испытательные коробки), установленные в непосредственной близости от электросчетчиков и обеспечить возможность их пломбировки. 2.7. При проведении работ по установке ИК на ПС, вторичные измерительные цепи от измерительных трансформаторов до счетчиков между панелями, шкафами, на территории ПС выполнять контрольным экранированным кабелем с резервной жилой; прокладку цепей напряжения присоединений 220 кВ на территории ПС выполнять кабелем в броневой оболочке; допускается выполнять вторичные цепи напряжения присоединений 20 кВ неэкранированным кабелем (проводом), при прохождении цепей только внутри релейных отсеков и соблюдении требований о предотвращении несанкционированного доступа к цепям учета. 2.8. При наличии догрузочных резисторов в токовых цепях учета установить дополнительные обводные коробки испытательные типа КИ-10 (или аналогичные) или установить дополнительные пломбируемые измерительные клеммы с размыкателями и короткозамыкателями, обеспечивающие возможность их выкорачивания. 2.9. Предусмотреть автоматические выключатели в цепях напряжения, используемых для учета; предусмотреть испытательные блоки в цепях ТН, используемых для учета. 2.10. Трансформаторы тока в ячейках КРУ, ЩСН должны иметь расширенную характеристику вторичной нагрузки обмотки для учета электроэнергии в соответствующем классе точности: от 1 ВА до Sном. 3. Требования к вводу АИИС КУЭ в эксплуатацию 3.1. После завершения проектных, строительно-монтажных и пусконаладочных работ для ввода АИИС КУЭ в опытную и промышленную эксплуатацию создается рабочая комиссия. В состав рабочей комиссии должны входить представители ПАО «Россети Московский регион», электросетевого филиала, филиала «Энергоучёт», подрядной организации. 3.2. Ввод в опытную эксплуатацию АИИС КУЭ ПС 3.2.1. Рабочей комиссии должны быть представлены: - смонтированный в соответствии с проектом действующие ИК, ИВКЭ и другое оборудование, используемое для учета; - утвержденное Техническое задание на АИИС КУЭ ПС, - рабочий проект, утвержденный ПАО «Россети Московский

Наименование мероприятия	Технологические решения
	регион»; - паспорта (формуляры) и руководства по эксплуатации на все приборы и устройства, используемые для учета; - действующие свидетельства о поверке на все заменяемые/вновь установленные средства измерений или отметки в паспортах о первичной поверке, - сертификаты об утверждении типа средств измерений на все средства измерений, - паспорта-протоколы на ИК, оформленные в соответствии с СО.34.09.101-94, - структура базы данных (существующая), - акт технической готовности строительно-монтажных работ АИИС КУЭ ПС, - акт об окончании пуско-наладочных работ АИИС КУЭ, - иные сопроводительные документы к техническим средствам (ГОСТ 2.102-2013, ГОСТ 2.601-2013) и программному обеспечению (ГОСТ 19.101-77), а также разработанные подрядной организации эксплуатационные документы, - протокол о проведении испытаний АИИС КУЭ, - программа и методика испытаний АИИС КУЭ в соответствии с требованиями ГОСТ 34.601-90, ГОСТ 34.603-92. 3.2.2. Решение о вводе АИИС КУЭ в опытную эксплуатацию принимается рабочей комиссией и оформляется Актом ввода АИИС КУЭ в опытную эксплуатацию. 3.3. Ввод в промышленную эксплуатацию АИИС КУЭ ПС: 3.3.1. Рабочей комиссии должны быть представлены: - смонтированный в соответствии с проектом действующие ИК, ИВКЭ и другое оборудование, используемое для учета; - утвержденное Техническое задание на АИИС КУЭ ПС, - рабочий проект, утвержденный ПАО «Россети Московский регион»; - паспорта (формуляры) и руководства по эксплуатации на все приборы и устройства, используемые для учета; - действующие свидетельства о поверке на все заменяемые/вновь установленные средства измерений или отметки в паспортах о первичной поверке, - сертификаты об утверждении типа средств измерений на все средства измерений, - паспорта-протоколы на ИК, оформленные в соответствии с СО.34.09.101-94. - структура базы данных (существующая), - акт технической готовности строительно-монтажных работ АИИС КУЭ ПС, - акт об окончании пуско-наладочных работ АИИС КУЭ

Наименование мероприятия	Технологические решения
	- сопроводительные документы к техническим средствам (ГОСТ 2.102-68, ГОСТ 2.601-2006) и программному обеспечению (ГОСТ 19.101-77), а также разработанные подрядной организации эксплуатационные документы. - программа и методика испытаний АИИС КУЭ в соответствии с требованиями ГОСТ 34.601-90, ГОСТ 34.603-92. - протокол о проведении испытаний АИИС КУЭ. - акт завершения опытной эксплуатации, - протокол соответствия АИИС КУЭ ПС утвержденному Техническому заданию, - акт о составлении баланса электроэнергии по ПС 220 кВ Молжаниновка за 1 календарный месяц, в период опытной эксплуатации. 3.3.2. Решение комиссии оформляется Актом ввода АИИС КУЭ в промышленную эксплуатацию с указанием возможности или невозможности ввести АИИС КУЭ ПС в промышленную эксплуатацию.
Метрологическое обеспечение	1. Проект «Метрологическое обеспечение» выполнить отдельным томом. 2. Каналы связи на момент ввода в эксплуатацию должны соответствовать, в части метрологических характеристик, Постановлению Правительства Российской Федерации от 16.11.2020 №1847, пп. 7.2.1., 7.3., 7.4., 7.5., 7.6. перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений. 3. Метрологические характеристики каналов связи должны быть определены в соответствии с утвержденными методиками (методами) измерений. В проектной документации указать ссылки на методики (методы) измерений в Федеральном информационном фонде обеспечения единства измерений ФГИС "Аршин". 4. В протоколах измерений метрологических характеристик каналов связи указать типы, заводские номера, номера свидетельств о поверке, дату поверки, дату следующей поверке применяемых средств измерений. Применение не поверенных средств измерений не допускается. 5. В проекте указать: 5.1. Типы, метрологические характеристики применяемых средств измерений; 5.2. Методики (методы) измерений (допускается указание ссылок на утвержденную методику (метод) измерений в Федеральном информационном фонде обеспечения единства измерений ФГИС "Аршин"); 5.3. Нормативные документы содержащих требования к выполнению измерений и средствам измерений;

Наименование мероприятия	Технологические решения
	5.4. Номера действующих Свидетельств об утверждении типа средств измерений и номера регистрации в Федеральном информационном фонде по обеспечению единства измерений, на все используемые средства измерений; 5.5. Перечни информационно-измерительных каналов с расчетом погрешности ИИК; 5.6. Проверку нагрузки вторичных цепей измерительных ТТ и ТН; 5.7. Перечень измеряемых на объекте параметров и точек (мест) измерений, диапазоны изменений измеряемых параметров и перечня влияющих на результат измерения внешних величин; 5.8. Отнесение измеряемого параметра к сфере Государственного регулирования обеспечения единства измерений; 5.9. Требования к нормам точности измерения параметров; 5.10. Необходимость интеграции измеряемого параметра в ИТС; 5.11. Основные требования по выбору СИ; 5.12. Основные требования к метрологическому обеспечению СИ на всех этапах жизненного цикла (проектирование, ввод в действие, эксплуатация). 6. Средства измерений, в том числе сигнализаторы плотности элегаза, плотномеры, устройство регистрации частичных разрядов, измерительные датчики тока, напряжения, температуры и других физических величин, применяемые для мониторинга, контроля и наблюдения за технологическими параметрами (в устройствах: контроля высоковольтных вводов трансформаторного оборудования, мониторинга состояния высоковольтных выключателей, управления и мониторинга элегазовой ячейки, контроля допустимых перегрузок трансформаторного оборудования, управления и мониторинга трансформаторного оборудования, диагностики и мониторинга высоковольтных кабельных линий и КРУЭ и т.д) должны иметь: 6.1. на момент согласования проектной документации: - свидетельства об утверждении типа СИ (допускается представление ссылок на утвержденные типы СИ в Федеральном информационном фонде обеспечения единства измерений ФГИС "Аршин"); 6.2. на момент ввода в эксплуатацию: - свидетельства о поверке или оттиски поверительного клейма (допускается представление ссылок на поверенные СИ в Федеральном информационном фонде обеспечения единства измерений РСТ "Метрология"); - положительное заключение аттестационной комиссии

Наименование мероприятия	Технологические решения

ПАО «Россети».

7. Метрологические характеристики средств измерений должны соответствовать требованиям действующих нормативных документов Российской Федерации и ПАО «Россети».

8. Для новых присоединений, а также для присоединений, оснащенных аналоговыми щитовыми измерительными приборами, предусмотреть в проектном решении цифровые щитовые измерительные приборы класса точности не хуже 0,5.

9. Щитовые измерительные приборы всех присоединений подключать к обмоткам измерительных трансформаторов класса точности не хуже 0,5 по аналоговому выходу ТТ и ТН, при отсутствии возможности подключения протоколов МЭК 61850 (Передачу информации на вышестоящие уровни требуется осуществлять в формате протоколов МЭК 61850).

10. При размещении цифровых щитовых приборов обеспечить возможность безопасного подключения калибровочного оборудования при проведении периодической калибровки в процессе эксплуатации СИ.

11. Автоматизированная система мониторинга и диагностики на момент ввода в эксплуатацию должна иметь действующие:

11.1. на момент согласования проектной документации:

- Свидетельства об утверждении типа СИ (допускается представление ссылок на утвержденные типы СИ в Федеральном информационном фонде обеспечения единства измерений ФГИС "Аршин");

11.2. на момент ввода в эксплуатацию:

- Свидетельства о поверке или оттиски поверительного клейма (допускается представление ссылок на поверенные СИ в Федеральном информационном фонде обеспечения единства измерений РСТ "Метрология");

11.3. положительное заключения аттестационной комиссии ПАО "Россети".

12. Требования к измерениям:

№ пп	Место выполнения измерений		Измеряемые вели		
			Ток, А	Напряжение, В (кВ)	Мощность активная, Вт (кВт, МВт)
1	РУ 20 кВ	ТСН	**1**	**1**	
2		ВЛ(КЛ)-20 кВ	**1**		**1**
3		Ввод-20 кВ	**3**		**1**
4		секция шин 20 кВ		**3**	
5	РУ 220 кВ	ВЛ-220 кВ	**3**		**1**
6		Ввод 220 кВ	**3**		**1**

Наименование мероприятия	Технологические решения

7		секция шин 220 кВ		**3**	

**1 – последовательное измерение параметра по фазам;
3 – параллельное измерение параметра по фазам.

13. Технические требования к щитовым приборам:
- габариты передней панели 120х120 мм;
- глубина не более 70 мм;
- возможность программирования коэффициента трансформации через кнопки управления на лицевой панели и индицирования коэффициента трансформации и измеряемого значения с учётом установленного коэффициента трансформации;
- должны быть оснащены интерфейсами RS485, USB (для подключения внешних устройств хранения информации, компьютера для сервисного обслуживания и т.п.);
- поддержка протокол МЭК 61850 (для работы в составе систем автоматизации и информационно-измерительных систем);
- отображающие на табло значения Uф, Uл, Iф, Iл, n, Q, P и cosφ;
- наличие аналогового выхода 4-20 мА;
- потребляемая мощностью не более 7 В*А;
- работа в температурном диапазоне –40°С до +50°С;
- относительная влажность воздуха не более 95% при температуре +35°С;
- напряжение питания – сеть переменного тока напряжением (85-240) В и частотой (45-65) Гц или постоянное напряжение (100-265) В;
- степень защиты по передней панели не хуже IP55;
- межповерочный интервал не менее 10 лет;
- класс точности не хуже 0,5;
- гарантийный срок службы не менее 60 мес;
- средний срок службы не менее 25 лет;
- срок наработки на отказ не менее 200 000 ч.;
- не имеют отрицательного опыта эксплуатации на энергообъектах ДЗО ПАО «Россети»;
- цвет индикаторов цифровых щитовых электроизмерительных приборов необходимо на стадии проектирования согласовать с филиалом;
- высота знака не менее 20 мм;
- приборы должны реализовывать функцию контроля минимального и максимального допустимых значений измеряемых величин. Выход измеряемой величины за установленные значения должен индицироваться световой индикацией на лицевой панели. Значения контролируемых

Наименование мероприятия	Технологические решения
	величин должны устанавливаться в условиях эксплуатации кнопками, установленными на передней панели; - входное сопротивление цепи измерения тока не более 20 мОм; - входное сопротивление цепи измерения напряжения не менее 1 МОм.
Качество электроэнергии	**1. Общие требования** 1.1. Тип прибора согласовать с Дирекцией метрологии и контроля качества электроэнергии на этапе проектирования. 1.2. В качестве приборов учета с функцией контроля качества электрической энергии на секции шин 20 кВ подстанции использовать «Binom 335» или аналогичные. 1.3. Приборы должны: - соответствовать классу А по ГОСТ 30804.4.30-2013 «Методы измерений показателей качества электроэнергии»; - обеспечивать измерение показателей качества электроэнергии в соответствии с ГОСТ 32144-2013 «Нормы качества электрической энергии в системах электроснабжения общего назначения»; - обеспечивать формирование протоколов качества электрической энергии в соответствии с действующими стандартами нормативной документации; - соответствовать требованиям МЭК 61850, в частности МЭК 61850-8-1 (MMS, GOOSE) и МЭК 61850-9-2 (SV). **2. Установка приборов** 2.1. Для обеспечения непрерывности измерений предусмотреть резервирование питания приборов контроля качества электроэнергии, устанавливаемых на подстанции, или подключение к источнику бесперебойного питания. 2.2. Предусмотреть резервирование информационных цепей ТН, используемых для контроля качества электроэнергии. 2.3. Для решения задач по компоновке и расположению приборов контроля качества электрической энергии и сопутствующего оборудования рекомендуется использовать типовые шкафы системы контроля качества электроэнергии. Приборы контроля качества электрической энергии должны устанавливаться на панелях, щитах, имеющих жесткую конструкцию. 2.4. Средства измерений (СИ) показателей качества электрической энергии должны быть внесены в Государственный реестр СИ, иметь сертификат об утверждении типа, действующие на момент ввода в эксплуатацию оттиски поверительных клейм или свидетельства о поверке (ст. 9 ФЗ РФ от 26.06.2008 г. №102-ФЗ «Об обеспечении единства измерений», п. 1.7 ПР 50.2.006-94 «Порядок проведения поверки

Наименование мероприятия	Технологические решения
	средств измерений»). В случае отсутствия действующих оттисков поверительных клейм или свидетельств о поверке провести метрологическое обеспечение средств измерений. **3. Передача данных** 3.1. Предусмотреть передачу данных с приборов контроля качества электрической энергии на АРМ ККЭ с установленным на нем программным обеспечением, позволяющим выводить на печать протоколы измерений качества электрической энергии. 3.2. Организовать удаленный доступ из отдела (сектора) контроля качества электроэнергии филиала ПАО «Россети Московский регион» – Московские высоковольтные сети через АСУ ТП к приборам контроля качества электроэнергии для получения информации. На компьютере АРМ в отделе контроля качества электроэнергии должно быть установлено программное обеспечение, соответствующее установленному типу приборов. **4. Требования к разработке проекта** 4.1. Проект «Качество электроэнергии» должен быть выполнен специализированной организацией, имеющей соответствующие лицензии, отдельным томом. Электронную копию проектной документации с разделом «Качество электрической энергии» представить в Дирекцию метрологии и контроля качества электроэнергии ПАО «Россети Московский регион». Проект должен быть согласован в филиале ПАО «Россети Московский регион» – Московские высоковольтные сети и утвержден в ПАО «Россети Московский регион». 4.2. Проект должен содержать: - Схему электрическую однолинейную с указанием точек контроля качества электрической энергии; - Структурную схему построения системы контроля качества электрической энергии; - Электрическую схему подключений СИ ПКЭ к ТТ и ТН; - Схему электрическую принципиальную питания системы контроля качества электрической энергии; - Схему электрическую принципиальную периферийного оборудования; - План, показывающий месторасположение шкафа контроля качества электроэнергии и электрических проводок, кабелей связи; - Чертеж, изображающий внешний вид шкафа контроля качества электроэнергии. **5. Требования к сдаче в эксплуатацию** 5.1. По окончании работ передать в филиал ПАО «Россети Московский регион» – Московские высоковольтные сети рабочую и эксплуатационную документацию на комплекс

Наименование мероприятия	Технологические решения
	контроля качества электрической энергии и комплект документов на приборы контроля качества электроэнергии с отметками или свидетельствами о поверке. 5.2. С целью подтверждения выполненных работ представить в Дирекцию метрологии и контроля качества электроэнергии ПАО «Россети Московский регион» протоколы измерений показателей качества электрической энергии по всем точкам контроля подстанции, оформленные в соответствии с действующими стандартами с рабочих мест отдела (сектора) контроля качества электроэнергии соответствующего филиала ПАО «Россети Московский регион».
Охранные мероприятия	В соответствии с требованиями Постановления Правительства Российской Федерации от 19.09.2015 №993 «Об утверждении требований к обеспечению безопасности линейных объектов топливно-энергетического комплекса» объект должен быть оснащен инженерно-техническими средствами охраны (ИТСО) в составе: 1. инженерно-технические средства защиты: 1.1. инженерные заграждения; 1.2. инженерные средства и сооружения; 1.3. контрольно-пропускные пункты (КПП); 1.4. помещения для размещения подразделений охраны. 2. технические средства охраны; 2.1. система автоматической охранной сигнализации периметра территории объекта (СПС) и внутренних помещений объекта (СОС); 2.2. система охранная телевизионная (СОТ); 2.3. система контроля и управления доступом (СКУД); 2.4. система сбора и обработки информации, в том числе подсистема связи и передачи извещений к пультам централизованного наблюдения (ССОИ). 3. вспомогательные системы и средства. 3.1. система охранного освещения (СОО); 3.2. система оповещения о тревоге, чрезвычайной ситуации и др.; 3.3. система электропитания. ИТСО должны поддерживать сопряжение друг с другом и представлять единую комплексную систему безопасности объекта, с передачей сигналов на диспетчерский пункт филиала или в инженерно-технический центр управления безопасностью. В целях обеспечения управления безопасностью и антитеррористической защищенностью объектов ПАО «Россети Московский регион» в единой системе ситуационно-аналитического управления, а также интеграции существующих и создаваемых систем управления безопасностью в ЦУБ

Наименование мероприятия	Технологические решения
	ПАО «Россети Московский регион», рекомендуется использование систем безопасности на базе ISS или LTV. При выборе оборудования учитывать совместимость поддержки протокола ONVIF, а также программного интерфейса интеграции приложений API.
Информационная безопасность	Применяется в случае модернизации, реконструкции или создания системы АСУ ТП (ТМ), СДТУ, АСМД, дистанционного управления КА и оборудованием РЗА. **Состав представляемых на рассмотрение материалов проектирования:** - анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии); - категории значимости объекта информационной инфраструктуры; - решения по организационным и техническим мерам обеспечения информационной безопасности объектов информационной инфраструктуры; - требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации; - требования к защите средств и систем, обеспечивающих функционирование объекта информационной инфраструктуры (обеспечивающей инфраструктуре); - требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями. Требования к предоставляемым материалам в части подсистемы **Информационной безопасности:** - Руководящие указания по установке и настройке средств защиты информации, настройке программных и программно-аппаратных средств безопасности объектов информационной инфраструктуры; - Руководящие указания по риск-ориентированному управлению объектами информационной инфраструктуры (ИТТ активами), организации в рамках процесса эксплуатации установки критических обновлений программного обеспечения для объектов; - Руководящие указания по конфигурации параметров программных и программно-аппаратных средств информационно-телекоммуникационной сети для обеспечения безопасности объектов информационной инфраструктуры, в том числе по обеспечению безопасного удаленного мониторинга

Наименование мероприятия	Технологические решения
	объектов информационной инфраструктуры Цифровой сети, организации удаленного доступа в информационно-телекоммуникационную сеть субъекта электроэнергетики; - Разработать и согласовать программу информирования и обучение персонала объекта информационной инфраструктуры; - Представить расчет нормативной численности персонала, ответственного за планирование и контроль мероприятий по обеспечению безопасности объекта информационной инфраструктуры, управление (администрирование) подсистемой информационной безопасности, управление средствами защиты информации, управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта, мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее - события безопасности), сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документах по безопасности значимого объекта; - Представить решения по централизованному управлению подсистемой безопасности объектов информационной инфраструктуры (при необходимости); - Разработать и согласовать план мероприятий по обеспечению безопасности объектов информационной инфраструктуры на случай возникновения нештатных (непредвиденных) ситуаций; - Разработать и согласовать проект Акта категорирования объекта критической информационной инфраструктуры. Материалы проектной и рабочей документации в части информационной безопасности согласовать с подразделением информационной безопасности Предприятия электрических сетей, Департаментом комплексной безопасности персонала, объектов и информационной безопасности ПАО «МОЭСК», а также иными заинтересованными лицами. <u>Требования по обеспечению информационной безопасности</u> Порядок создания подсистемы информационной безопасности, построение этапов работ, а также разработка технической и рабочей документации должны соответствовать ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения». Обеспечить создание подсистемы информационной безопасности, а также обеспечить выполнение:

Наименование мероприятия	Технологические решения
	- требований 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконных актов; - требований Приказа ФСТЭК от 14.03.2014 №31 - **не ниже 3 класса** защищенности автоматизированной системы управления; - требований РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» **не ниже уровня 1 Г**; - требований Распоряжения ПАО «Россети» от 01.04.2016 №140 «Об утверждении минимальных требований к информационной безопасности АСТУ» (в редакции распоряжения ПАО «Россети» от 27.04.2016 №178р и распоряжения ПАО «Россети» от 08.02.2019 №70р); - средства защиты информации должны соответствовать требованиям не ниже 6-го или более высокого уровня доверия («Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденные приказом ФСТЭК России от 02.06.2020 N 76). Применяемое оборудование должно быть включено в Реестр промышленной продукции, произведенной на территории Российской Федерации. Применяемое программное обеспечение должно быть включено в Единый реестр российских программ для электронно-вычислительных машин и баз данных. Применяемое оборудование и программное обеспечение средств информационной безопасности, сети передачи данных, АСУТП, ТМ должно быть сертифицированным ФСТЭК России и/или допущенным к применению на объектах ПАО "Россети", в соответствии с требованиями Приказа ПАО «Россети» от 28.07.2020 №329 «Об утверждении методики и порядка проведения проверки качества (аттестации) оборудования и типового регламента работы комиссии по допуску оборудования» и прошедшим проверку в соответствии с требованиями приказа ПАО «Россети» от 28.08.2020 №391 «Об утверждении Методики проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе». В случае модернизации, реконструкции или создания

Наименование мероприятия	Технологические решения
	автоматизированной системы мониторинга и диагностики энергетического оборудования, обеспечить выполнение требований Приказа Министерства энергетики РФ от 06.11.2018 №1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования». При проектировании и выполнении работ, учесть мероприятия, выполняемые в рамках смежных проектов. Тома проектной и рабочей документации в части информационной безопасности и тома в части защищаемых объектов информационной инфраструктуры (системы АСУ ТП, ТМ, СДТУ, АСМД, дистанционного управления КА и/или оборудования РЗА) согласовать со структурным подразделением информационной безопасности филиала и ДКБПОиИБ ИА Общества. Обеспечить комплексную защиту информации, определяющей режим функционирования и/или раскрывающей систему защиты конкретного объекта, в случае ее передачи за пределы контролируемой территории. 1. Оборудование структурных компонентов (функциональных систем и подсистем) систем обеспечения безопасности объекта, а также помещений, в которых размещаются центральный и локальные пульты управления с устанавливаемым в них оборудованием, должно проводиться с учетом реализации технических мероприятий по защите информации. 2. На структурные компоненты (функциональные системы и подсистемы) систем обеспечения безопасности объекта, разработать модели угроз для каждого типа энергообъекта. 3. Обеспечить целостность информации при передаче по внешним каналам связи по протоколу МЭК 670-5-101/104 с использование шифрования или технологии инспекции промышленных протоколов. 4. Обеспечить целостность информации при передаче по внешним каналам связи по протоколу МЭК 670-5-101/104 с использование шифрования. 5. Требования информационной безопасности, применяемые на всех объектах защиты: - в случае наличия парольной защиты доступа, все пароли по умолчанию должны быть изменены; - парольная политика к объектам защиты должна соответствовать установленным требованиям: по сложности

Наименование мероприятия	Технологические решения
	пароля (не менее 12 символов, наличие символов в разном регистре, наличие специальных символов), сроку действия паролей и истории паролей; - доступ персонала вне зависимости от объекта защиты должен быть персонализирован, необходимо исключить (при наличии технической возможности) возможность доступа к объектам защиты под одной учетной записью (одним паролем) для различных работников; - встроенные учетные записи на всех компонентах объектов защиты должны быть отключены; - высший приоритет применения на объектах защиты должны иметь механизмы доступа с применением многофакторной аутентификации; - незадействованный функционал и компоненты объектов защиты должны быть отключены; - на всех объектах защиты и их компонентах, должны быть включены и настроены функции регистрации событий безопасности с передачей на специально выделенный сервер сбора информации подсистемы мониторинга информационной безопасности; - по всем компонентам объектов защиты должны быть установлены процедуры обновлений безопасности, время применения обновления безопасности на компонентах объектов защиты не должно превышать 24 часов. 6. Требования информационной безопасности, применяемые к информационно-телекоммуникационной сети (далее - ИТС): - должен быть организован периметр технологического сегмента ИТС Объекта. Организация сетевого периметра ИТС Объекта должна быть обеспечена посредством межсетевых экранов; - физическое соединение технологического сегмента ИТС Объекта с остальной ИТС Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции межсетевого экранирования; - физическое соединение технологического сегмента ИТС Объекта с остальной ИТС Объекта при ее наличии, должно обеспечиваться только через устройство, реализующее функции межсетевого экранирования; - выделение сегментов должно обеспечиваться посредством, одновременного применения следующих технологий и методов в порядке эффективности защиты (при наличии такой возможности): - физическое выделение, посредством организации сегментов за счет выделенных коммутирующих устройств, подключаемых только к межсетевым экранам (наиболее защищенный вариант);

Наименование мероприятия	Технологические решения
	- с применением средств криптографической защиты доступа к сети и защиты трафика (VPN) при условии, что указанные средства в сегменте образуются посредством установки специализированного ПО на каждом из конечных узлов (серверов, АРМ); - VLAN; - VRF. - На каждом из Объектов в ИТС должны быть выделены сегменты управления: - сегмент управления ИТС (имеет доступ персонал, осуществляющий функции управления ИТС); - сегмент управления АСТУ (имеет доступ персонал, осуществляющий функции управления АСТУ); - сегмент управления подсистемами ИБ; - сегмент оперативного управления Объектом (имеет доступ персонал, осуществляющий оперативное управление оборудованием Объекта). - доступ к технологическому сегменту ИТС и другим входящим в него сегментам АС должен осуществляться только из сегмента оперативного управления. - взаимодействие сегментов должно ограничиваться следующими правилами: - доступ к сегментам управления из других сегментов запрещен; - взаимодействие между сегментами должно происходить исключительно через средства межсетевого экранирования; - взаимодействие между сегментами автоматизированных систем должно обеспечиваться в случае необходимости только посредством выделения специализированных выделенных «буферных» сегментов; - правила на межсетевых экранах должны быть максимально точными включая указание адресов назначения и источника, портов назначения и источника. - для взаимодействия с внешними сетями и АС должны создаваться «демилитаризованные» зоны – сегменты сети, в которые могут обращаться внешние «потребители» и из которых исключена возможность инициации соединений во внутренние сегменты сети Объекта; - служебные протоколы оборудования образующего ИТС, должны быть доступны только из сегмента управления ИТС; - должны быть отключены неиспользуемые и небезопасные (передающие информацию по сети в открытом, незашифрованном виде) протоколы и сервисы на сетевом оборудовании; - неиспользуемые порты на коммутационном оборудовании

Наименование мероприятия	Технологические решения
	должны быть отключены логически и физически; - доступ на уровне ИТС должен осуществляться в случае необходимости дополнительных мер с применением протоколов 802.1x и фильтрации MAC адресов; - устройства беспроводной связи должны находиться физически и логически за организованным периметром ИТС Объекта; - технологические протоколы необходимо строго изолировать от внешнего проникновения; - на сетевом оборудовании должны быть включены функции от подмены сетевых адресов и меры защиты от внедрения ложной маршрутной информации в протоколы маршрутизации; - должен быть включен сбор событий на уровне трафика в сети и передаваться на сервер подсистемы мониторинга информационной безопасности для контроля легитимности сетевых соединений. 7. Требования информационной безопасности, применяемые к автоматизированным системам (далее АС): - каждая АС должна быть изолирована, от других АС, при необходимости взаимодействия с другими АС, взаимодействие должно быть обеспечено методами исключающими возможность его использование в деструктивных целях для обоих АС; - при необходимости сбора необходимой информации с АС, указанные АС должны позволять передавать информацию посредством отправки технологической и другой информации инициируя соединения самостоятельно (по примеру протокола Syslog). Методы в виде опроса сервисов, баз данных и т.д. систем должны быть исключены; - должно обеспечиваться резервирование конфигураций и баз данных АС; - все применяемые АС должны иметь актуальную и доступную проектную и эксплуатационную документацию; - в целевом исполнении АС должны иметь механизмы электронной подписи и криптографической защиты информации, а также должны обладать процедурами двойного контроля или паритета ответственности, когда выполнение критических действий невозможно выполнить одновременно одним лицом; - прямой доступ к базам данных АС должен быть исключен; - территориально распределенные АС, с выведенным функционалом по управлению на централизованное удаление управление в частности АСТУ, должны позволять осуществлять перевод управления на нижний (местный, Объектовый уровень). Функция отключения указанного внешнего управления должна

Наименование мероприятия	Технологические решения
	гарантировать исключение возможности включения удаленного управления из вне; - при выполнении контроля за АС необходимо обеспечить контроль за всеми ее компонентами на каждом конкретном Объекте (уровень системного программного обеспечения, уровень прикладного программного обеспечения (далее - ПО), уровень баз данных). 8. Требования информационной безопасности, применяемые к автоматизированным рабочим местам (далее АРМ) и серверам: - На серверах АС и АРМ в обязательном порядке должны быть установлены средства антивирусной защиты с актуальными обновлениями; - Должна быть исключена возможность использования внешних устройств беспроводной связи на серверах и АРМ (блокировка необходимых портов как физически так и логически); - Подключение внешних устройств хранения данных по умолчанию должно быть запрещено, подключение должно быть вызвано потребностью технологического бизнес-процесса и только на ограниченное время с контролем со стороны работника службы безопасности; - Должны быть включены пароли на доступ к встроенному ПО (BIOS, UEFI, сервисы управления) серверов и АРМ; - Должен применяться только необходимый и согласованный состав ПО на АРМ и серверах. При наличии возможности со стороны средств безопасности установленных на АРМ и серверах должна быть реализована политика белых списков в отношении, используемого ПО; - В целом исполнении доступ к АРМ и серверам должен обеспечиваться посредством средств многофакторной аутентификации; - Подключение к сети Интернет АРМ, с которых осуществляется выполнение критических операций должно быть запрещено; - Должен производиться контроль за хранением на серверах и АРМ парольной информации. В случае выявления должны быть инициированы проверки целостности скомпрометированных узлов и незамедлительная замена парольной информации для всех учетных записей, а также ревизия учетных записей; - На всех АРМ и серверах должны быть включены персональные межсетевые экраны с правилами минимально необходимыми для функционирования объектов защиты. Весь остальной сетевой доступ должен быть заблокирован. 9. Требования к оборудованию:

Наименование мероприятия	Технологические решения
	- На всем технологическом оборудовании Объекта и оборудовании безопасности имеющим функции управления, должны быть максимально использованы функции безопасности при их наличии; - Оборудование должно подключаться только к своим сегментам ИТС; - Неиспользуемый функционал и интерфейсы связи должны быть отключены. 10. Требования к подсистемам информационной безопасности: Минимальный состав подсистем ИБ должен состоять из: - подсистемы антивирусной защиты; - подсистемы межсетевого экранирования ИТС и конечных узлов; - подсистемы анализа сетевого трафика и обнаружения компьютерных атак; - подсистемы мониторинга информационной безопасности (централизация сбора и анализа событий безопасности регистрируемых на конечных узлах Объекта с целью контроля и выявления нарушений). Предусмотреть сбор событий информационной безопасности для передачи в САЦ сетевой компании. Необходимость разработки мероприятий защиты информации для каждого конкретного объекта определяется по результатам предпроектного обследования. Использовать отдельные туннелированные каналы связи (стандарт VPN) для телеизмерений, учёта и качества электроэнергии, средств физической безопасности). Создаваемые в рамках проводимых работ центральные и удаленные пульты управления безопасностью должны быть аттестованы на предмет соответствия требованиям РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1Г. **Исполнитель (соисполнитель) работ должен отвечать следующим требованиям по наличию:** - Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно п.п. б), г), д), е) ст.4 Положения введенного Постановлением Правительства РФ 2012 года №79; - Лицензии ФСБ на осуществлении работ по пунктам 2, 3, 8, 9, 12-14, 21-23 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств».

Наименование мероприятия	Технологические решения
	Нормативно-технические документы (НТД), определяющие требования к оформлению и содержанию проектной документации (ПД): - Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». - Политика ПАО «Россети» в области информационных технологий, автоматизации и телекоммуникаций (Политика ИТТ, утверждена Советом директоров ПАО «Россети» (Протокол от 11.09.2017 №276). - ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
Системы технологического видеонаблюдения	1. На подстанции провести обследование мест расположения первичного оборудования. Определить места установки видеокамер системы технологического видеонаблюдения. 2. Система технологического видеонаблюдения должна обеспечивать: - визуальный контроль помещений ЗРУ и ОРУ цифровой ПС с основным технологическим оборудованием; - визуальный контроль за работой и состоянием отдельных элементов, функциональных узлов и измерительных приборов оборудования; - визуальный контроль за помещениями оборудованными системами пожаротушения с анализом видеоинформации и формированием тревожных сигналов (визуальное обнаружение возгорания, наличие людей в защищаемом помещении, визуальный контроль работы систем противопожарной защиты); - визуальный контроль зон установки шкафов с микропроцессорным оборудованием и шкафов управления; - визуальный контроль положения дистанционно управляемых коммутационных аппаратов на ОРУ, ЗРУ; - визуальный контроль за безопасным выполнением работ персоналом ремонтных бригад в помещениях с повышенной опасностью, ОРУ, ЗРУ. 3. Результаты обследования согласовать с ПАО «Россети Московский регион». 4. Обеспечить сбор в систему АСУТП и отображение на АРМ ОП видеосигнала от системы технологического видеонаблюдения. Экранные формы отображения видеоинформации определить на этапе проектирования и согласовать с ПАО «Россети Московский регион». 5. Система технологического видеонаблюдения должна обеспечивать в автоматическом режиме позиционирование видеокамер на зону, в которой произошло срабатывание

Наименование мероприятия	Технологические решения
	сигнализации (в том числе, при получении информации из АСУТП о срабатывании датчиков открытия дверей шкафов и т.д.) и вывод соответствующего изображения на АРМы диспетчера (в том числе удаленного). При выполнении операций с коммутационной аппаратурой или срабатыванием устройств РЗА должно обеспечиваться позиционирование видеокамер на коммутационный аппарат или на оборудование, на котором произошло короткое замыкание или сработали датчики технологических защит. 6. Видеокамеры, устанавливаемые в помещениях, должны быть цифровыми, передавать данные по протоколу IP, не иметь встроенных возможностей беспроводной передачи данных, с наличием объектива с автоматической регулировкой диафрагмы и функцией ночного видения. 7. Видеокамеры, устанавливаемые на открытом воздухе, должны быть цифровыми, передавать данные по протоколу IP, не иметь встроенных возможностей беспроводной передачи данных, с наличием объектива с автоматической регулировкой диафрагмы, размещаться в кожухе, иметь солнцезащитный козырек, обеспечивать надежную работу в соответствующих климатических условиях, обеспечены устройствами грозозащиты. 8. Система технологического видеонаблюдения должна взаимодействовать с системой противопожарной защиты и обеспечивать приоритетное отображение на экране монитора зоны, из которой поступил сигнал тревоги. 9. Устройства контроля и управления должны обеспечивать последовательное и полиэкранное воспроизведение изображений от всех видеокамер, а также возможность одновременного просмотра и записи поступающих видеосигналов. 10. Видеокамеры должны обеспечивать возможность передачи изображения и управления с рабочего места удаленного пользователя после прохождения индивидуальной аутентификации пользователем. 11. Разрешение видеокамер должно обеспечивать на мониторах четкое изображение поступающих видеосигналов. 12. Электропитание устройств видеонаблюдения должно осуществляться от сети 220 В через устройство бесперебойного питания, работающее в режиме «ON-LINE».
Пожарная безопасность	1. Разработать раздел проектной документации «Мероприятия по обеспечению пожарной безопасности» в соответствии с требованиями Постановления Правительства Российской Федерации от 16.02.2008 года №87 «О составе разделов проектной документации и требованиях к их

Наименование мероприятия	Технологические решения
	содержанию». 2. Для обеспечения пожарной безопасности в проектной документации обосновать: - противопожарный разрыв или расстояние от проектируемого здания или сооружения, электротехнического оборудования до ближайшего здания, сооружения или наружной установки; - принимаемые значения характеристик огнестойкости и пожарной опасности элементов строительных конструкций и систем инженерно-технического обеспечения; - принятое разделение здания или сооружения на пожарные отсеки; - расположение, габариты и протяженность путей эвакуации людей при возникновении пожара, обеспечение противодымной защиты путей эвакуации, характеристики пожарной опасности материалов отделки стен, полов и потолков на путях эвакуации, число, расположение и габариты эвакуационных выходов; - характеристики или параметры систем обнаружения пожара, оповещения и управления эвакуацией людей при пожаре, а также автоматического пожаротушения и систем противодымной защиты (при наличии); - меры по обеспечению возможности проезда и подъезда пожарной техники, безопасности доступа личного состава подразделений пожарной охраны и подачи средств пожаротушения к очагу пожара, параметры систем пожаротушения, в том числе наружного и внутреннего противопожарного водоснабжения; - организационно-технические мероприятия по обеспечению пожарной безопасности здания или сооружения в процессе их строительства и эксплуатации. 3. При установке противопожарных систем применять оборудование, позволяющее осуществлять его дистанционную настройку, управление и мониторинг состояния. 4. Приложить расчет категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности, выполненный только расчетом в соответствии с действующими нормативными документами с учетом проектируемых технологических процессов, используемых технологических сред, геометрических размеров помещений, способов размещения, фактического количества и физико-химических параметров пожарной нагрузки. 5. При проектировании обеспечить выполнение требований действующих федеральных нормативных документов в сфере пожарной безопасности, ведомственных норм технологического проектирования электросетевых предприятий, стандартов

Наименование мероприятия	Технологические решения
	организации ПАО «Россети».
Энергетическая эффективность	1. Определить расход электрической энергии на собственные нужды ПС и расход электрической энергии на хозяйственные нужды с учетом: а) расчёта для выбранного типа (авто)трансформаторов расхода электрической энергии на технические потери и систему охлаждения при запланированном цикле нагрузки; б) выполнения сравнения на примере как минимум двух (авто)трансформаторов аналогичной мощности с улучшенными характеристиками по энергоэффективности. Если разница издержек основного и одного из альтернативных вариантов превышает разницу в стоимости таких вариантов в течение срока менее 7 лет, такой альтернативный вариант рекомендовать к установке (предпочтение отдается такому альтернативному варианту, разница стоимости которого по отношению к основному варианту покрывается за счет меньших технологических потерь). 2. Расчет технических потерь электрической энергии выполнить на основании методики расчета и обоснования нормативов технологических потерь электроэнергии при ее передаче по электрическим сетям, утвержденной приказом Министерства энергетики Российской Федерации от 30.12.2008 №326, в программном комплексе РТП 3 с учетом коэффициента загрузки (авто)трансформатора равного 0,4. Допускается принять другой коэффициент загрузки при условии его обоснования в работе. Время работы (авто)трансформатора принять 8760 часов/год. Расход электрической энергии на системы охлаждения (авто)трансформаторов принять согласно Инструкции по нормированию расхода электроэнергии на собственные нужды подстанции (РД 34.09.208). При отсутствии в инструкции данных по требуемому типу системы охлаждения информацию получить у производителя. 3. Выполнить подключение энергопринимающих устройств, не относящихся к собственным нуждам подстанции, к щиту хозяйственных нужд подстанции и организовать отдельный учет потребления электроэнергии на хозяйственные нужды в соответствии с Типовой инструкцией по учету электроэнергии при ее производстве, передаче и распределении (РД 34.09.101-94). 4. Обеспечить установку автоматики включения/отключения по температурному режиму на отопительные приборы и устройства кондиционирования подстанции в помещениях, используемых обслуживающим персоналом (общеподстанционный пункт управления, складские помещения, помещения используемые персоналом

Наименование мероприятия	Технологические решения
	подразделений РЗА). 5. Предусмотреть установку энергоэффективного освещения. В туалете, коридорах, на лестницах и в складских помещениях установить автоматику отключения освещения. 6. Предоставить на рассмотрение и согласование в ПАО «Россети Московский регион» том, содержащий раздел «Энергетическая эффективность», в электронном виде. Проектная документация с поясняющими рисунками и схемами предоставляется в формате *.pdf (Adobe Acrobat Reader) без защиты содержимого с возможностью работы с текстом (поиск, копирование, печать) в электронном виде. Не допускается передача документации в формате Adobe Acrobat Reader с пофайловым разделением страниц. Предоставить на рассмотрение и согласование расчетные модели, использованные для проведения расчетов технических потерь электрической энергии, в электронном виде в формате программного комплекса РТП 3 (*.fdb) на CD с применением пароля для защиты от несанкционированного доступа.
Инженерно-обеспечивающие системы	1. Строительные конструкции зданий и инженерных сооружений электрических объектов должны обеспечивать требуемую надежность при их сроке эксплуатации не менее 50 лет. 2. В качестве фундаментов под оборудование следует применять облегченные предварительно - напряженные железобетонные стойки, сплошные блоки из тяжелого бетона, железобетонные сваи, монолитные и винтовые сваи. 3. Стальные опоры под оборудование, а также стальные детали железобетонных стоек порталов и опор под оборудование должны быть защищены от коррозии на заводах-изготовителях с применением технологии горячего цинкования. 4. При устройстве фундаментов под трансформаторы и маслоприемных устройств маслонаполненного оборудования использовать метод заливного армированного бетона с использованием полимерных добавок для улучшения характеристик бетона. 5. При устройстве маслохозяйства (маслоприемников, маслоотводов) необходимо руководствоваться требованиями ПУЭ 6-7 изд. (п.4.2.69). 6. Дно маслоприемника аварийного слива масла от трансформатора должно иметь уклон не менее 0,005 в сторону приямка с засыпкой гравием только отводящего приямка по металлической решетке, что выполняет роль огнепреградителя. 7. Для защиты железобетонных фундаментов от воздействия агрессивных сред в зависимости от степени этого воздействия следует применять соответствующие марки бетона по

Наименование мероприятия	Технологические решения
	водонепроницаемости W8 и морозостойкости F200, а также бетон на сульфато-стойком цементе. 8. В качестве дополнительной защиты при необходимости может применяться покрытие фундаментов гидроизоляцией (в том числе их надземной части) в соответствии с действующими нормами. 9. При обустройстве территории ОРУ спланировать территорию. 10. В местах проезда специализированного транспорта устроить асфальтовое или бетонное (возможно использование дорожных плит) дорожное покрытие.
Освещение	При проектировании освещения подстанции необходимо предусмотреть применение энергосберегающих светодиодных светильников со сроком службы не менее 10 лет. Периметральное освещение должно включаться вручную и автоматически от датчика освещенности. Освещение ОРУ и внутриподстанционных площадок должно включаться вручную. Запрещено применение светильников и указателей со встроенными аккумуляторными батареями, все аварийные осветительные и указательные приборы должны быть запитаны от СОПТ в послеаварийном режиме, все указанные приборы должны иметь возможность питания переменным и постоянным током 220 В. Выключатели основного освещения в помещениях должны быть установлены в ряду ближе к входной двери, аварийного – дальше. На лестничных клетках, а также в проходных помещениях необходимо устанавливать систему проходного управления светом. Схема питания освещения ОРУ должна быть кольцевой с обеспечением возможности вывода из работы любого участка кабельной линии и осветительного прибора.
Мероприятия по охране окружающей среды	В соответствии с Федеральным законом от 10.01.2002 №7-ФЗ «Об охране окружающей среды» и другими действующими нормативными документами предусмотреть мероприятия по предотвращению и (или) снижению возможного негативного воздействие электросетевого объекта (подстанции) на окружающую среду на период проведения строительных работ и последующей эксплуатации. Проектирование вести по результатам выполненных инженерно-экологических изысканий. В соответствии с действующими нормативными документами разработать разделы проектной документации: - Перечень мероприятий по охране окружающей среды;

Наименование мероприятия	Технологические решения
	- Дендрологическая часть проекта (при необходимости); - Проект благоустройства и озеленения (при необходимости). Содержание раздела 8 «Перечень мероприятий по охране окружающей среды» выполнить согласно Постановлению Правительства РФ от 16.02.2008 №87 «О составе разделов проектной документации и требованиях к их содержанию» (п. 25). Выделить подразделы с описанием мероприятий по отдельным компонентам окружающей среды (воздух, вода, почва, отходы, растительный и животный мир). Представить полный перечень отходов, образующихся в период строительства. Указать, что все образующиеся отходы передаются по договорам организациям, имеющим лицензии на обращение с данными видами отходов. В графической части представить ситуационный план (карту-схему) с указанием размещения проектируемых объектов, границ зон с особыми условиями использования территории (ООПТ, водоохранных зон и т.д.), местоположением ближайших к участку проектирования нормируемых объектов (жилой застройки).
Благоустройство	Работы по благоустройству территории необходимо проводить после окончания строительно-монтажных работ. Перед началом работ по благоустройству необходимо осуществить вывоз всех образовавшихся в ходе проведения работ строительных отходов, оборудования и др., освободить площадки от временных зданий и сооружений, очистить площадки от дренирующих и щебеночных грунтов, спланировать поверхности в существующих отметках. Перечень работ по благоустройству должен включать в себя восстановление и устройство дорожных покрытий, проездов, дорожек, тротуаров и газонов для территорий различного функционального назначения. При планировании работ по благоустройству территорий необходимо учитывать требования: - Постановление Правительства РФ от 16.02.2008 №87 (ред. от 27.05.2022) "О составе разделов проектной документации и требованиях к их содержанию"; - СП 82.13330.2016. Свод правил. Благоустройство территорий. Актуализированная редакция СНиП III-10-75; - СП 68.13330.2017. Свод правил. Приемка в эксплуатацию законченных строительством объектов. Основные положения. Актуализированная редакция СНиП 3.01.04-87»; - ГОСТ 17.5.3.04-83. Государственный стандарт Союза ССР. Охрана природы. Земли. Общие требования к рекультивации земель"; и др.

Наименование мероприятия	Технологические решения
Требования по установлению санитарно-защитных зон	Отдельным томом разработать проект санитарно-защитных зон объекта, согласовать его и подготовить пакет документов для установлении санитарно-защитных зон и направления в уполномоченный орган в целях принятия решения об установлении санитарно-защитных зон.

8. Требования к оформлению и содержанию проектной документации.

Проектирование выполнить согласно требованиям Типового ЗП (распоряжение №628р от 17.11.2017).

Проектирование выполнить в соответствии с Постановлением Правительства РФ №87 от 16.02.2008 (с изменениями и дополнениями) "О составе разделов проектной документации и требованиях к их содержанию" и в соответствии с ГОСТ Р 21.1101-2013 СПДС. Основные требования к проектной и рабочей документации.

Проектная документация должна быть согласована с:

- ПАО «Россети Московский регион»;
- филиалом ПАО «Россети Московский регион» - «Московские высоковольтные сети»;
- Центральным Управлением по технологическому и экологическому надзору Ростехнадзора по Центральному Федеральному Округу;
- Московским РДУ;
- Главным управлением культурного наследия (при необходимости - государственной историко-культурной экспертизой);
- Межрегиональным территориальным управлением воздушного транспорта центральных районов Федерального агентства – в случае размещения объекта в границах ЗОУИТ - приаэродромной территории;

и другими заинтересованными организациями.

При проектировании необходимо руководствоваться последними редакциями документов, действующих на момент разработки проектно-сметной документации.

До начала разработки проектной документации Проектировщик разрабатывает и согласовывает с Заказчиком состав проекта, в соответствии с которым осуществляется дальнейшее проектирование и приемка выполненных работ.

В части «Цифровых подстанций»:

1. Состав предоставляемых на согласование АО «СО ЕЭС» материалов (оформляются отдельным(ми) томом(ами)):

а) схемы распределения устройств информационно-технологических систем по ТТ и ТН (включая устройства РЗА, АСУ ТП (ССПИ, ТМ), АИИС КУЭ, СМиУКЭ) на объекте проектирования и на объектах, технологически связанных с объектом проектирования (в объеме распределительного устройства с присоединениями, на которых создаются или модернизируются устройства РЗА) с отражением функций;

б) функциональные блок схемы взаимодействия устройств РЗА между собой и с внешними устройствами, на которых в графическом виде должны быть представлены все коммуникации между устройствами РЗА, преобразователями аналоговых сигналов и преобразователями дискретных сигналов;

в) принципиальные, функционально-логические схемы и схемы программируемой логики устройств РЗА;

г) ориентировочный расчет параметров срабатывания устройств РЗ, СА, ПА и необходимые для этого расчеты токов КЗ;

д) решения по регистрации аварийных событий и процессов;

е) схемы организации передачи сигналов и команд РЗА (ВОЛС, ВЧ каналы, другое) с учетом резервирования каналов, а также схему организации передачи доаварийной информации для ПА с учетом резервирования каналов;

ж) схемы организации цепей оперативного тока устройств РЗА.

2. Отдельным(ми) томом(ами) выполнить/определить/подготовить:

2.1 Функциональные блок схемы взаимодействия вновь устанавливаемых типовых шкафов между собой (с учетом структурно-функциональных схем типовых шкафов), с существующими устройствами (комплексами) РЗА, коммутационными аппаратами, ТТ и ТН:

а) наименования сигналов в семантике серии стандартов МЭК 61850 с указанием передаваемых объектов/атрибутов данных;

б) используемых коммуникационных сервисов передачи данных (Sampled Values, GOOSE, Report и др.).

2.2. Файл SSD (System Specification Description) с описанием однолинейной схемы объекта проектирования, а также распределения логических узлов первичного оборудования и функций вторичных подсистем по присоединениям в синтаксисе языка SCL (System Configuration Language).

2.3. Файл SCD с описанием схемы распределения логических узлов первичного оборудования и функций.

2.4. Предусмотреть для устройств (комплексов) РЗА, в части цифровых коммуникаций, селективную сигнализацию о неисправности связей по отдельным GOOSE/Sampled Values-сообщениям с выводом информации на МП устройство РЗА и в АСУ ТП по отказавшему соединению.

2.5. Структурную схему АСУ ТП с отражением топологии ЛВС, применяемых устройств (комплексов) РЗА, используемых протоколов резервирования в сети и точной синхронизации времени.

2.6. Распределение информационных потоков данных по шине станции и шине процесса.

2.7. Предусмотреть установку системы мониторинга сетевого трафика и контроля соответствия передачи данных по протоколам GOOSE, Sampled Values и MMS электронному проекту (SCD-файлу) с мониторингом аномальных режимов и регистрацией событий на основе сообщений GOOSE/Sampled Values, включающую в себя в том числе:

а) оценку текущей загруженности ЛВС;

б) анализ сообщений протоколов GOOSE, Sampled Values и MMS на предмет потери или искажения пакетов;

в) анализ конфигурации информационной сети (анализ соответствия сети SCD-файлу);

г) контроль появления MAC-адресов в информационной сети для обеспечения информационной безопасности;

д) контроль появления не авторизированных сообщений в сети (белый шум);

е) выдача сигнализации о неисправностях и ошибках сети в АСУ ТП;

ж) блокировка портов коммутаторов (критерии блокировки определить при проектировании).

2.8. Расчет загруженности ЛВС с учетом выбранной топологии информационной сети и максимальной загрузки в режиме повышенной информационной нагрузки «шторм».

2.9. Отдельной спецификацией необходимо представить наименования сигналов в семантике серии стандартов МЭК 61850 и соответствующее им наименование из поля «Описание» (Description).

9. Особые условия.

Проектная организация предоставляет ПАО «Россети Московский регион» все расчетные модели (включая графические схемы), использованные для проведения расчетов электроэнергетических режимов и токов короткого замыкания в форматах программных комплексов, с помощью которых проведены расчеты

Оформление текстовых и графических материалов, входящих в состав проектной документации, выполнить в соответствии с приказом Минрегиона России от 02.04.2009 №108 «Об утверждении правил выполнения и оформления текстовых и графических материалов, входящих в состав проектной и рабочей документации».

Согласование документации осуществляется в системе «Архив ПСД» с заведением документации в электронном виде через личный кабинет Проектировщика.

Проектирование выполнить согласно требованиям Типового ЗП, (распоряжение №628р от 17.11.2017).

В соответствии с «Инструкцией по порядку согласования сметной документации по объектам строительства Общества», утвержденной приказом ПАО «Россети Московский регион» от 24.08.2020 №857, сметная документация, после получения положительного заключения экспертизы, подлежит проверке в департаменте ценового контроля ПАО «Россети Московский регион» (п.3.2, п.3.5.1).

10. Выделение этапов строительства.

Возможность подготовки проектной документации в отношении отдельных этапов строительства должна быть обоснована расчетами, подтверждающими технологическую возможность реализации принятых проектных решений при осуществлении строительства по этапам.

Проектная документация в отношении отдельного этапа строительства разрабатывается в объеме, необходимом для осуществления этого этапа строительства. Указанная документация должна отвечать требованиям к составу и содержанию разделов проектной документации, установленным постановлением Правительства Российской Федерации от 16.02.2008 №87, для объектов капитального строительства.

Под этапом строительства понимается строительство одного из объектов капитального строительства, строительство которого планируется осуществить на одном земельном участке, если такой объект может быть введен в эксплуатацию и эксплуатироваться автономно, то есть независимо от строительства иных объектов капитального строительства на этом земельном участке, а также строительство части объекта капитального строительства, которая может быть введена в эксплуатацию и эксплуатироваться автономно, то есть независимо от строительства иных частей этого объекта капитального строительства.

При необходимости неодновременной подачи на государственную экспертизу проектной документации по выделенным этапам строительства проектную документацию на каждый этап строительства сформировать отдельными

комплектами в соответствии с требованиями постановления Правительства Российской Федерации от 16.02.2008 №87 «О составе разделов проектной документации и требованиях к их содержанию».

Выделение работ по демонтажу зданий, строений, сооружений и т.п. в отдельный этап строительства, который не содержит строительство (реконструкцию) объектов, подлежащих вводу в эксплуатацию на таком этапе строительства, запрещается.

11. Исходные данные для разработки проектной документации.

Перечень исходных данных, сроки их подготовки и передачи определяются условиями Договора на разработку проектной документации и календарным графиком. Получение исходных данных проектной организацией выполняется с выездом на объекты. Заказчик обеспечивает организационную поддержку доступа представителей проектной организации для получения информации.

Исходные данные, передаваемые Заказчиком Проектной организации:

- ТУ на ТП №И-23-00-624621/102 от 15.06.2023;
- Настоящее ЗП;
- Типовое ЗП (распоряжение №628р от 17.11.2017).

Исходные данные предоставляются по письменному запросу от Проектной организации.

12. Прочие сведения.

12.1. Документация, передаваемая проектной организацией заказчику.

Сформировать и передать заказчику комплекты документации в полном объеме, в том числе:

Проектная и рабочая документация, согласованная в установленном порядке (комплект с согласованиями) передается заказчику в следующем количестве:

- бумажная версия – по 2 экземпляра;
- электронная версия в формате *.pdf (цвет, с согласованиями, с разбивкой по томам, каждый том отдельным файлом) – 3 экземпляра на 3-х компакт дисках (в т.ч. 2 экз. – для торгово-закупочных процедур);
- электронная версия в системе AutoCAD (*.dwg) и текстовые документы в системе MS Office – 1 экземпляр.

Сметная документация передается заказчику в следующем количестве:

- бумажная версия – 2 экземпляра;
- электронная версия в формате *.pdf – 3 экземпляра на 3-х компакт дисках (в т.ч. 2 экз. – для торгово-закупочных процедур);
- электронная редактируемая версия сметной документации:
- в формате Smeta.ru (*.sob) – 1 экз.;
- в формате АРПС 1.10. (*.apr) – 1 экз.;
- в формате MS Office Excel – 1 экз.

Количество экземпляров передаваемой проектной организацией заказчику по договору должно соответствовать указанному в ЗП.

12.2. Разработка программы ПНР и комплексного опробования (индивидуальных испытаний) оборудования.

При необходимости, разработать отдельным томом программу ПНР. Объем и нормы испытаний электрооборудования и ПНР определить проектом в соответствии с требованиями СНиП 3.05.06-85 «Электротехнические устройства», производителей

оборудования, ПУЭ «Правила устройства электроустановок».

Выполнить сметный расчет согласно требованиям МДС 81-40.2006 (Указания по применению федеральных единичных расценок на пусконаладочные работы) и ТСН-2001.5.

12.3. Авторский надзор.

Авторский надзор осуществлять на протяжении всего периода строительства и ввода объекта капитального строительства в эксплуатацию в соответствии с требованиями свода правил СП 246.1325800.2016 «Положение об авторском надзоре за строительством зданий и сооружений», утвержденных Приказом Минстроя России от 19.02.2016 №98/пр.

12.4. Требования по обеспечению защиты сведений, составляющих государственную тайну.

При получении инженерно-геодезических изысканий, выполненных на секретной геоподоснове, либо использование иных документов, содержащих секретные сведения, необходимо при выполнении работ обеспечить соблюдение требований законодательных и иных нормативных актов Российской Федерации по обеспечению защиты сведений, составляющих государственную тайну.

Обеспечить выполнение требований закона РФ от 21.07.1993 №5485-1 «О государственной тайне».

12.5. Согласование проекта.

Согласование документации с Московским РДУ выполняет ПАО «Россети Московский регион».

Согласование документации с остальными организациями, указанными в разделе 8, всеми землепользователями и другими заинтересованными организациями выполняет Проектная организация.

Не допускается передача проектной документации в ГАУ «Московская государственная экспертиза» (Мособлэкспертиза) до согласования ее с ПАО «Россети Московский регион» и Московским РДУ в полном объеме.

Срок действия настоящего ЗП составляет: 5 лет с момента утверждения.