Общество с ограниченной ответственностью
«НОВЫЕ РЕСУРСЫ»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

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

Подраздел 5. Сети связи

Часть 4. Информационная безопасность

Книга 1. Производство полистирола и объекты общезаводского хозяйства

NKNH21002-ПС-ЭБСМ-ИОС5.4.1

Том 5.5.4.1

2024

Общество с ограниченной ответственностью
«НОВЫЕ РЕСУРСЫ»

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

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

Подраздел 5. Сети связи

Часть 4. Информационная безопасность

Книга 1. Производство полистирола и объекты общезаводского хозяйства

NKNH21002-ПС-ЭБСМ-ИОС5.4.1

Том 5.5.4.1

Руководитель проектов **А.А. Стариков**
(подпись, дата)

Главный инженер проекта **Д.И. Вавилов**
(подпись, дата)

2024

Взам. инв. №

Подп. и дата

Инв. № подл.

ООО «Платформикс»

Платформикс

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

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

Подраздел 5. Сети связи

Часть 4. Информационная безопасность

Книга 1. Производство полистирола и объекты общезаводского хозяйства

NKNH21002-ПС-ЭБСМ-ИОС5.4.1

Том 5.5.4.1

Руководитель проектов	(подпись, дата)	**Е.Ю. Виннер**
Главный инженер проекта	(подпись, дата)	**К.А. Зац**

2024

Взам. инв. №

Подп. и дата

Инв. № подл.

СОДЕРЖАНИЕ ТОМА

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.1-С		
Разраб.		Зац			11.10.24	Содержание тома	Стадия	Лист	Листов
							П		1
Н. контр.		Чекалёв			11.10.24		Платформикс		
ГИП		Зац			11.10.24				

ООО «Платформикс»

Платформикс

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Ведомость проекта

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-В

2024

ВЕДОМОСТЬ ПРОЕКТА

Обозначение	Формат	Наименование	Приме-чание
NKNH21002-ПС-ЭБСМ-ИОС5.4.1-П2	А4	Пояснительная записка по СОИБ	Лист 5
NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С2	А3	Схема функциональной структуры	Лист 98
NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С1	А3	Структурная схема комплекса технических средств СОИБ	Лист 99
NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С7	А4	Схема расположения оборудования в Аппаратной	Лист 100
NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-СА	А4	Чертежи установки технических средств	Лист 101

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.1-В		
Разраб.		Зац			11.10.24	Ведомость проекта	Стадия	Лист	Листов
							П		1
Н. контр.		Чекалёв			11.10.24		Платформикс		
ГИП		Зац			11.10.24				

ООО «Платформикс»

Платформикс

Заказчик – **ПАО «Нижнекамскнефтехим»**

«Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

ПРОЕКТНАЯ ДОКУМЕНТАЦИЯ

Пояснительная записка

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-П2

2024

СОДЕРЖАНИЕ

Лист

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.1-П2		
Разраб.		Зац			11.10.24	Пояснительная записка	Стадия	Лист	Листов
							П	1	92
Н. контр.		Чекалёв			11.10.24		Платформикс		
ГИП		Зац			11.10.24				

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Наименование системы

Полное наименование системы – Система обеспечения информационной безопасности Интегрированной системы управления и безопасности производства этилбензола мощностью 350 тыс. тонн и производства стирола мощностью 400 тыс. тонн в год на площадке ПАО «НКНХ» и Интегрированной системы управления и безопасности производства полистирола мощностью 250 тыс. тонн в год и общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год на площадке ПАО «НКНХ».

Сокращенное наименование – СОИБ.

1.2 Общие сведения

Основанием для выполнения проекта является Техническое задание на проектирование объекта «Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», утвержденное Руководителем группы проектов Раковым С.Г.

В данном документе представлено описание технических решений обеспечения информационной безопасности Интегрированной системы управления и безопасности производства полистирола мощностью 250 тыс. тонн в год и общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год на площадке ПАО «НКНХ».

Настоящий документ разработан в составе проектной документации для проектируемого объекта «Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год».

Почтовый (строительный) адрес объекта капитального строительства: Российская Федерация, Республика Татарстан, Нижнекамский муниципальный район, город Нижнекамск, ул. Соболековская, ПАО «Нижнекамскнефтехим», первая промышленная зона.

Технические решения, принятые в проекте, соответствуют требованиям к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, к обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ и других норм, действующих на территории Российской Федерации.

Полный перечень нормативной документации, положениям и требованиям которой соответствуют принятые в проектной документации решения, представлен в перечне нормативной документации настоящего тома.

Объектами защиты является информация, обрабатываемая в АС, ИТ-инфраструктуре, каналах связи, обеспечивающих автоматизацию.

2 ОБЩЕСИСТЕМНЫЕ РЕШЕНИЯ

2.1 Объекты автоматизации

Объекты производства ПС250 и ОЗХ, как объекты управления, представляют собой технологический комплекс на площадке ПАО «Нижнекамскнефтехим».

Для контроля и управления объектами автоматизации производства ПС250 и ОЗХ предусмотрено создание модернизируемой и масштабируемой интегрированной автоматизированной системы управления и безопасности производства ПС250 и ОЗХ (далее ИСУБ ПС250 и ОЗХ), построенной на базе микропроцессорной техники и основанной на цифровой электронной технологии.

ИСУБ ПС250 и ОЗХ обеспечивает автоматизированный диалоговый режим контроля и управления объектами в режиме реального времени без постоянного присутствия персонала в зоне оборудования, необходимые скорость, точность, качество контроля и регулирования параметров, безопасные условия труда для персонала, целостность оборудования и безопасность окружающей среды.

ИСУБ ПС250 и ОЗХ представляет собой распределенную (по функциям и территориально), многофункциональную, информационно-измерительную и управляющую систему, построенную по иерархическому принципу, с использованием стандартных протоколов межуровневого обмена данными, способную к расширению интеграции с другими системами, а также с вышестоящим уровнем управления.

ИСУБ ПС250 и ОЗХ состоит из:

– распределенной системы управления (РСУ), осуществляющей оперативный контроль и управление технологическими процессами;

– системы противоаварийной автоматической защиты (ПАЗ), повышенного, заранее определенного уровня надежности, осуществляющей безаварийное приведение процесса к рабочему (регламентному) режиму или к его остановке, и реализованной на базе программно-технического комплекса повышенной надежности. Основные функции безопасности (остановка оборудования, закрытие/открытие арматуры и т. д.) выполняются независимо от работоспособности РСУ;

– системы контроля загазованности (СКЗ), предназначенной для контроля загазованности воздушной среды в пределах контролируемой зоны, сигнализации и оповещения о нештатной ситуации;

– автоматизированной системы пожарной сигнализации и пожаротушения (АСПСиПТ);

– локальных систем автоматизированного управления (ЛСАУ), интегрированных в РСУ, комплектно-поставляемых с блочным оборудованием (включая системы узлов коммерческого учета);

– системы управления активами предприятия (IAMS), обеспечивающей централизованное (из помещения инженерных станций) контроль и обслуживание интеллектуально полевого оборудования посредством подключений по протоколу HART;

– системы усовершенствованного управления технологическими процессами (СУУТП).

ИСУБ ПС250 и ОЗХ взаимодействует со следующими системами, не входящими в их состав:

– стационарной системой мониторинга динамического оборудования (ССМД);

– системы усовершенствованного управления технологическими процессами (СУУТП);

– аналитической системой мониторинга и сбора данных (AMADAS);

– системой непрерывного контроля выбросов (CEMS);

– компьютерного тренажерного комплекса;

– автоматизированной системой управления электроснабжением (АСУЭ);

– автоматизированной системой оперативного диспетчерского управления (АСОДУ).

2.2 Характеристики автоматизированной системы

Для ИСУБ ПС250 и ОЗХ применимы следующие утверждения, описывающие применяемые технологии:

– автоматизированной беспроводная сеть не используется;

– мобильные устройства используются;

– суперкомпьютеры не используются;

– веб-доступ не используется;

– голосовой ассистент не используется;

– удаленное администрирование используется;

– системы хранения данных используются;

– удаленный внеполосный доступ не используется;

– электронные почтовые службы не используются;

– технологии Big-Data не используются;

– RDP используется;

– одноразовые пароли не используются.

Применение программно-технических средств защиты информации не приводит к отклонениям от установленного режима функционирования автоматизированной системы и не оказывает отрицательного влияния на ход автоматизируемых технологических процессов.

Мероприятия по обеспечению безопасности информации автоматизированной системы максимально учитывают применение встроенных механизмов защиты информации, реализуемых общим программным обеспечением операционных систем серверов, автоматизированных рабочих мест, систем управления базами данных;

специального программного обеспечением (SCADA), встроенного программного обеспечения программно-технических средств защиты информации.

Контроль и управление объектами производства ПС250 и ОЗХ предусматривается централизовано из помещения операторного зала «Операторная производства полипропилена (существующая)» (титул 005).

Основное оборудование средств автоматизации, системные шкафы, коммутационные шкафы, серверные шкафы, системные блоки автоматизированных рабочих мест, шкафы вспомогательных систем и т. п. установлены в Аппаратной (титул 2201) и на Складе ОЗХ (титул 3404).

3 НАБОР МЕР ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Базовый набор мер защиты информации

В соответствии с документом «Акт классификации АСУ», разработанному на основании требований приказа ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», в СОИБ необходимо включить требования по 3-му классу защищенности автоматизированных систем управления.

В соответствии с документом «Акт категорирования АСУ», разработанному на основании требований Федерального закона № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» и постановления Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», в СОИБ не включаются требования по 1-3 категории значимости в связи с присвоением категории «без категории».

Исходя из вышеуказанной информации, базовый набор мер защиты информации включает в себя меры защиты информации, указанные в таблице 3.1.

Таблица 3.1 – Базовый набор мер защиты информации

Условное обозначение и номер меры	Содержание меры защиты информации
1 Идентификация и аутентификация (ИАФ)	
ИАФ.0	Разработка политики идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.5	Идентификация и аутентификация внешних пользователей
ИАФ.7	Защита аутентификационной информации при передаче
2 Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.0	Разработка политики управления доступом
УПД.1	Управление учетными записями пользователей
УПД.2	Реализация политик управления доступа
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему

Условное обозначение и номер меры	Содержание меры защиты информации
УПД.10	Блокирование сеанса доступа пользователя при неактивности
УПД.11	Управление действиями пользователей до идентификации и аутентификации
УПД.13	Реализация защищенного удаленного доступа
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем
3 Ограничение программной среды (ОПС)	
В рамках базового набора мер защиты информации меры ОПС отсутствуют	
4 Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.0	Разработка политики защиты машинных носителей информации
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление физическим доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.7	Контроль подключения машинных носителей информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации
5 Аудит безопасности (АУД)	
АУД.0	Разработка политики аудита безопасности
АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.3	Генерирование временных меток и (или) синхронизация системного времени
АУД.4	Регистрация событий безопасности
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.10	Проведение внутренних аудитов
6 Антивирусная защита (АВЗ)	
АВЗ.0	Разработка политики антивирусной защиты
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Антивирусная защита электронной почты и иных сервисов
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
7 Обнаружение вторжений (СОВ)	
В рамках базового набора мер защиты информации меры СОВ отсутствуют	
8 Обеспечение целостности (ОЦЛ)	
ОЦЛ.0	Разработка политики обеспечения целостности
ОЦЛ.1	Контроль целостности программного обеспечения
9 Обеспечение доступности (ОДТ)	
ОДТ.0	Разработка политики обеспечения доступности
ОДТ.4	Резервное копирование информации
ОДТ.5	Обеспечение возможности восстановления информации
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи

10 Защита технических средств и систем (ЗТС)	
ЗТС.0	Разработка политики защиты технических средств и систем
ЗТС.2	Организация контролируемой зоны
ЗТС.3	Управление физическим доступом
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ЗТС.5	Защита от внешних воздействий
11 Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.5	Организация демилитаризованной зоны
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств
ЗИС.32	Защита беспроводных соединений
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
ЗИС.38	Защита информации при использовании мобильных устройств
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных
12 Реагирование на компьютерные инциденты (ИНЦ)	
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты
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
13 Управление конфигурацией (УКФ)	
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы
УКФ.2	Управление изменениями
14 Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Разработка политики управления обновлениями программного обеспечения
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника
ОПО.2	Контроль целостности обновлений программного обеспечения
ОПО.3	Тестирование обновлений программного обеспечения
ОПО.4	Установка обновлений программного обеспечения
15 Планирование мероприятий по обеспечению безопасности (ПЛН)	
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации

ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации
16 Обеспечение действий в нештатных ситуациях (ДНС)	
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях
ДНС.1	Разработка плана действий в нештатных ситуациях
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения
17 Информирование и обучение персонала (ИПО)	
ИПО.0	Разработка политики информирования и обучения персонала
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

3.2 Адаптация базового набора мер защиты информации

С учетом применимых технологий для ИСУБ, в таблице 3.2 приведен адаптированный базовый набор мер защиты информации.

Таблица 3.2 – Адаптированный базовый набор мер защиты информации

Условное обозначение и номер меры	Содержание меры защиты информации	Статус меры защиты информации
1 Идентификация и аутентификация (ИАФ)		
ИАФ.0	Разработка политики идентификации и аутентификации	Применима
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	Применима
ИАФ.2	Идентификация и аутентификация устройств	Применима
ИАФ.3	Управление идентификаторами	Применима
ИАФ.4	Управление средствами аутентификации	Применима
ИАФ.5	Идентификация и аутентификация внешних пользователей	Не применима
ИАФ.7	Защита аутентификационной информации при передаче	Применима
2 Управление доступом субъектов доступа к объектам доступа (УПД)		
УПД.0	Разработка политики управления доступом	Применима
УПД.1	Управление учетными записями пользователей	Применима
УПД.2	Реализация политик управления доступа	Применима
УПД.4	Разделение полномочий (ролей) пользователей	Применима
УПД.5	Назначение минимально необходимых прав и привилегий	Применима
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	Не применима

Условное обозначение и номер меры	Содержание меры защиты информации	Статус меры защиты информации
УПД.10	Блокирование сеанса доступа пользователя при неактивности	Не применима
УПД.11	Управление действиями пользователей до идентификации и аутентификации	Применима
УПД.13	Реализация защищенного удаленного доступа	Не применима
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	Не применима
3 Ограничение программной среды (ОПС)		
В рамках базового набора мер защиты информации меры ОПС отсутствуют		
4 Защита машинных носителей персональных данных (ЗНИ)		
ЗНИ.0	Разработка политики защиты машинных носителей информации	Применима
ЗНИ.1	Учет машинных носителей информации	Применима
ЗНИ.2	Управление физическим доступом к машинным носителям информации	Применима
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	Применима
ЗНИ.7	Контроль подключения машинных носителей информации	Применима
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	Применима
5 Аудит безопасности (АУД)		
АУД.0	Разработка политики аудита безопасности	Применима
АУД.1	Инвентаризация информационных ресурсов	Применима
АУД.2	Анализ уязвимостей и их устранение	Применима
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	Применима
АУД.4	Регистрация событий безопасности	Применима
АУД.6	Защита информации о событиях безопасности	Применима
АУД.7	Мониторинг безопасности	Применима
АУД.8	Реагирование на сбои при регистрации событий безопасности	Применима
АУД.10	Проведение внутренних аудитов	Применима
6 Антивирусная защита (АВЗ)		
АВЗ.0	Разработка политики антивирусной защиты	Применима
АВЗ.1	Реализация антивирусной защиты	Применима
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	Не применима
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Применима
7 Обнаружение вторжений (СОВ)		
В рамках базового набора мер защиты информации меры СОВ отсутствуют		
8 Обеспечение целостности (ОЦЛ)		
ОЦЛ.0	Разработка политики обеспечения целостности	Применима
ОЦЛ.1	Контроль целостности программного обеспечения	Применима

Условное обозначение и номер меры	Содержание меры защиты информации	Статус меры защиты информации
9 Обеспечение доступности (ОДТ)		
ОДТ.0	Разработка политики обеспечения доступности	Применима
ОДТ.4	Резервное копирование информации	Применима
ОДТ.5	Обеспечение возможности восстановления информации	Применима
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	Применима
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	Применима
10 Защита технических средств и систем (ЗТС)		
ЗТС.0	Разработка политики защиты технических средств и систем	Применима
ЗТС.2	Организация контролируемой зоны	Применима
ЗТС.3	Управление физическим доступом	Применима
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Применима
ЗТС.5	Защита от внешних воздействий	Применима
11 Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)		
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	Применима
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	Применима
ЗИС.2	Защита периметра информационной (автоматизированной) системы	Применима
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	Применима
ЗИС.5	Организация демилитаризованной зоны	Применима
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	Применима
ЗИС.19	Защита информации при ее передаче по каналам связи	Не применима
ЗИС.20	Обеспечение доверенных канала, маршрута	Не применима
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	Применима
ЗИС.32	Защита беспроводных соединений	Не применима
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	Применима
ЗИС.38	Защита информации при использовании мобильных устройств	Не применима
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Не применима
12 Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	Применима
ИНЦ.1	Выявление компьютерных инцидентов	Применима

Условное обозначение и номер меры	Содержание меры защиты информации	Статус меры защиты информации
ИНЦ.2	Информирование о компьютерных инцидентах	Применима
ИНЦ.3	Анализ компьютерных инцидентов	Применима
ИНЦ.4	Устранение последствий компьютерных инцидентов	Применима
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	Применима
13 Управление конфигурацией (УКФ)		
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	Применима
УКФ.2	Управление изменениями	Применима
14 Управление обновлениями программного обеспечения (ОПО)		
ОПО.0	Разработка политики управления обновлениями программного обеспечения	Применима
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	Применима
ОПО.2	Контроль целостности обновлений программного обеспечения	Применима
ОПО.3	Тестирование обновлений программного обеспечения	Применима
ОПО.4	Установка обновлений программного обеспечения	Применима
15 Планирование мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации	Применима
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	Применима
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	Применима
16 Обеспечение действий в нештатных ситуациях (ДНС)		
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	Применима
ДНС.1	Разработка плана действий в нештатных ситуациях	Применима
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	Применима
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	Применима
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	Применима
17 Информирование и обучение персонала (ИПО)		
ИПО.0	Разработка политики информирования и обучения персонала	Применима
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	Применима
ИПО.2	Обучение персонала правилам безопасной работы	Применима

Условное обозначение и номер меры	Содержание меры защиты информации	Статус меры защиты информации
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	Применима

3.3 Уточнение адаптированного базового набора мер

В соответствии с документом «Модель угроз безопасности информации. NKNH21002-ПС-ЭБСМ-ИД1», сформирован перечень актуальных угроз безопасности информации.

Маппинг мер защиты информации на перечень актуальных угроз безопасности информации приведен в таблице 3.3.

Таблица 3.3 – Маппинг мер защиты информации на перечень актуальных угроз безопасности

Идентификатор	Наименование	Меры защиты информации
Угрозы безопасности информации БДУ ФСТЭК России		
6	Угроза внедрения кода или данных	АВЗ.0, АВЗ.1
7	Угроза воздействия на программы с высокими привилегиями	УПД.2
8	Угроза восстановления и/или повторного использования аутентификационной информации	УПД.1, УПД.5
13	Угроза деструктивного использования декларированного функционала BIOS	ИАФ.1
22	Угроза избыточного выделения оперативной памяти	АУД.2
25	Угроза изменения системных и глобальных переменных	УПД.1, АУД.2
26	Угроза искажения XML-схемы	УПД.2, УПД.4, УПД.5
27	Угроза искажения вводимой и выводимой на периферийные устройства информации	УПД.0, УПД.2, ИПО.0, ИПО.1, ИПО.2, ИПО.4
30	Угроза использования информации идентификации/аутентификации, заданной по умолчанию	ИАФ.3, ИАФ.4, УПД.0, УПД.1
31	Угроза использования механизмов авторизации для повышения привилегий	УПД.2, УПД.4, УПД.5, АУД.2
32	Угроза использования поддельных цифровых подписей BIOS	АУД.2, УКФ.3, УКФ.4, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4
33	Угроза использования слабостей кодирования входных данных	ОЦЛ.4
34	Угроза использования слабостей протоколов сетевого/локального обмена данными	ЗИС.0, ЗИС.2, ЗИС.5, ЗИС.6
39	Угроза исчерпания запаса ключей, необходимых для обновления BIOS	АУД.2, ЗИС.2

Идентификатор	Наименование	Меры защиты информации
45	Угроза нарушения изоляции среды исполнения BIOS	УПД.2, ОПС.2, ЗТС.2, ЗТС.3
49	Угроза нарушения целостности данных кеша	УПД.2, АУД.2
51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	ОДТ.4, ОДТ.5, ОДТ.6
63	Угроза некорректного использования функционала программного и аппаратного обеспечения	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7
67	Угроза неправомерного ознакомления с защищаемой информацией	УПД.2, УПД.4, УПД.5, ЗТС.0, ЗТС.2, ЗТС.3, ЗТС.4
68	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	УПД.2, АУД.4, АУД.7, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5
74	Угроза несанкционированного доступа к аутентификационной информации	ИАФ.4, ИАФ.7
86	Угроза несанкционированного изменения аутентификационной информации	ИАФ.0, ИАФ.3, ИАФ.4, УПД.0, УПД.1, УПД.2, УПД.4, УПД.5, АУД.2, ЗИС.1
87	Угроза несанкционированного использования привилегированных функций BIOS	УПД.2, АУД.2, ЗТС.2, ЗТС.3, ОПО.3
88	Угроза несанкционированного копирования защищаемой информации	УПД.2, УПД.4, УПД.5, ЗНИ.2, ЗНИ.5, ЗНИ.8, ЗТС.2, ЗТС.3
89	Угроза несанкционированного редактирования реестра	УПД.1, УПД.2, УПД.4, УПД.5, АУД.2
90	Угроза несанкционированного создания учётной записи пользователя	ИАФ.0, ИАФ.3, ИАФ.4, УПД.0, УПД.1, УПД.2, АУД.2
91	Угроза несанкционированного удаления защищаемой информации	УПД.5, ЗНИ.2, ЗНИ.5, ЗНИ.8, АУД.0, АУД.4, АУД.7, ОДТ.4, ОДТ.5, ЗТС.2, ЗТС.3, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5
94	Угроза несанкционированного управления синхронизацией и состоянием	УПД.2
95	Угроза несанкционированного управления указателями	УПД.2, УПД.4, УПД.5, АУД.2
98	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	ЗНИ.0, ЗНИ.8, АУД.2, ЗИС.2
99	Угроза обнаружения хостов	АУД.0, АУД.2, ЗИС.2
100	Угроза обхода некорректно настроенных механизмов аутентификации	ИАФ.4, УПД.2, УПД.4,
102	Угроза опосредованного управления группой программ через совместно используемые данные	УПД.2, УПД.4, УПД.5, АУД.2
103	Угроза определения типов объектов защиты	ЗИС.2, ЗИС.5, ЗИС.8
104	Угроза определения топологии вычислительной сети	ЗИС.2, ЗИС.5, ЗИС.8
107	Угроза отключения контрольных датчиков	АУД.2

Идентификатор	Наименование	Меры защиты информации
111	Угроза передачи данных по скрытым каналам	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7, ЗИС.2, ЗИС.6, ЗИС.31, ЗИС.35
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	УПД.2, ЗТС.2, ЗТС.3, ЗИС.1, ЗИС.2
114	Угроза переполнения целочисленных переменных	УПД.2, АУД.2, ОЦЛ.4
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	УПД.2, ЗТС.2, ЗТС.3
116	Угроза перехвата данных, передаваемых по вычислительной сети	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7, ЗИС.2, ЗИС.6, ЗИС.31, ЗИС.35
117	Угроза перехвата привилегированного потока	УПД.1, УПД.2, УПД.4, УПД.5, АУД.2, ОПО.3
118	Угроза перехвата привилегированного процесса	УПД.1, УПД.2, УПД.4, УПД.5, АУД.2, ОПО.3
121	Угроза повреждения системного реестра	УПД.1, УПД.2, УПД.4, УПД.5, АУД.2, ОДТ.4, ОДТ.5
122	Угроза повышения привилегий	УПД.1, УПД.2, УПД.4, УПД.5, АУД.0, АУД.2, АУД.4, АУД.7, ОПО.3
124	Угроза подделки записей журнала регистрации событий	УПД.2, УПД.4, УПД.5, АУД.6, АУД.8
132	Угроза получения предварительной информации об объекте защиты	УПД.1, УПД.2, АУД.2, ЗИС.5,
140	Угроза приведения системы в состояние «отказ в обслуживании»	ЗИС.2
143	Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7, ЗИС.2
145	Угроза пропуска проверки целостности программного обеспечения	УПД.5, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4
150	Угроза сбоя процесса обновления BIOS	ОДТ.4, ОДТ.5, ОДТ.6, ОПО.2, ОПО.3
152	Угроза удаления аутентификационной информации	ИАФ.4, АУД.2, ОДТ.4, ОДТ.5
153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов	ЗИС.2, ЗИС.3, ЗИС.5
154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	УПД.2, УПД.4, АУД.2, ОПО.0, ОПО.1, ОПО.2, ОПО.3, ОПО.4
155	Угроза утраты вычислительных ресурсов	ЗИС.2, ЗИС.3, ЗИС.5
156	Угроза утраты носителей информации	ЗНИ.0, ЗНИ.1, ЗНИ.8
158	Угроза форматирования носителей информации	ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5

Идентификатор	Наименование	Меры защиты информации
162	Угроза эксплуатации цифровой подписи программного кода	АУД.2, УКФ.3
163	Угроза перехвата исключения/сигнала из привилегированного блока функций	УПД.2, УПД.4, УПД.5, ОПС.2,
165	Угроза включения в проект не достоверно испытанных компонентов	ОПС,1, АУД.2
169	Угроза наличия механизмов разработчика	ОПС,1, АУД.2
170	Угроза неправомерного шифрования информации	УПД.2, УПД.4, УПД.5
176	Угроза нарушения технологического / производственного процесса из-за временны́х задержек, вносимых средством защиты	АУД.2
177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	АУД.2
178	Угроза несанкционированного использования системных и сетевых утилит	АУД.2
179	Угроза несанкционированной модификации защищаемой информации	АУД.2, УКФ.0, УКФ.2, УКФ.3
180	Угроза отказа подсистемы обеспечения температурного режима	ОДТ.2
183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7, ЗИС.2
185	Угроза несанкционированного изменения параметров настройки средств защиты информации	УПД.2
187	Угроза несанкционированного воздействия на средство защиты информации	УПД.2
189	Угроза маскирования действий вредоносного кода	ЗИС.2
191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	АВЗ.0, АВЗ.1, УКФ.3
192	Угроза использования уязвимых версий программного обеспечения	АУД.0, АУД.2, УФК.3, ОПО.3
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	АВЗ.3, ЗИС.2
195	Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы	АВЗ.0, АВЗ.1, ЗИС.2
198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	УПД.0, УПД.1, УПД.2, АУД.2, УКФ.3
203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	ЗТС.3
204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	ИАФ.1, АВЗ.1
205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	ОПО.1

Идентификатор	Наименование	Меры защиты информации
208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	УПД.2, АУД.4, АУД.7, ЗИС.35, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5
210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	ОПО.2, ОПО.3
211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем	АУД.2, ОЦЛ.4, УКФ.3
212	Угроза перехвата управления информационной системой	ИАФ.0, ИАФ.1, ИАФ.3, ИАФ.4
214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы (в том числе средствами защиты информации) на события безопасности информации	АУД.2, АУД.4, АУД.7, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3, ИНЦ.4, ИНЦ.5
217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	ОПО.0, ОПО.1, ОПО.2
Дополнительные угрозы безопасности информации		
1.1	Угроза получения информации об объектах воздействия из официальных источников	ДМУ.1
1.15	Угроза получения информации об объектах воздействия или аутентификационной информации через поиск и покупку баз данных на нелегальных площадках	ИАФ.4, УПД.1
1.16	Угроза получения доступа к информации в базах данных результатов проведенных инвентаризаций, реестрах установленного оборудования и ПО, данным проведенных аудитов безопасности, в том числе через получение доступа к таким данным через компрометацию подрядчиков и партнеров	УПД.2, УПД.4, УПД.5, ДМУ.4
2.3	Угроза получения доступа путем эксплуатации уязвимостей сетевого оборудования и/или средств защиты вычислительных сетей	АУД.0, АУД.2, АУД.4
2.4	Угроза получения доступа путем использования ошибок конфигурации сетевого оборудования и/или средств защиты	АУД.0, АУД.2
2.7	Угроза получения доступа через эксплуатацию (заражение вредоносным программным обеспечением) внешних носителей информации	ЗНИ.2, ЗНИ.7, АВЗ.0, АВЗ.1, АВЗ.4
2.8	Угроза получения доступа методом социальной инженерии	ИПО.0, ИПО.1, ИПО.2, ИПО.4

Идентификатор	Наименование	Меры защиты информации
2.11	Угроза получения доступа методом применения аутентификационной информации, используемой в смежных системах и ранее полученной	ИАФ.4
3.6	Угроза внедрения и исполнения вредоносного кода от имени пользователя	УПД.2, УПД.4, УПД.5, АВЗ.1, АВЗ.4
3.7	Угроза внедрения и исполнения вредоносного кода за счет подмены файлов и библиотек в системе	ИАФ.1, УПД.2, УПД.4, УПД.5, АВЗ.1, АВЗ.4
3.8	Угроза внедрения и исполнения вредоносного кода за счет подмены обновлений программного обеспечения, хранящихся в системе	АВЗ.0, АВЗ.1, АВЗ.4, ОПО.0, ОПО.1, ОПО.2, ОПО.3
3.10	Угроза внедрения и исполнения вредоносного кода за счет подмены дистрибутивов программного обеспечения на носителях информации или общих сетевых ресурсах	УПД.2, УПД.4, УПД.5, ЗНИ.2, АВЗ.0, АВЗ.1, АВЗ.4
3.12	Угроза внедрения и исполнения вредоносного кода за счет компрометации средств разработчика	ОПО.0, ОПО.1, ОПО.2, ОПО.3
3.13	Угроза внедрения и исполнения вредоносного кода за счет компрометации средств сборки, конфигурирования и разворачивания программного кода, а также средств создания узкоспециализированного кода	АВЗ.1
4.2	Угроза обеспечения повторного доступа в систему, используя штатные средства удаленного доступа и управления операционной системы	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7, ЗИС.2, ЗИС.3, ЗИС.6, ЗИС.35
4.3	Угроза обеспечения повторного доступа в систему по средствам скрытой установки программ, обеспечивающий удаленный доступ	УПД.2, УПД.4, УПД.5, АУД.2, АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
4.4	Угроза обеспечения повторного доступа в систему за счет подключения к корпоративной сети внешних устройств и маскирования их под легитимные	АУД.1, АУД.2, АУД.10, ЗИС,35, УКФ.4
4.7	Угроза обеспечения повторного доступа в систему за счет копирование вредоносного кода в области, редко подвергаемых проверке	АВЗ.1, АВЗ.4
5.1	Угроза управления вредоносным обеспечением, используя стандартные протоколы	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
5.2	Угроза управления вредоносным обеспечением, используя штатные средства удаленного доступа	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
5.3	Угроза управления вредоносным обеспечением, используя взаимодействие с внешними серверами через разрешенные известные порты	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
5.4	Угроза управления вредоносным обеспечением, используя взаимодействие с внешними серверами через разрешенные нестандартные порты	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35

Идентификатор	Наименование	Меры защиты информации
5.5	Угроза управления вредоносным обеспечением, используя съемные носители информации	ЗНИ.5, ЗНИ.7, АВЗ.1, АВЗ.4
5.6	Угроза управления вредоносным обеспечением, используя взаимодействие с внешними серверами по средствам проксирования трафика	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
5.7	Угроза управления вредоносным обеспечением, используя взаимодействие с внешними серверами по средствам туннелирование трафика управления через VPN	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
5.8	Угроза управления вредоносным обеспечением, используя взаимодействие с внешними серверами по средствам туннелирование трафика управления в поля заполнения и данных служебных протоколов	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
5.10	Угроза управления вредоносным обеспечением, используя взаимодействие с внешними серверами по средствам обфускации, шифрования, стеганогравирования трафика	АУД.4, АУД.7, АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.35
5.11	Угроза управления вредоносным обеспечением, используя взаимодействие по разрешенным протоколам	АВЗ.1, АВЗ.4, ЗИС.2, ЗИС.6, ЗИС.35
6.4	Угроза запуска операций или скриптов от имени учетной записи, имеющей повышенные привилегии, за счет эксплуатации уязвимостей имперсонации	ИАФ.0, ИАФ.1, ИАФ.3, УПД.0, УПД.1, УПД.2, УПД.5
6.5	Угроза повышения привилегий за счет эксплуатации параметров, определяющих права доступа (идентификатор сессии, токен доступа)	ИАФ.4, УПД.2
6.7	Угроза повышения привилегий за счет использования уязвимостей конфигураций систем, служб и приложений, позволяющих запускать скрипты от имени привилегированной учетной записи	УПД.2, АУД.0, АУД.2
7.1	Угроза сокрытия вредоносных действий путем использования штатных программных инструментов и сокрытие действий под легитимные	ИАФ.1, УПД.1, УПД.2, УПД.4, УПД.5
7.2	Угроза сокрытия вредоносных действий путем редактирования (затирания) журналов регистрации событий	УПД.4, УПД.5, АУД.6
7.3	Угроза сокрытия вредоносных действий путем удаления или перезаписывание файлов	УПД.5, АУД.4, АУД.7, ИНЦ.0, ИНЦ.1, ИНЦ.2, ИНЦ.3
7.4	Угроза сокрытия вредоносных действий путем воздействия на средства защиты информации: прекращение работы	УПД.2, УПД.4, УПД.5, АУД.3, АУД.6, АУД.8, ИНЦ.6
7.5	Угроза сокрытия вредоносных действий путем воздействия на средства мониторинга промышленных систем: прекращение работы	УПД.0, УПД.1, УПД.2, АУД.2

Идентификатор	Наименование	Меры защиты информации
7.6	Угроза сокрытия вредоносных действий путем воздействия на средства защиты информации: подмена обрабатываемых данных	УПД.2, УПД.4, АУД.0, АУД.2
7.7	Угроза сокрытия вредоносных действий путем воздействия на средства мониторинга промышленных систем: подмена обрабатываемых данных	УПД.0, УПД.1, УПД.2, АУД.2
7.8	Угроза сокрытия вредоносных действий путем воздействия на средства защиты информации: отказ в обслуживании каналов связи	ЗТС.2, ЗТС.3, ЗИС.2
7.10	Угроза сокрытия вредоносных действий путем внедрения вредоносного кода в доверенные процессы	АВЗ.1, АВЗ.4
7.11	Угроза сокрытия вредоносных действий путем изменения вредоносного кода для усложнения отслеживания его присутствия и воздействия	АВЗ.1, АВЗ.4
7.12	Угроза сокрытия вредоносных действий путем изменения параметров запускаемых процессов и сокрытие их под легитимные	УПД.0, УПД.1, УПД.2, АВЗ.1, АВЗ.4
7.13	Угроза сокрытия вредоносных действий путем создания скрытых файлов и учетных записей	УПД.0, УПД.1, УПД.2, АУД.2, АВЗ.1, АВЗ.4
7.14	Угроза сокрытия вредоносных действий путем установки ложного корневого сертификата, подтверждающего легитимность вредоносных программ	УПД.0, УПД.1, УПД.2, АУД.2, АВЗ.1, АВЗ.4
7.16	Угроза сокрытия вредоносных действий путем установки временного ограничения для распространения или активации вредоносного кода	АУД.2, АВЗ.1, АВЗ.4
7.17	Угроза сокрытия вредоносных действий путем сокрытия вредоносного кода и его действий в системе методами обфускации, шифрования или стеганографии	АВЗ.1, АВЗ.4
7.18	Угроза сокрытия вредоносного кода, находящегося в системе, путем использования средств виртуализации	ИАФ.1, АВЗ.1, АВЗ.4
7.19	Угроза сокрытия вредоносных действий путем управления вредоносным обеспечением, используя взаимодействие с внешними серверами по средствам туннелирование трафика управления через VPN	АВЗ.1, АВЗ.4, ЗИС.2
7.20	Угроза сокрытия вредоносных действий путем управления вредоносным обеспечением, используя взаимодействие с внешними серверами по средствам туннелирование трафика управления в поля заполнения и данных служебных протоколов	АВЗ.1, АВЗ.4, ЗИС.2

Идентификатор	Наименование	Меры защиты информации
7.21	Угроза сокрытия вредоносных действий путем изменения конфигурации телекоммуникационного оборудования с целью маскирование вредоносных действий под легитимные	УПД.2, УПД.4, УПД.5, АУД.2, АУД.4, АУД.7, АВЗ.1, АВЗ.4
8.2	Угроза распространения доступа путем эксплуатации средств удаленного управления	ЗИС.2, ЗИС.3, ЗИС.5
8.3	Угроза распространения доступа путем использования механизмов дистанционной установки программного обеспечения и конфигурирования	УПД.4, УПД.5, УКФ.0, УКФ.2, УКФ.3, УКФ.4
8.4	Угроза распространения доступа путем распространения вредоносного кода	АВЗ.0, АВЗ.1, АВЗ.4
8.5	Угроза распространения доступа путем изменения конфигурации телекоммуникационного оборудования	УПД.1, УПД.2, УПД.4, УПД.5, АУД.2, АУД.4, АУД.7, ЗИС.0, ЗИС.1, УКФ.0, УКФ.2, УКФ.4
8.7	Угроза получения доступа путем размещения вредоносного кода на общих сетевых ресурсах с целью привлечения к запуску	УПД.2, УПД.4, УПД.5, АВЗ.0, АВЗ.1, АВЗ.4
8.8	Угроза получения доступа путем распространения вредоносного воздействия через интеграцию со смежными системами	АВЗ.0, АВЗ.1, АВЗ.4
9.1	Угроза утечки информации, используя стандартные протоколы управления	АУД.4, АУД.7, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6
9.2	Угроза утечки информации, используя штатные средства удаленного доступа	УПД.2, УПД.4, УПД.5, АУД.4, АУД.7, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6
9.3	Угроза утечки информации по средствам вывода на внешний сервер, используя известные порты	АУД.4, АУД.7, ЗИС.2, ЗИС.3, ЗИС.5, ЗИС.6, ЗИС.35
9.4	Угроза утечки информации по средствам вывода на внешний сервер, используя разрешенные нестандартные порты	АУД.4, АУД.7, АУД.10, ЗИС.2, ЗИС.5, ЗИС.6, ЗИС.35
9.5	Угроза утечки информации, используя разрешенные протоколы управления и передачи данных	АУД.4, АУД.7, ЗИС.2, ЗИС.5, ЗИС.6, ЗИС.35
9.6	Угроза утечки информации, используя собственные протоколы управления и передачи данных	АУД.4, АУД.7, ЗИС.2, ЗИС.5, ЗИС.6, ЗИС.35
9.7	Угроза утечки информации, используя проксирование трафика при передаче	АУД.4, АУД.7, ЗИС.2
9.8	Угроза утечки информации, используя туннелирование трафика при передаче через VPN	ЗИС.2, ЗИС.31
9.9	Угроза утечки информации, используя туннелирование трафика управления в поля заполнения и данных служебных протоколов	ЗИС.2
9.10	Угроза утечки информации, используя съемные носители	ЗНИ.0, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.7, ЗТС.3

Идентификатор	Наименование	Меры защиты информации
10.3	Угроза несанкционированного воздействия на прикладное программное обеспечение с целью нанесения ущерба	УПД.1, УПД.2, УПД.4, УПД.5, АУД.4, АУД.7
10.5	Угроза несанкционированного воздействия на системное программное обеспечение с целью нанесения ущерба	УПД.1, УПД.2, УПД.4, УПД.5, АУД.4, АУД.7

С учетом маппинга мер защиты информации на перечень актуальных угроз безопасности информации, сформирован уточненный адаптированный базовый набор мер, приведенный в таблице 3.4.

Таблица 3.4 – Уточненный адаптированный базовый набор мер защиты информации

Условное обозначение и номер меры	Содержание меры защиты информации
1 Идентификация и аутентификация (ИАФ)	
ИАФ.0	Разработка политики идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.7	Защита аутентификационной информации при передаче
2 Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.0	Разработка политики управления доступом
УПД.1	Управление учетными записями пользователей
УПД.2	Реализация политик управления доступа
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий
УПД.11	Управление действиями пользователей до идентификации и аутентификации
3 Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения
4 Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.0	Разработка политики защиты машинных носителей информации
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление физическим доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.7	Контроль подключения машинных носителей информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации
5 Аудит безопасности (АУД)	
АУД.0	Разработка политики аудита безопасности
АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.3	Генерирование временных меток и (или) синхронизация системного времени

Условное обозначение и номер меры	Содержание меры защиты информации
АУД.4	Регистрация событий безопасности
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.10	Проведение внутренних аудитов
6 Антивирусная защита (АВЗ)	
АВЗ.0	Разработка политики антивирусной защиты
АВЗ.1	Реализация антивирусной защиты
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
8 Обеспечение целостности (ОЦЛ)	
ОЦЛ.0	Разработка политики обеспечения целостности
ОЦЛ.1	Контроль целостности программного обеспечения
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему
9 Обеспечение доступности (ОДТ)	
ОДТ.0	Разработка политики обеспечения доступности
ОДТ.2	Резервирование средств и систем
ОДТ.4	Резервное копирование информации
ОДТ.5	Обеспечение возможности восстановления информации
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи
10 Защита технических средств и систем (ЗТС)	
ЗТС.0	Разработка политики защиты технических средств и систем
ЗТС.2	Организация контролируемой зоны
ЗТС.3	Управление физическим доступом
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ЗТС.5	Защита от внешних воздействий
11 Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.5	Организация демилитаризованной зоны
ЗИС.6	Управление сетевыми потоками
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств
ЗИС.31	Защита от скрытых каналов передачи информации
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)

Условное обозначение и номер меры	Содержание меры защиты информации
ЗИС.35	Управление сетевыми соединениями
12 Реагирование на компьютерные инциденты (ИНЦ)	
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты
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
13 Управление конфигурацией (УКФ)	
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы
УКФ.2	Управление изменениями
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения
УКФ.4	Контроль действий по внесению изменений
14 Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Разработка политики управления обновлениями программного обеспечения
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника
ОПО.2	Контроль целостности обновлений программного обеспечения
ОПО.3	Тестирование обновлений программного обеспечения
ОПО.4	Установка обновлений программного обеспечения
15 Планирование мероприятий по обеспечению безопасности (ПЛН)	
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации
16 Обеспечение действий в нештатных ситуациях (ДНС)	
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях
ДНС.1	Разработка плана действий в нештатных ситуациях
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения
17 Информирование и обучение персонала (ИПО)	
ИПО.0	Разработка политики информирования и обучения персонала
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы
ИПО.2	Обучение персонала правилам безопасной работы

Условное обозначение и номер меры	Содержание меры защиты информации
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы
Дополнительные меры по результатам моделирования угроз безопасности информации	
ДМУ.1	Запрет публикации информации о Системе в публичных источника (официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций)
ДМУ.2	Смена идентификационной информации, используемой подрядчиками перед вводом в эксплуатацию компонентов Системы

3.4 Дополнение уточненного адаптированного базового набора мер защиты информации

Заказчик является субъектом КИИ.

ИСУБ является объектом критической информационной инфраструктуры с категорией значимости «без категории».

Исходя из вышеописанного, необходимо учесть следующие дополнительные меры защиты информации в составе СОИБ, указанные в таблице 3.5.

Таблица 3.5 – Дополнительные меры защиты информации

Условное обозначение и номер меры	Содержание меры защиты информации
Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»	
ДОП.1	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА путем направления в НКЦКИ в соответствии с определенными НКЦКИ форматами с использованием технической инфраструктуры НКЦКИ (в случае отсутствия подключения к технической инфраструктуре НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru») следующей информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры: – дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел компьютерный инцидент; – наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой; – связь с другими компьютерными инцидентами (при наличии); – состав технических параметров компьютерного инцидента; – последствия компьютерного инцидента.

Условное обозначение и номер меры	Содержание меры защиты информации
ДОП.2	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, не позднее 24 часов с момента обнаружения компьютерного инцидента
ДОП.3	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА путем ее направления в НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru» иной информации в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, предоставляемая субъектами критической информационной инфраструктуры и иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными, в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты
Приказ ФСТЭК России от 21 декабря 2017 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»	
ДОП.4	Обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты (при необходимости)
Приказ ФСБ России от 06 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»	
ДОП.5	Применение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в соответствии с требованиями приказа ФСБ России от 06 мая 2019 г. № 196

Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»	
ДОП.6	Применение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, с соблюдением порядка, технических условий установки и эксплуатации данных средств
Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»	
ДОП.7	Запрет использования средств защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними (начало действия требования с 01.01.2025).

3.5 Итоговый набор мер защиты информации

По результатам адаптации, уточнения, дополнения базового набора мер защиты информации, приведенных в пунктах 3.2, 3.3, 3.4, сформирован итоговый набор мер защиты информации, указанный в таблице 3.6.

Таблица 3.6 – Итоговый набор мер защиты информации

Условное обозначение и номер меры	Содержание меры защиты информации
1 Идентификация и аутентификация (ИАФ)	
ИАФ.0	Разработка политики идентификации и аутентификации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИАФ.7	Защита аутентификационной информации при передаче
2 Управление доступом субъектов доступа к объектам доступа (УПД)	
УПД.0	Разработка политики управления доступом
УПД.1	Управление учетными записями пользователей
УПД.2	Реализация политик управления доступа
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий
УПД.11	Управление действиями пользователей до идентификации и аутентификации
3 Ограничение программной среды (ОПС)	
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения
4 Защита машинных носителей персональных данных (ЗНИ)	
ЗНИ.0	Разработка политики защиты машинных носителей информации

Условное обозначение и номер меры	Содержание меры защиты информации
ЗНИ.1	Учет машинных носителей информации
ЗНИ.2	Управление физическим доступом к машинным носителям информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
ЗНИ.7	Контроль подключения машинных носителей информации
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации
5 Аудит безопасности (АУД)	
АУД.0	Разработка политики аудита безопасности
АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.3	Генерирование временных меток и (или) синхронизация системного времени
АУД.4	Регистрация событий безопасности
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.10	Проведение внутренних аудитов
6 Антивирусная защита (АВЗ)	
АВЗ.0	Разработка политики антивирусной защиты
АВЗ.1	Реализация антивирусной защиты
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
8 Обеспечение целостности (ОЦЛ)	
ОЦЛ.0	Разработка политики обеспечения целостности
ОЦЛ.1	Контроль целостности программного обеспечения
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему
9 Обеспечение доступности (ОДТ)	
ОДТ.0	Разработка политики обеспечения доступности
ОДТ.2	Резервирование средств и систем
ОДТ.4	Резервное копирование информации
ОДТ.5	Обеспечение возможности восстановления информации
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи
10 Защита технических средств и систем (ЗТС)	
ЗТС.0	Разработка политики защиты технических средств и систем
ЗТС.2	Организация контролируемой зоны
ЗТС.3	Управление физическим доступом
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр
ЗТС.5	Защита от внешних воздействий

11 Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)	
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями
ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.5	Организация демилитаризованной зоны
ЗИС.6	Управление сетевыми потоками
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств
ЗИС.31	Защита от скрытых каналов передачи информации
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)
ЗИС.35	Управление сетевыми соединениями
12 Реагирование на компьютерные инциденты (ИНЦ)	
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты
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
13 Управление конфигурацией (УКФ)	
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы
УКФ.2	Управление изменениями
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения
УКФ.4	Контроль действий по внесению изменений
14 Управление обновлениями программного обеспечения (ОПО)	
ОПО.0	Разработка политики управления обновлениями программного обеспечения
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника
ОПО.2	Контроль целостности обновлений программного обеспечения
ОПО.3	Тестирование обновлений программного обеспечения
ОПО.4	Установка обновлений программного обеспечения
15 Планирование мероприятий по обеспечению безопасности (ПЛН)	
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации
16 Обеспечение действий в нештатных ситуациях (ДНС)	
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях
ДНС.1	Разработка плана действий в нештатных ситуациях
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях

ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения
17 Информирование и обучение персонала (ИПО)	
ИПО.0	Разработка политики информирования и обучения персонала
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
Дополнительные меры по результатам моделирования угроз безопасности информации	
ДМУ.1	Запрет публикации информации о Системе в публичных источника (официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций)
ДМУ.2	Смена идентификационной информации, используемой подрядчиками перед вводом в эксплуатацию компонентов Системы
Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»	
ДОП.1	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА путем направления в НКЦКИ в соответствии с определенными НКЦКИ форматами с использованием технической инфраструктуры НКЦКИ (в случае отсутствия подключения к технической инфраструктуре НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru») следующей информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры: – дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел компьютерный инцидент; – наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой; – связь с другими компьютерными инцидентами (при наличии); – состав технических параметров компьютерного инцидента; – последствия компьютерного инцидента
ДОП.2	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, не позднее 24 часов с момента обнаружения компьютерного инцидента

ДОП.3	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА путем ее направления в НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru» иной информации в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, предоставляемая субъектами критической информационной инфраструктуры и иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными, в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты
Приказ ФСТЭК России от 21 декабря 2017 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»	
ДОП.4	Обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты (при необходимости)
Приказ ФСБ России от 06 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»	
ДОП.5	Применение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в соответствии с требованиями приказа ФСБ России от 06 мая 2019 г. № 196
Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»	
ДОП.6	Применение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, с соблюдением порядка, технических условий установки и эксплуатации данных средств

Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»	
ДОП.7	Запрет использования средств защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними (начало действия требования с 01.01.2025).

4 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

4.1 Реализация требований по обеспечению информационной безопасности системы

Описание порядка реализации итогового набора мера защиты информации, представлено в таблице 3.1.

Таблица 3.1 – Описание порядка реализации мер защиты информации

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
1 Идентификация и аутентификация (ИАФ)		
ИАФ.0	Разработка политики идентификации и аутентификации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	Функционал Комплекса средств защиты от несанкционированного доступа, механизм Контроля входа пользователей в систему, встроенные механизмы безопасности ОС и ПО; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию, NAC
ИАФ.2	Идентификация и аутентификация устройств	Функционал Комплекса средств защиты от несанкционированного доступа, Идентификация компьютеров, съемных машинных носителей информации
ИАФ.3	Управление идентификаторами	Функционал Комплекса средств защиты от несанкционированного доступа, Управление учетными записями; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию, NAC
ИАФ.4	Управление средствами аутентификации	Функционал Комплекса средств защиты от несанкционированного доступа встроенные механизмы безопасности ОС и ПО; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.7	Защита аутентификационной информации при передаче	Функционал Комплекса средств защиты от несанкционированного доступа, Защита от перехвата пароля при сетевых обращениях, встроенные механизмы безопасности ОС

2 Управление доступом (УПД)		
УПД.0	Разработка политики управления доступом	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
УПД.1	Управление учетными записями пользователей	Функционал Комплекса средств защиты от несанкционированного доступа, Управление учетными записями в программе управления пользователями, встроенные механизмы ОС и ПО; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию, NAC
УПД.2	Реализация политик управления доступа	Функционал Комплекса средств защиты от несанкционированного доступа, Дискреционный метод разграничения доступа, встроенные механизмы ОС и ПО; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию, NAC
УПД.4	Разделение полномочий (ролей) пользователей	Функционал Комплекса средств защиты от несанкционированного доступа, Права доступа / группы администраторов, встроенные механизмы ОС и ПО; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию, NAC
УПД.5	Назначение минимально необходимых прав и привилегий	Функционал Комплекса средств защиты от несанкционированного доступа, Права доступа / группы администраторов, встроенные механизмы ОС и ПО; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию, NAC
УПД.11	Управление действиями пользователей до идентификации и аутентификации	Функционал Комплекса средств защиты от несанкционированного доступа механизм Контроля входа пользователей в систему, встроенные механизмы безопасности ОС и ПО
3 Ограничение программной среды (ОПС)		
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
4 Защита машинных носителей персональных данных (ЗНИ)		
ЗНИ.0	Разработка политики защиты машинных носителей информации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗНИ.1	Учет машинных носителей информации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

ЗНИ.2	Управление физическим доступом к машинным носителям информации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	Функционал Комплекса средств защиты от несанкционированного доступа, Разграничение доступа к устройствам, встроенные механизмы ОС
ЗНИ.7	Контроль подключения съемных машинных носителей информации	Функционал Комплекса средств защиты от несанкционированного доступа, Разграничение доступа к устройствам, встроенные механизмы ОС
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	Функционал Комплекса средств защиты от несанкционированного доступа, Затирание удаляемой информации
5 Аудит безопасности (АУД)		
АУД.0	Разработка политики аудита безопасности	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
АУД.1	Инвентаризация информационных ресурсов	Функционал Комплекса анализа защищенности инфраструктуры
АУД.2	Анализ уязвимостей и их устранение	Функционал Комплекса анализа защищенности инфраструктуры
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	NTP-сервер СОИБ
АУД.4	Регистрация событий безопасности	Функционал Комплекса сбора, анализа и корреляции событий безопасности
АУД.6	Защита информации о событиях безопасности	Функционал Комплекса сбора, анализа и корреляции событий безопасности
АУД.7	Мониторинг безопасности	Функционал Комплекса сбора, анализа и корреляции событий безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности	Функционал Комплекса сбора, анализа и корреляции событий безопасности
АУД.10	Проведение внутренних аудитов	Функционал Комплекса анализа защищенности инфраструктуры
6 Антивирусная защита (АВЗ)		
АВЗ.0	Регламентация политики антивирусной защиты	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
АВЗ.1	Реализация антивирусной защиты	Функционал Комплекса антивирусной защиты
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов	Функционал Комплекса антивирусной защиты
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Функционал Комплекса антивирусной защиты

8 Обеспечение целостности (ОЦЛ)		
ОЦЛ.0	Регламентация политики обеспечения целостности	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ОЦЛ.1	Контроль целостности программного обеспечения	Функционал Комплекса средств защиты от несанкционированного доступа, Контроль целостности
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему	Посредством встроенных механизмов защиты ПО ИСУБ
9 Обеспечение доступности (ОДТ)		
ОДТ.0	Регламентация политики обеспечения доступности	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ОДТ.2	Резервирование средств и систем	Реализация на уровне архитектуры ИСУБ Резервирование критичных компонентов СОИБ: межсетевых экранов, АСО, серверного оборудования
ОДТ.4	Резервное копирование информации	Функционал Комплекса резервного копирования информационных ресурсов
ОДТ.5	Обеспечение возможности восстановления информации	Функционал Комплекса резервного копирования информационных ресурсов
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	Функционал Комплекса резервного копирования информационных ресурсов
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
10 Защита технических средств (ЗТС)		
ЗТС.0	Разработка политики защиты технических средств и систем	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗТС.2	Организация контролируемой зоны	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗТС.3	Управление физическим доступом	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗТС.5	Защита от внешних воздействий	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

11 Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)		
ЗИС.0	Регламентация политики защиты информационной (автоматизированной) системы и ее компонентов	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	Функционал Комплекса средств защиты от несанкционированного доступа
ЗИС.2	Защита периметра информационной (автоматизированной) системы	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	Функционал Комплекса обеспечения сетевой безопасности; Функционал Комплекса средств защиты от несанкционированного доступа
ЗИС.5	Организация демилитаризованной зоны	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.6	Управление сетевыми потоками	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.31	Защита от скрытых каналов передачи информации	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	Функционал Комплекса обеспечения сетевой безопасности,
ЗИС.35	Управление сетевыми соединениями	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Функционал Комплекса защиты среды виртуализации (выполнение требований к защите среды виртуализации компонентов СОИБ)
12 Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Регламентация политики реагирования на компьютерные инциденты	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИНЦ.1	Выявление компьютерных инцидентов	Функционал Комплекса сбора, анализа и корреляции событий безопасности
ИНЦ.2	Информирование о компьютерных инцидентах	Функционал Комплекса сбора, анализа и корреляции событий безопасности
ИНЦ.3	Анализ компьютерных инцидентов	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИНЦ.4	Устранение последствий компьютерных инцидентов	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах	Функционал Комплекса сбора, анализа и корреляции событий безопасности
13 Управление конфигурацией (УКФ)		
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
УКФ.2	Управление изменениями	Функционал Комплекса контроля безопасности конфигураций, NA и ICC
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения посредством централизованных средств управления обновлениями ОС и средств защиты информации
УКФ.4	Контроль действий по внесению изменений	Функционал Комплекса контроля безопасности конфигураций, NA и ICC Функционал Комплекса сбора, анализа и корреляции событий безопасности
14 Управление обновлениями программного обеспечения (ОПО)		
ОПО.0	Регламентация политики управления обновлениями программного обеспечения	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	Функционал Комплекса управления обновлениями программного обеспечения, передача файлов обновлений из МСПД на Файловый сервер СОИБ
ОПО.2	Контроль целостности обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения посредством централизованных средств управления обновлениями ОС и средств защиты информации
ОПО.3	Тестирование обновлений программного обеспечения	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ОПО.4	Установка обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения, посредством централизованных средств управления обновлениями ОС и средств защиты информации
15 Планирование мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
16 Обеспечение действий в нештатных ситуациях (ДНС)		
ДНС.0	Разработка политики обеспечения действий в нештатных ситуациях	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ДНС.1	Разработка плана действий в нештатных ситуациях	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	Посредством Комплекса резервного копирования информационных ресурсов, резервное копирование виртуальных машин и конфигураций с использованием СРК
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
17 Информирование и обучение персонала (ИПО)		
ИПО.0	Регламентация политики информирования и обучения персонала	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИПО.2	Обучение персонала правилам безопасной работы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
Дополнительные меры по результатам моделирования угроз безопасности информации		
ДМУ.1	Запрет публикации информации о Системе в публичных источника (официальный сайт (сайты) организации, СМИ, социальные сети, фотобанки, сайты поставщиков и вендоров, материалы конференций)	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ДМУ.2	Смена идентификационной информации, используемой подрядчиками перед вводом в эксплуатацию компонентов Системы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»		
ДОП.1	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА путем направления в НКЦКИ в соответствии с определенными НКЦКИ форматами с использованием технической инфраструктуры НКЦКИ (в случае отсутствия подключения к технической инфраструктуре НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru») следующей информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры: – дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел компьютерный инцидент; – наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой; – связь с другими компьютерными инцидентами (при наличии); – состав технических параметров компьютерного инцидента; последствия компьютерного инцидента	Функционал Комплекса сбора, анализа и корреляции событий безопасности, Центральная нода SIEM (МСПД)

ДОП.2	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, не позднее 24 часов с момента обнаружения компьютерного инцидента	Функционал Комплекса сбора, анализа и корреляции событий безопасности Центральная нода SIEM (МСПД)
ДОП.3	Предоставление субъектом критической информационной инфраструктуры в ГосСОПКА путем ее направления в НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «http://cert.gov.ru» иной информации в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, предоставляемая субъектами критической информационной инфраструктуры и иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными, в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты	Функционал Комплекса сбора, анализа и корреляции событий безопасности, Центральная нода SIEM (МСПД)

Приказ ФСТЭК России от 21 декабря 2017 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»		
ДОП.4	Обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты (при необходимости)	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
Приказ ФСБ России от 06 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»		
ДОП.5	Применение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в соответствии с требованиями приказа ФСБ России от 06 мая 2019 г. № 196	Функционал Комплекса сбора, анализа и корреляции событий безопасности
Приказ ФСБ России от 19 июня 2019 г. № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»		
ДОП.6	Применение средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, с соблюдением порядка, технических условий установки и эксплуатации данных средств	Функционал Комплекса сбора, анализа и корреляции событий безопасности

4.2 Решения по построению СОИБ

С учетом описания порядка реализации мер защиты информации, структура СОИБ должна состоять из следующих комплексов:

– комплекс средств защиты от несанкционированного доступа;

– комплекс антивирусной защиты;

– комплекс анализа защищенности инфраструктуры;

– комплекс сбора, анализа и корреляции событий безопасности;

– комплекс резервного копирования информационных ресурсов;

– комплекс обеспечения сетевой безопасности;

– комплекс защиты среды виртуализации;

– комплекс контроля конфигураций;

– комплекс управления обновлениями программного обеспечения;

– комплекс централизованного управления доступом к активному сетевому оборудованию;

– комплекс организационных мероприятий по обеспечению информационной безопасности.

4.2.1 Комплекс средств защиты от несанкционированного доступа

Комплекс средств защиты от несанкционированного доступа включает в себя следующий перечень решений:

– использование наложенных средств защиты от несанкционированного доступа, устанавливаемые на АРМ и серверы ИСУБ ПС250 и ОЗХ;

– настройка встроенных механизмов защиты прикладного ПО;

– настроек встроенных механизмов защиты активного сетевого оборудования.

На АРМ и серверах под управлением ОС Astra Linux, соответствующие меры защиты реализуются встроенными механизмами ОС, в соответствии с эксплуатационная документацией и справочной информацией по функционированию и настройке штатных средств защиты информации Astra Linux, для используемого дистрибутива.

4.2.1.1 Решение наложенных средств защиты от несанкционированного доступа

Решение наложенных средств защиты от несанкционированного доступа строится на базе решения Secret Net Studio, предназначенного для обеспечения безопасности АРМ и серверов ИСУБ.

Решение наложенных средств защиты от несанкционированного доступа обеспечивает:

– контроль входа в ОС (идентификация и аутентификация пользователей);

– разграничение доступа к файловым ресурсам и устройствам;

– контроль целостности файловых объектов и реестра;

– затирание удаляемой информации;

– защиту содержимого локальных жестких дисков при несанкционированной загрузке операционной системы;

– регистрацию событий безопасности;

– централизованное и локальное управление параметрами работы механизмов защиты;

– мониторинг и оперативное управление защищаемыми компьютерами;

– централизованный сбор, хранение и архивирование журналов.

Решение наложенных средств защиты от несанкционированного доступа состоит из следующих программных пакетов, устанавливаемых на АРМ, серверах ИСУБ ПС250 и ОЗХ и выделенном сервере управления комплексом:

– клиент Secret Net Studio или Secret Net LSP;

– сервер безопасности Secret Net Studio;

– центр управления Secret Net Studio.

Клиентская часть решения предназначена для реализации защиты АРМ или сервера, на которых установлен данный компонент. Защита реализуется путем применения защитных механизмов, расширяющих и дополняющих средства безопасности ОС.

Клиентские части решения работают в сетевом режиме, предусматривающем локальное и централизованное управление защитными механизмами, а также централизованное получение информации и изменение состояния защищаемых АРМ или серверов.

На АРМ и серверах, работающих под управлением ОС Astra Linux, и реализующих необходимые меры безопасности посредством механизмов ОС, клиентские части решения не устанавливаются. Для других ОС на базе ядра Linux, на АРМ и серверах, в качестве клиентской части решения, используются Secret Net LSP или Secret Net Studio для Linux.

Сервер безопасности Secret Net Studio реализует возможности централизованного управления клиентами в сетевом режиме функционирования и устанавливается на выделенном виртуальном сервере СОИБ, Сегмент СЗИ (титул 2201). Компонент обеспечивает:

– затирание удаляемой информации;

– хранение данных централизованного управления;

– координацию работы АРМ и серверов в процессе централизованного управления системой;

– получение от клиентов и обработку информации о состоянии защищаемых компьютеров;

– управление пользователями и авторизацией сетевых соединений;

– централизованный сбор, хранение и архивирование журналов;

– отказ сервиса в критических режимах работы ИСУБ (например, срабатывании ПАЗ).

Центр управления Secret Net Studio используется для централизованного управления сервером безопасности и клиентами в сетевом режиме функционирования и устанавливается на АРМ администратора СОИБ, Сегмент управления (титул 2201). Компонент обеспечивает:

– управление параметрами объектов;

– отображение информации о состоянии защищаемых АРМ и серверов и произошедших событиях тревоги;

– загрузку журналов событий.

Защита входа в систему обеспечивает предотвращение доступа посторонних лиц к АРМ или серверу. Используются следующие механизмы защиты входа:

– средства для идентификации и аутентификации пользователей;

– средства блокировки компьютера.

Идентификация и аутентификация пользователя выполняются при каждом входе в систему.

Контроль подключения машинных носителей осуществляется с использованием механизма разграничения доступа к устройствам. Разграничение доступа пользователей к устройствам выполняется на основании списков устройств, которые формируются механизмом контроля подключения и изменения устройств. Механизм контроля подключения и изменения устройств обеспечивает своевременное обнаружение изменений аппаратной конфигурации компьютера и реагирование на эти изменения. Используется динамический контроль конфигурации. Во время работы АРМ или сервера (а также при выходе из спящего режима) драйвер-фильтр устройств отслеживает факты подключения, отключения или изменения параметров устройств. С использованием механизма разграничения доступа к устройствам, администратор осуществляет контроль и установку стандартных разрешений и запретов на выполнение операций с машинными носителями.

Для уничтожения (стирания) или обезличивания данных на машинных носителях используется механизм затирания удаляемой информации. Затирание удаляемой информации делает невозможным восстановление и повторное использование данных после их удаления. Гарантированное уничтожение достигается путем записи случайных последовательностей чисел на место удаленной информации в освобождаемой области памяти. Используется вариант затирания при удалении файловых объектов с машинных носителей, выбранных пользователем, по команде из контекстного меню.

Механизм самозащиты предотвращает несанкционированные остановку критических служб и процессов и выгрузку драйверов Secret Net Studio, обеспечивает защиту программных модулей и ключей системного реестра, необходимых для работы Secret Net Studio, от несанкционированной модификации или удаления. контролируются следующие операции с компонентами клиента Secret Net Studio:

- остановка критических служб и процессов;
- выгрузка драйверов;
- модификация или удаление ключей системного реестра;
- модификация или удаление файлов, в том числе от имени системной учетной записи;
- изменение прав доступа к файлам, папкам и ключам системного реестр.

События, происходящие на АРМ или сервере и связанные с безопасностью системы, регистрируются в соответствующем журнале. Все записи журнала хранятся в файле на системном диске. Также, в базе данных Сервера безопасности, накапливаются журналы событий тревоги со всех управляемых АРМ и серверов, журналы событий, объединяющий журналы решения и штатные журналы ОС со всех управляемых АРМ и серверов.

Механизм контроля целостности предназначен для слежения за неизменностью содержимого ресурсов АРМ и серверов. Действие этого механизма основано на сравнении текущих значений контролируемых параметров проверяемых ресурсов и значений, принятых за эталон. Эталонные значения контролируемых параметров определяются или рассчитываются при настройке механизма. В процессе контроля, при обнаружении несоответствия текущих и эталонных значений, система оповещает администратора о нарушении целостности ресурсов.

Модель данных контроля целостности применяется для ПО ИСУБ, а также используются следующие задания, реализуемые механизмом по умолчанию:

- задание для контроля ресурсов Secret Net Studio;
- задание для контроля реестра ОС;
- задание для контроля файлов ОС.

Синхронизация контрольных сумм осуществляется централизованно и выполняется при загрузке АРМ или сервера.

В механизме дискреционного управления доступом предусмотрена возможность для привилегированных пользователей – администраторов изменять права доступа на любых каталогах и файлах локальных дисков независимо от установленных прав доступа к самим ресурсам. Доступ на изменение каталогов программ, запрещен для пользователей.

Защита доступа к локальным дискам (логическим разделам) АРМ или сервера осуществляется с использованием механизма защиты дисков. Механизм блокирует доступ к дискам при несанкционированной загрузке. Загрузка считается санкционированной, если она выполнена средствами операционной системы с установленным ПО Клиентской части решения. Все другие способы загрузки ОС считаются несанкционированными с точки зрения функционирования механизма.

При отсутствии возможности установки на АРМ сетевой версии клиентской части решения, устанавливается автономная версия с идентичными политиками безопасности.

Сервер безопасности централизованно передает события информационной безопасности, собранные решением в SIEM-коллектор по протоколу syslog.

Параметры политик безопасности решения приведены в таблице 4.2.1.

Таблица 4.2.1 – Параметры политик безопасности Secret Net Studio

Параметр	Значение
Группа «Вход в систему»	
Максимальный период неактивности до блокировки экрана	Не используется
Запрет вторичного входа в систему	Да
Количество неудачных попыток аутентификации	Не используется
Время блокировки при достижении количества неудачных попыток аутентификации	Не используется
Режим идентификации пользователя	По имени (логин и пароль)
Режим аутентификации пользователя	Усиленная аутентификация по паролю
Парольная политика	В соответствии с регламентом
Минимальная длина пароля	Не менее 8 символов. В соответствии с регламентом
Срок действия пароля	Не более 90 дней. В соответствии с регламентом
Сложность пароля	Да
Группа «Журнал»	
Максимальный размер журнала защиты	Не менее 4096
Политика перезаписи событий	Затирать события по мере необходимости
Учетные записи с привилегией просмотра журнала системы защиты	Локальная группа администраторов
Учетные записи с привилегией управления журналом системы защиты	Локальная группа администраторов
Группа «Ключи пользователей»	
Усиленная аутентификация не используется	
Группа «Оповещение о тревогах»	
Локальное оповещение о тревогах	Включено
Группа «Контроль RDP-подключений»	
Перенаправление устройств в RDP-подключениях	COM-портов – Запрещено LPT-портов – Запрещено Дисков – Запрещено Устройств Plug and Play – Запрещено подключать удаленные устройства
Группа «Контроль административных привилегий»	
Самозащита продукта	Включить
Учетные записи с привилегией управления механизмом самозащиты	Локальная группа администраторов
Группа «Дискреционное управление доступом»	
Учетные записи с привилегией управления правами доступа	Локальная группа администраторов
Группа «Затирание данных»	
Количество циклов затирания на локальных дисках	Не менее 1

Параметр	Значение
Количество циклов затирания на сменных носителях	Не менее 1
Количество циклов затирания оперативной памяти	Не используется
Количество циклов затирания по команде «Удалить безвозвратно»	Не менее 1
Количество циклов затирания при уничтожении данных на дисках	Не менее 1
Группа «Полномочное управление доступом»	
Не используется	
Группа «Замкнутая программная среда»	
Не используется	
Группа «Межсетевой экран»	
Не используется	
Группа «Авторизация сетевых соединений»	
Не используется	
Группа «Контроль устройств»	
Список устройств: Параметры контроля	Параметры заданы, при этом для групп «Устройства USB», включен режим «Подключение устройства запрещено»
Список устройств: Разрешения	Заданы
Группа «Контроль печати»	
Список принтеров: Разрешения	Заданы
Группа «Антивирус»	
Не используется	
Группа «Обнаружение вторжений»	
Не используется	
Группа параметров «Идентификатор» в диалоге «Параметры безопасности»	
Не используется	
Группа параметров «Доступ» в диалоге «Параметры безопасности»	
Не используется	
Диалог «Режимы» в диалоговом окне настройки свойств компьютера	
Не используется	
Диалоговое окно настройки параметров задания контроля СЗИ	
Метод контроля ресурсов	Содержимое
Алгоритм	CRC32
Регистрация событий: Успех завершения	Да
Регистрация событий: Ошибка завершения	Да
Регистрация событий: Ошибка проверки	Да
Реакция на отказ: Действия	Игнорировать ошибку
Расписание	При загрузке ОС и по расписанию
Диалоговое окно настройки параметров задания контроля ОС (файлы и реестр)	
Метод контроля ресурсов	Содержимое
Алгоритм	CRC32

Параметр	Значение
Регистрация событий: Успех завершения	Да
Регистрация событий: Ошибка завершения	Да
Регистрация событий: Успех проверки	Нет
Регистрация событий: Ошибка проверки	Да
Реакция на отказ: Действия	Игнорировать ошибку
Расписание	При загрузке ОС и по расписанию

Сертификат ФСТЭК России №3745 (действителен до 16 мая 2025 года) подтверждает соответствие требованиям по безопасности информации, установленных 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 средствах контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной технички. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности при выполнении указаний по эксплуатации, приведенных в формуляре RU.88338853.501400.001 40. Secret Net Studio является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, может применяться в АСУ ТП до 1 класса включительно.

Сертификат ФСТЭК России №2790 (действителен до 18 декабря 2028 года) удостоверяет, что средство защиты информации «Secret Net LSP», является программным средством защиты от несанкционированного доступа к информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленных 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 средствах контроля съемных машинных носителей информации» (ФСТЭК России, 2014), «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты. ИТ.СКН.П4.ПЗ» (ФСТЭК России, 2014), «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по 5 классу защищенности при выполнении условий по эксплуатации, приведенных в формуляре RU.88338853.501410.017 30.

4.2.1.2 Встроенные механизмы защиты прикладного ПО

Встроенные механизмы прикладного ПО предназначены для обеспечения защищенного режима функционирования прикладного ПО ИСУБ ПС250 и ОЗХ. Комплекс встроенных средств встроенных средств прикладного ПО ИСУБ выполняет следующие функции по обеспечению безопасности информации:

– идентификация и аутентификация субъектов доступа при входе в прикладное ПО ИСУБ серверов и АРМ по идентификатору и паролю условно-постоянного действия;

– создание, активация, модификация, отключение и удаление учетных записей;

– регулярная смена пароля для входа в прикладное ПО ИСУБ;

– разграничение доступа субъектов к защищаемым информационным ресурсам на уровне прикладного ПО;

– разграничение доступа к конфигурационным файлам прикладного ПО ИСУБ;

– регистрация действий пользователей и процессов;

– ограничение возможности доступа к уровню операционной системы в среде исполнения;

– аудит событий.

Настройки средств защиты прикладного ПО определены таким образом, чтобы обеспечить:

– состояние защищенности при штатном функционировании ПТК ИСУБ;

– отсутствие влияния на ход автоматизируемого технологического процесса.

4.2.1.3 Встроенные механизмы защиты активного сетевого оборудования

Комплекс встроенных средств активного сетевого оборудования (АСО) предназначен для обеспечения защищенного режима функционирования сетевого оборудования ИСУБ и СОИБ.

С помощью встроенных средств защиты АСО предусматривается принятие следующих мер:

– ограничение доступа к консолям управления АСО списками контроля доступа. Доступ к консолям разрешается только с АРМ администратора СОИБ;

– применение протокола SSH версии 2 для организации защищенного управления;

– включение на АСО маскирования паролей локальных учетных записей;

– для учетных записей администраторов АСО предъявление требования к парольной политике в соответствии с регламентом: минимальная длина пароля должна составлять 8 символов; срок действия пароля учетной записи не должен превышать 3 месяцев; пароль должен состоять из букв разного регистра, цифр и специальных символов;

– ограничение времени действия неиспользуемых открытых консолей управления АСО (время действия ограничивается продолжительностью в 60 секунд);

– ограничение количества неудачных попыток входа в консоль управления АСО, устанавливается равным трём, доступ к консоли при этом блокируется на 120 секунд;

– отключение на АСО неиспользуемых сервисов, предоставляющих возможность организации/возникновения DoS или других видов атак на сетевые ресурсы или ресурсы самого АСО;

– настройка функции port-security на портах АСО, предназначенных для подключения оконечных устройств;

– настройка на АСО запрета доступа к консоли управления по протоколам http, https и telnet;

– отключение на АСО всех неиспользуемых интерфейсов;

– отключение вывода системных сообщений на консольные порты АСО в целях минимизации вероятности истощения их процессорных ресурсов;

– настройка на АСО регистрации и передачи событий ИБ на сервер Комплекса сбора, анализа и корреляции событий безопасности по протоколу syslog;

– создание для сетевого администратора и администратора безопасности информации на АСО отдельных локальных учетных записей с уровнями привилегий 15 (с неограниченными правами на управление АСО) и 1 (с правами на просмотр настроек АСО) соответственно;

– настройка на АСО синхронизации системного времени с использованием NTP-сервера СОИБ.

4.2.2 Комплекс антивирусной защиты

Решение антивирусной защиты строится на базе решений:

– Kaspersky Industrial CyberSecurity for Nodes и Kaspersky Industrial CyberSecurity for Linux Nodes, предназначенного для обеспечения безопасности АРМ и серверов ИСУБ;

– Kaspersky Endpoint Security для Windows и Kaspersky Endpoint Security для Linux, предназначенных для обеспечения безопасности АРМ и серверов СОИБ.

Комплекс антивирусной защиты обеспечивает:

– постоянную защиту файлов на присутствие вирусов и других программ, представляющих угрозу;

– контроль запуска программ;

– защиту от эксплойтов;

– защиту от шифрования;

– регистрацию событий безопасности;

– централизованное и локальное управление параметрами работы механизмов защиты;

– мониторинг и оперативное управление защищаемыми компьютерами;

– централизованный сбор, хранение и архивирование журналов.

Решение наложенных средств защиты от несанкционированного доступа состоит из следующих программных пакетов, устанавливаемых на АРМ, серверах ИСУБ ПС250 и ОЗХ, серверах СОИБ и выделенном сервере управления комплексом:

– функциональный модуль Kaspersky Industrial CyberSecurity for Nodes, клиентская часть решения;

– функциональный модуль Kaspersky Endpoint Security, клиентская часть решения;

– Kaspersky Security Center, сервер управления решением.

Клиентская часть решения предназначена для реализации защиты АРМ или сервера, на которых установлен данный компонент. Является функциональным модулем, фиксирует информацию о состоянии узлов технологической сети, а также выполняет защиту узлов от вредоносного программного обеспечения и других угроз.

Kaspersky Security Center реализует возможности централизованного управления клиентами в сетевом режиме функционирования и устанавливается на выделенном виртуальном сервере СОИБ, Сегмент СЗИ (титул 2201).

Управление решением осуществляется с АРМ администратора СОИБ, Сегмент управления (титул 2201), при подключении к консоли Kaspersky Security Center.

Задача постоянной защиты файлов Kaspersky Industrial CyberSecurity for Nodes проверяет следующие объекты, при доступе к ним:

– затирание удаляемой информации;

– файлы;

– альтернативные потоки данных файловой системы;

– основную загрузочную запись и загрузочные секторы локальных жестких дисков и внешних устройств;

– файлы-контейнеры ОС.

Комплекс антивирусной защиты перехватывает все файлы, с которыми ПО или пользователь осуществляют операции чтения или записи, проверяет эти файлы на наличие угроз и, при обнаружении угрозы, выполняет одно из действий:

– пытается вылечить файл;

– перемещает файл на карантин;

– удаляет его.

Постоянная защита файлов ищет вредоносные программы с помощью:

– затирание удаляемой информации;

– сигнатурного анализа вредоносных программ;

– эвристического анализа.

Используется «рекомендуемый» уровень безопасности, обеспечивающий оптимальное качество защиты и влияния на производительность АРМ и серверов. Уровень рекомендован производителем как достаточный для защиты устройств и установлен по умолчанию.

Компонент контроля запуска программ Kaspersky Industrial CyberSecurity for Nodes отслеживает попытки запуска программ пользователями и проверяет, входят ли данные программы в список разрешенных. Компонент передает администратору СОИБ информацию о запуске любой программы, не входящей в разрешенный список, и автоматически блокирует её.

Задача контроля запуска программ работает по принципу запрета по умолчанию: все программы, не указанные в качестве разрешенных в параметрах задачи, автоматически блокируются. При запуске каждого объекта проверяется наличие для него правил. Запуск разрешается, если есть разрешающее правило и нет запрещающих правил.

В качестве атрибутов программы, с помощью которых можно создавать правила белых и черных списков используются контрольные суммы (SHA-256):

– разрешенные файлы четко заданы контрольной суммой;

– позволяют блокировать запуск известных вредоносных объектов в случае инцидентов. Опубликованные в публичных источниках SHA256 хеш-суммы добавляются в правила блокировки.

Задача контроля запуска программ работает в Режиме статистики, обеспечивающем фиксацию запуска объектов.

Компонент защиты от эксплойтов Kaspersky Industrial CyberSecurity for Nodes защищает память исполняемых процессов от эксплуатации уязвимостей. Специальная служба Kaspersky Security Exploit Prevention Service (kavsslp) внедряет агента защиты exploitblocker.dll в защищаемые процессы, который контролирует их целостность. Список программ, которые защищает компонент от эксплуатации уязвимостей в них, ограничен техническими решениями Kaspersky.

Компонент защиты от эксплойтов работает в режиме «Terminate on exploit», обеспечивающим завершение скомпрометированного процесса. При обнаружении эксплуатации уязвимости в критичном процессе Windows, решение не будет останавливать данный процесс.

Задача защиты от шифрования Kaspersky Industrial CyberSecurity for Nodes отслеживает активность в папках общего доступа защищаемых серверов ИСУБ. Компонент защиты от шифрования использует эвристических механизм для определения попыток шифрования данных. Если компонент обнаруживает попытки вредоносного шифрования в папках общего доступа, то сессия удаленного пользователя блокируется на определенный администратором СОИБ период времени.

Защита от шифрования не блокирует доступ со стороны узла к папке общего доступа на защищаемом АРМ до тех пор, пока активность этого узла не признана вредоносной.

Задача работает в активном режиме и автоматически блокирует доступ к файловым ресурсам для текущей пользовательской сессии, если будет обнаружена активность, схожая с действиями вредоносных программ-шифровальщиков.

На АРМ операторов АСУ (титул 005), дополнительно, на клиентских частях Kaspersky Industrial CyberSecurity for Nodes, используется задача управления сетевых экраном, обеспечивающая контроль состояния параметров и правил сетевого экрана ОС. Программа блокирует любую настройку параметров сетевого экрана ОС, когда, например, программа или инструмент добавляют или удаляют какое-то правило. Решение проверяет сетевой экран ОС и, при необходимости, восстанавливает набор правил сетевого экрана.

Kaspersky Endpoint Security используется в версии «Стандартный» и обеспечивает:

- защиту от файловых угроз;
- защиту от атак BadUSB;
- контроль приложений;
- анализ поведения;
- защиту от эксплойтов;
- откат вредоносных действий.

Сервер управления решением Kaspersky Security Center централизованно передает события информационной безопасности, собранные Комплексом антивирусной защиты в SIEM-коллектор по протоколу syslog.

Сертификат ФСТЭК России №3907 (действителен до 3 апреля 2026 года) удостоверяет, что программное изделие «Kaspersky Industrial CyberSecurity for Nodes», является средством антивирусной защиты, 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 2 уровню доверия (в исполнениях Windows и Linux), «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012) (в исполнениях Windows и Linux), задании по безопасности 643.46856491.00093-08 99 01 (в исполнениях Windows и Linux) при выполнений указаний по эксплуатации, приведенных в формуляре 643.46856491.00093-08 30 01.

Сертификат ФСТЭК России №3155 (действителен до 6 мая 2025 года) удостоверяет, что программное изделие «Kaspersky Security Center», является средством антивирусной защиты, 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 2 уровню доверия, «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа А второго класса защиты. ИТ.САВЗ.А2.ПЗ» (ФСТЭК России, 2012) и заданий по безопасности 643.46856491.00069-09 99 91 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00069-09 30 01.

Сертификат ФСТЭК России №4068 (действителен до 22 января 2029 года) удостоверяет, что программное изделие «Kaspersky Endpoint Security для Windows», является средством антивирусной защиты, 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 2 уровню доверия, «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной

защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012) и заданий по безопасности 643.46856491.00100-08 99 01 при выполнении указаний по эксплуатации, приведенных в формуляре 643.46856491.00100-08 30 01.

4.2.3 Комплекс анализа защищенности инфраструктуры

Решение Комплекса анализа защищенности инфраструктуры строится на базе решения XSpider, предназначенного для обеспечения безопасности АРМ и серверов ИСУБ.

Комплекс анализа защищенности инфраструктуры предназначен для обеспечения функций по инвентаризации информационных систем, выявлению уязвимостей компонентов ИСУБ ПС250 и ОЗХ и определению способов их устранения.

XSpider реализует концепцию сканирования узлов без применения заранее установленных агентов. XSpider использует сеть для связи с объектами сканирования. На межсетевых экранах Комплекса обеспечения сетевой безопасности СОИБ производится открытие сетевых портов, используемых сканером.

Комплекс анализа защищенности инфраструктуры обеспечивает выполнение следующих функций:

– инвентаризация информационных систем (активного сетевого оборудования, серверов и АРМ);

– сканирование доступности сетевых портов компонентов ИСУБ ПС250 и ОЗХ и СОИБ;

– автоматический поиск (анализ) уязвимостей компонентов ИСУБ ПС250 и ОЗХ и СОИБ, и группировку обнаруженных уязвимостей по приоритетам;

– определение рекомендаций по устранению выявленных уязвимостей.

Для решения указанных задач средствами Комплекса анализа защищённости инфраструктуры производится сканирование узлов сетевых сегментов и формирование отчетов по результатам сканирования. Перечень узлов для сканирования определяется Администратором СОИБ и задается в настройках сканирования.

Комплекс анализа защищенности инфраструктуры обеспечивает сканирование узлов с использованием следующих профилей: профиль анализа уязвимостей, профиль инвентаризации и профиль соответствия требованиям.

Анализ защищенности контролируемых узлов производится при сканировании с использованием профилей анализа уязвимостей и профиля соответствия требованиям.

Сканирование с использованием профиля анализа уязвимостей направлено на получение оценки защищенности контролируемого узла. С помощью данного сканирования выявляются уязвимости программного обеспечения, проверка стойкости паролей и отсутствующие обновления ОС.

При сканировании с использованием профиля анализа уязвимостей выявляются уязвимости, которые могут быть использованы внешним по отношению к контролируемому узлу нарушителем (т.е. нарушителем, который для реализации угрозы может использовать только взаимодействие с контролируемым узлом по доступным протоколам сетевого и транспортного уровней). Отчет об уязвимостях, выявленных с использованием профиля анализа уязвимостей, содержит перечень протоколов, доступных для взаимодействия с контролируемым узлом, и выявленные уязвимости в реализации данных протоколов.

Контроль соответствия требованиями безопасности производится при сканировании с использованием профиля соответствия требованиям.

При сканировании в режиме соответствия требованиям, выполняется проверка контролируемого узла на соответствие стандартам безопасности.

Инвентаризация программного и аппаратного обеспечения контролируемых узлов производится при сканировании с использованием профиля инвентаризации. Для представления собранной инвентаризационной информации используется отчет об инвентаризации. Сведения, отображаемые в отчете об инвентаризации, определяются типом сканируемого узла.

В общем виде, перечень результатов сканирования включает в себя:

- перечень сетевых служб, предоставляемых сканируемым узлом (протокол, порт, идентификатор службы – если по результатам сканирования ее удалось идентифицировать);
- перечень выявленных уязвимостей (отдельно по каждой службе) с информацией по каждой уязвимости;
- информация об операционной системе;
- перечень идентифицированных программных средств;
- перечень выявленных уязвимостей (отдельно по каждому программному средству).

Информация о выявленных уязвимостях включает в себя:

- описание уязвимости;
- индекс уязвимости в каталоге CVE (если уязвимость присутствует в каталоге);
- оценку критичности уязвимости;
- рекомендации по устранению уязвимости;
- ссылки на публикации об уязвимости.

XSpider обеспечивает автоматический запуск задач на сканирование в соответствии с задаваемым Администратором СОИБ расписанием. Периодичность расписания сканирования задается в соответствии с соответствующим регламентом.

Комплекс анализа защищенности инфраструктуры реализуется в виде виртуального сервера и располагается в сегменте СОИБ, Сегмент СЗИ (титул 2201).

Сертификат ФСТЭК России №3247 (действителен до 24 октября 2025 года) удостоверяет, что программное изделие «Сетевой сканер безопасности XSpider 7.8.25», является средством автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем и средств вычислительной техники, обрабатывающих информацию, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) – по 4 уровню доверия и технических условиях ЕВРГ.620129000.XS-7.8.25 ТУ при выполнении указаний по эксплуатации, приведенных в формуляре ЕВРГ.620129000.XS-7.8.25 30 02.

4.2.4 Комплекс сбора, анализа и корреляции событий безопасности

Решение Комплекса сбора, анализа и корреляции событий безопасности строится на базе решения Kaspersky Unified Monitoring and Analysis Platform.

Комплекс сбора, анализа и корреляции событий безопасности обеспечивает:

- обнаружение, сбор и фильтрация событий безопасности;
- корреляцию и агрегация событий безопасности, и обнаружение инцидентов ИБ;
- построение отчетов и оповещение об инцидентах ИБ;
- обеспечение хранилища исходных и нормализованных событий безопасности;
- возможность управления журналами событий безопасности.

Комплекс сбора, анализа и корреляции событий включает в себя:

- SIEM-коллектор Kaspersky Unified Monitoring and Analysis Platform, обеспечивающий сбор событий безопасности с АРМ, серверов ИСУБ ПС250 и ОЗХ, серверов СОИБ;
- Windows Agent, обеспечивающий сбор и отправку на SIEM-коллектор событий безопасности с серверов Windows в пассивном режиме WEC, по подписке.

SIEM-коллектор позволяет собирать, нормализовать, анализировать события с источников операционных систем семейства Windows путем настройки аудита на источнике и создания пользователя с правами на чтение журналов событий и отправку событий на компонент Windows Agent.

Для более подробного анализа событий WinEventLog в системе на источниках настраивается расширенный аудит событий системы. Аудит настраивается путем применения групповых политик к серверам и пользовательским компьютерам в соответствии с типом источника.

Windows Agent обеспечивает сбор и отправку на SIEM-коллектор по протоколу http событий, хранящихся в следующих журналах:

- Application;
- System;
- Forwarded Events.

SIEM-коллектор позволяет собирать, нормализовать, анализировать события с источников операционных систем семейства Linux путем настройки журналирования на источнике и отправки событий по syslog.

Для более подробного анализа событий Linux в системе на источниках настраивается расширенный аудит событий системы. Аудит настраивается путем применения настройки службы auditd на каждом источнике отдельно.

Также SIEM-коллектор позволяет собирать, нормализовать, анализировать события со следующих источников, путем настройки журналирования на источниках и отправки событий по syslog:

– сервер безопасности Комплекса средств защиты от несанкционированного доступа;

– сервер централизованного управления МСЭ Комплекса обеспечения сетевой безопасности;

– сервер управления решением Комплекса централизованного управления доступом к активному сетевому оборудованию и Комплекса контроля конфигураций;

– система виртуализации СОИБ;

– активное сетевого оборудования СОИБ;

– OPC-коллектор.

SIEM-коллектор позволяет собирать события с Сервера управления решением Комплекса антивирусной защиты KSC, путем подключения к базам SQL источников с помощью учетной записи, созданной и для Windows источников.

Передача событий с источников на SIEM-коллектор осуществляется в одностороннем порядке с инициацией отправки событий от источника.

Порт прослушивания для разного типа источников используется разный, так как на одном ресурсе, SIEM-коллектор позволяет использовать нормализатор только для одного типа источников.

SIEM-коллектор СОИБ отправляет нормализованные и агрегированные события в коррелятор и хранилище Kaspersky Unified Monitoring and Analysis Platform, расположенных в корпоративном сегменте.

SIEM-коллектор и Windows Agent устанавливаются на выделенных виртуальных серверах СОИБ, Сегмент СЗИ (титул 2201).

Сертификат ФСТЭК России №4455 (действителен до 28 сентября 2026 года) удостоверяет, что программное изделие «Kaspersky Unified Monitoring and Analysis Platform», является системой управления событиями информационной безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия технических условиях ТУ 643.468556491.0016-03 при выполнении указаний по эксплуатации, приведенных в формуляре 643.468556491.0016-03 30 01.

4.2.5 Комплекс резервного копирования информационных ресурсов

Решение Комплекса резервного копирования информационных ресурсов строится на базе решения Кибер Бэкап, устанавливаемый в виде пакетов на ОС сервера СИЛА СР2-6327.

Комплекс резервного копирования предназначен для резервного копирования и восстановления данных АРМ и серверов ИСУБ ПС250 и ОЗХ, компонентов СОИБ.

Комплекс резервного копирования выполняет следующие функции:

– выполнение резервного копирования и восстановления виртуальных машин (серверов), размещённых во внедряемой среде виртуализации;

– резервное копирование и восстановление данных внутри виртуальных машин с использованием агентов резервного копирования;

– позволяет создавать дополнительные резервные копии для переноса на съемные носители информации;

– обеспечение резервного копирования и восстановления конфигурационных файлов;

– выполнение резервного копирования по расписанию;

– контроль целостности резервных копий;

– шифрование резервных копий;

– управление процессами резервного копирования и восстановления данных.

Система резервного копирования взаимодействует со следующими подсистемами:

– система виртуализации СОИБ;

– АРМ и серверы ИСУБ ПС250 и ОЗХ;

– контроллер домена СОИБ.

Комплекс резервного копирования информационных ресурсов состоит из программных пакетов, устанавливаемых на АРМ, серверах ИСУБ ПС250 и ОЗХ, серверах СОИБ, выделенном сервере управления и узле хранения:

– сервер управления решением;

– узел хранения;

– агенты резервного копирования.

Сервер управления решением (далее СУ) является ядром системы, к нему подключаются устройства, регистрируются агенты, создаются планы резервного копирования, репликации резервных копий, проверки целостности, очистки и приходит информация о выполнении назначенных планов. К СУ производится подключение хранилищ резервных копий и управление ими. СУ осуществляет мониторинг событий и позволяет создавать отчеты по резервному копированию. СУ отвечает за обмен данными с агентами защиты и выполняет задания общего характера по управлению планом.

СУ комплекса резервного копирования устанавливается на выделенном виртуальном сервере СОИБ, Сегмент инфраструктурных сервисов СОИБ (титул 2201).

Узел хранения — это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров управляемых машин), требуемых для защиты корпоративных данных. Это достигается путем организации хранилищ и управления хранилищами, выделенными для корпоративных архивов резервных копий (управляемыми хранилищами).

Наиболее важной функцией узла хранения является дедупликация и сжатие резервных копий в его хранилищах. Дедупликация означает, что из резервных копий исключаются дубликаты повторяющихся копий данных и заменяются ссылкой на уникальные данные. Таким образом минимизируется использование сети при резервном копировании и занимаемое дисковое пространство.

Узел хранения располагается на выделенном физическом сервере с локальными дисками, предназначенными для организации хранения и обработки данных резервных копий.

Агенты — это приложения (пакеты), выполняющие резервное копирование данных, их восстановление и другие операции на машинах под управлением СУ.

Система резервного копирования также позволяет осуществлять процесс резервного копирования платформы виртуализации в «безагентном» режиме резервного копирования. Безагентный режим означает, что агент резервного копирования не устанавливается внутрь виртуальных машин, а ставится в виде отельной виртуальной машины или в виде приложений (пакетов) на хосты гипервизора и позволяют взаимодействовать с платформой виртуализации через API интерфейс системы.

Управление решением осуществляется с АРМ администратора СОИБ, Сегмент управления (титул 2201), при подключении к консоли Сервера управления решением.

Резервное копирование осуществляется:

– централизованное автоматическое резервное копирование виртуальных машин;

– при помощи Агентов резервного копирования, устанавливаемых на АРМ и серверах ИСУБ ПС250 и ОЗХ, с передачей резервных копий в Систему хранения данных.

Решение обеспечивает реализацию следующего функционала:

– создание полных, дифференциальных и инкрементных резервных копий;

– блочное и файловое резервное копирование;

– резервное копирование с помощью технологии Changed Block Tracking (CBT) и Volume Shadow Copy Service (VSS);

– сжатие резервных копий;

– исключение файлов из копирования;

– дедупликацию данных;

– ограничение доступа к управлению резервным копированием и восстановлением данных;

– восстановления резервной копии диска в новую виртуальную машину;

– поддержка Pre и Post команды для операций резервных копий.

Сертификат ФСТЭК России №4337 (действителен до 11 декабря 2025 года) удостоверяет, что программный комплекс «Кибер Бэкап», является программным средством резервного копирования и восстановления информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 4 уровню доверия и технических условиях 29176085.582929.015 ТУ 01-1 при выполнении указаний по эксплуатации, приведенных в формуляре 29176085.582929.015 30 01-1.

4.2.6 Комплекс обеспечения сетевой безопасности

Решение Комплекса обеспечения сетевой безопасности строится на базе решения InfoWatch ARMA.

Комплекс обеспечения сетевой безопасности предназначен для обеспечения защиты компонентов ИСУБ ПС250 и ОЗХ и компонентов СОИБ при взаимодействии с иными системами и информационно-телекоммуникационными сетями.

Комплекс обеспечения сетевой безопасности обеспечивает следующие функции:

– защита периметра АСУ;

– управление сетевыми потоками и сетевыми соединениями;

– эшелонированная защита АСУ;

– сегментация сети;

– ограничение доступа к архитектуре и конфигурации защищаемой системы;

– управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами АСУ, а также между СОИБ и иными системами и сетями связи;

– защита от скрытых каналов передачи информации;

– регистрация и хранение информации о сетевых потоках и соединениях, событий безопасности, регистрируемых компонентами комплекса.

Комплекс обеспечения сетевой безопасности включает в себя следующий перечень компонентов:

– межсетевые экраны периметра АСУ;

– межсетевые экраны периметра ЛСУ;

– сервер централизованного управления МСЭ.

Межсетевые экраны периметра АСУ реализуются в виде отказоустойчивого кластера аппаратных межсетевых экранов ARMA-19RACK-10G, функционирующего в режиме Active/Passive. МСЭ периметра АСУ обеспечивают контроль и фильтрацию трафика между СОИБ, технологическим сегментом АСУ и внешними по отношению к СОИБ системами и сетями связи.

Межсетевые экраны периметра ЛСУ устанавливаются в виде отказоустойчивого кластера аппаратных межсетевых экранов ARMA-19RACK-10G, функционирующего в режиме Active/Passive. МСЭ периметра ЛСУ обеспечивают контроль и фильтрацию трафика между СОИБ, технологическим сегментом ЛСУ, а также контроль и фильтрацию необходимого трафика между технологическими сегментами АСУ и ЛСУ.

Сервер централизованного управления МСЭ реализуется в виде виртуальной машины в среде виртуализации СОИБ, Сегмент СЗИ (титул 2201) на базе программного обеспечения ARMA Management Console, и обеспечивает централизованное управление МСЭ в составе комплекса, объектами и элементами политик МСЭ, централизованный сбор и хранение событий безопасности с МСЭ.

Межсетевые экраны периметра АСУ реализуют следующие внутренние сегменты:

- сегмент СЗИ СОИБ;
- сегмент инфраструктурных сервисов СОИБ;
- сегмент управления СОИБ;
- сегмент АСУ.

Межсетевые экраны периметра ЛСУ реализуют внутренний Сегмент ЛСУ.

ARMA Industrial Firewall используют лицензию Enterprise МЭ плюс СОВ (межсетевой экран «следующего поколения» NGFW). Лицензия Enterprise СОВ расширяется совместным приобретением лицензий:

- Enterprise Промышленные протоколы;
- Enterprise OPCDA.

СОВ в ARMA Industrial Firewall основана на ПО «Suricata» с открытым исходным кодом и использует метод захвата пакетов «Netmap» для повышения производительности и минимизации нагрузки на центральный процессов.

СОВ в ARMA Industrial Firewall позволяет решать следующие задачи:

– обнаружение и предотвращение эксплуатирования уязвимостей в протоколах DNS, FTP, ICMP, IMAP, POP3, HTTP, NetBIOS, DCERPC, SNMP, TFTP, VOIP;

– обнаружение и предотвращение использования эксплойтов и уязвимостей сетевых приложений;

- обнаружение и блокировка DOS-атак;
- обнаружение и блокировка сетевого сканирования;
- блокировка трафика ботнетов;
- блокировка трафика от скомпрометированных хостов;

– блокировка трафика от хостов, зараженных троянским ПО и сетевыми червями.

Подсистема контроля уровня приложений модуля СОВ реализована на базе технологии глубокой инспекции пакетов протоколов прикладного уровня, включая промышленные протоколы.

Межсетевые экраны СОИБ позволяют контролировать и обнаруживать вторжения по таким протоколам, как Modbus TCP, Modbus TCP x90 func. code (UMAS), OPC UA, OPC DA, IEC 60870 5 104, IEC 61850-8-1 MMS, IEC 61850-8-1 GOOSE.

Взаимодействие между сетями кластера межсетевых экранов МСЭ СОИБ периметра ЛСУ и Кластера МСЭ СОИБ периметра АСУ осуществляется на 3 (сетевом) уровне модели OSI. Ограничения во взаимодействии между сетями периметра ЛСУ и периметра АСУ реализованы посредством заранее согласованных разрешающих правил доступа.

Межсетевые экраны СОИБ обеспечивают возможность передачи технологических данных с OPC-коллектора в Концентратор данных ДМЗ ОКИИ.

Межсетевые экраны СОИБ обеспечивают возможность взаимодействия агентских компонентов Комплексов СОИБ с соответствующими серверами управления Комплексов СОИБ.

Список правил доступа определяется в рабочей документации / на момент проведения пуско-наладочных работ.

Сервер управления решением централизованно передает события информационной безопасности, собранные Комплексом обеспечения сетевой безопасности в SIEM-коллектор по протоколу syslog.

ARMA Industrial Firewall отправляет события безопасности модулей МЭ, СОВ, контроля уровня приложений, а также системные события.

Для управления учетными записями администраторов и синхронизации с сервером точного времени, Сервер управления решением подключается к Контроллеру домена СОИБ.

Сертификат ФСТЭК России №4429 (действителен до 27 июля 2026 года) удостоверяет, что программный комплекс «InfoWatch ARMA Industrial Firewall Решение» является программным средством защиты информации, соответствует требованиям по безопасности информации по 4 уровню доверия, требованиям к МЭ типа «Д» 4 класса защиты (ИТ.МЭ.Д4.П3) и СОВ уровня сети 4 класса защиты (ИТ.СОВ.С4.П3) и задании по безопасности. Может применяться в АСУ ТП, 1 класса защищенности включительно.

4.2.7 Комплекс защиты среды виртуализации

Комплекс защиты среды виртуализации, реализуется на базе встроенных функций системы виртуализации zVirt Max.

Комплекс защиты среды виртуализации обеспечивает следующие функции:

– идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

– управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

– регистрация событий безопасности в виртуальной инфраструктуре;

– разбиение виртуальной инфраструктуры на сегменты.

Управление доступом в виртуальной инфраструктуре реализуется на базе встроенного функционала Системы виртуализации СОИБ с использованием ролевой модели. Роли предоставляют разрешения на доступ к различным уровням ресурсов в центре данных и к конкретным физическим и виртуальным ресурсам и управление ими.

В качестве внешней службы каталогов пользователей используется LDAP на Контроллере домена СОИБ. По умолчанию пользователи домена не могут входить в систему, поэтому им назначаются необходимые права доступа.

Утилита ovirt-aaa-jdbc-tool переопределяет политику паролей по умолчанию, которая применяется к паролям, задаваемым посредством ovirt-aaa-jdbc-tool.

Политиками безопасности системы виртуализации обеспечивается, в соответствии с соответствующим регламентом:

– управление минимальной длины пароля с использованием параметра MIN_LENGTH;

– управление сроком действия для паролей с использованием параметра PASSWORD_EXPIRATION_DAYS;

– управление количеством старых паролей, которые не должны повторяться при смене пароля, с использованием параметра PASSWORD_HISTORY_LIMIT;

– управление количеством дней по уведомлению пользователя до истечения срока действия пароля, с использованием параметра PASSWORD_EXPIRATION_NOTICE_DAYS;

– управление сложностью паролей, с использованием шаблона PASSWORD_COMPLEXITY.

Управление доступом внутри виртуальных машин реализуется при помощи функционала разграничения доступа наложенных средств защиты от несанкционированного доступа Комплекса средств защиты от несанкционированного доступа на базе решения Secret Net Studio.

На сетевом (канальном) уровне обеспечивается изоляция трафика внутри сегментов с использованием виртуальных локальных сетей (VLAN).

Виртуальные серверы размещаются в следующих сетевых сегментах:

– сегмент СЗИ СОИБ;

– сегмент инфраструктурных сервисов СОИБ.

Система виртуализации обеспечивает передачу событий безопасности на SIEM-коллектор Комплекса сбора, анализа и корреляции событий безопасности по протоколу syslog.

Сертификат ФСТЭК России № 4780 (действителен до 19 февраля 2029 года) подтверждает соответствие требованиям руководящих документов к 4 уровню доверия средств обеспечения безопасности информационных технологий. Защищенная среда виртуализации zVirt Max может применяться для обеспечения информационной безопасности в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности.

4.2.8 Комплекс контроля конфигураций

Комплекс контроля конфигураций реализуется на базе решения Efros Defence Operations.

Комплекс контроля конфигураций предназначен для обеспечения централизованного контроля изменений конфигурационных файлов активного сетевого оборудования, средств межсетевого экранирования и ОС в составе СОИБ и ИСУБ ПС250 и ОЗХ.

Функционал Комплекса контроля конфигураций состоит из следующих модулей:

– модуль контроля сетевых устройств Efros Network Assurance: предназначен для контроля активного сетевого оборудования и межсетевых экранов, с последующим их отображением на карте сети с возможностью моделирования прохождения трафика;

– модуль контроля операционных систем Efros Integrity Check Compliance: предназначен для контроля конфигураций операционных систем.

Комплекс контроля конфигураций выполняет следующие функции:

– контроль изменения конфигураций сетевого оборудования;

– контроль изменения конфигураций межсетевых экранов;

– проверки соответствия безопасности сетевого оборудования;

– проверки соответствия безопасности межсетевых экранов;

– визуализация на карте сети возможных маршрутов прохождения заданного типа трафика;

– контроль целостности и оперативное восстановление конфигураций;

– моделирование трафика на основе маршрутов и правил межсетевых экранов;

– контроль изменения конфигураций операционных систем;

– осуществление проверок соответствия (compliance) объектов защиты требованиям регуляторов, корпоративным стандартам безопасности;

– предоставление рекомендаций по внесению изменений для соответствия стандартам безопасности.

Комплекс контроля конфигураций входит в состав единого программного комплекса, реализующего функционал контроля безопасности конфигураций и централизованного управления доступом к активному сетевому оборудованию.

Комплекс состоит из следующих программных пакетов, устанавливаемых на АРМ, серверах ИСУБ ПС250 и ОЗХ, серверах СОИБ:

– сервер управления решением;

– агенты контроля конфигураций.

Сервер управления решением по контролю конфигураций входит в состав единого программного комплекса совместно с комплексом централизованного управления доступом к активному сетевому оборудованию и устанавливается на выделенный виртуальный сервер СОИБ, Сегмент СЗИ (титул 2201).

Сервер управления решением реализует функционал по контролю и проверке конфигураций сетевого оборудования и МСЭ, управляет агентами и консолидирует информацию в единой централизованной системе.

Агенты контроля конфигураций устанавливаются на контролируемые серверы и обеспечивают операции контроля конфигураций операционных систем.

Сервер управления решением передает события информационной безопасности, собранные решением в SIEM-коллектор по протоколу syslog.

Сертификат ФСТЭК России № 4618 (действителен до 7 декабря 2027 года) удостоверяет, что программный комплекс по защите системно-технической инфраструктуры «Efros Defense Operations», является программным средством контроля (анализа) защищенности информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «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 и технических условиях ТУ 58.2940-077-72410666-2021, при выполнении указаний по эксплуатации, приведённых в формуляре 643.72410666.00077-02 30 01.

4.2.9 Комплекс управления обновлениями программного обеспечения

Комплекс управления обновлениями программного обеспечения предназначен для обновления операционных систем, прикладного ПО, баз данных сигнатур, компонентов СОИБ. Комплекс управления обновлениями программного обеспечения выполняет следующие функции:

– обновление базы данных сигнатур Комплекса антивирусной защиты и Комплекса сетевой безопасности;

– обновление операционных систем АРМ, серверов ИСУБ и компонентов СОИБ;

– обновление прикладного ПО на АРМ и серверах ИСУБ;

– обновление средств защиты информации, входящих в состав СОИБ, активного сетевого оборудования СОИБ, инфраструктурных сервисов СОИБ;

– контроль целостности устанавливаемых обновлений;

– тестирование устанавливаемых обновлений.

Комплекс управления обновлениями программного обеспечения состоит из следующих программных пакетов, устанавливаемых на выделенных серверах управления комплексом:

– файловый сервер;

– сервер обновления операционных систем Windows на базе решения Windows Server Update Services;

– сервер обновления операционных систем Linux на базе решения Astra Configuration Manager;

– Компоненты Комплексов СОИБ, обеспечивающие централизованную установку обновлений для соответствующих средств защиты информации.

Файловый сервер используется для доставки из МСПД протестированных на совместимость обновлений прикладного ПО, обновлений операционных систем, баз данных сигнатур, прошивок активного сетевого оборудования.

Доставка обновлений из МСПД производится вручную, инициация доставки со стороны Файлового сервера запрещена. Файловый сервер используется Сервером обновлений операционных систем и Компонентами Комплексов СОИБ, обеспечивающих централизованную установку обновлений, в качестве источника обновлений.

Серверы обновлений операционных систем и Компоненты Комплексов СОИБ, обеспечивающие централизованную установку обновлений, используется для централизованного обновления операционных систем и Комплексов СОИБ, соответственно.

Обновление компонентов СОИБ и ИСУБ может производится как в автоматическом, так и в ручном режиме, в соответствии с принятыми правилами и процедурами управления обновлениями программного обеспечения.

Файловый сервер устанавливается на выделенном виртуальном сервере СОИБ, Сегмент инфраструктурных сервисов СОИБ (титул 2201).

Серверы обновления операционных систем устанавливается на выделенных виртуальных серверах СОИБ, Сегмент инфраструктурных сервисов СОИБ (титул 2201).

Управление решением осуществляется с АРМ администратора СОИБ, Сегмент управления (титул 2201).

4.2.10 Комплекс централизованного управления доступом к активному сетевому оборудованию

Комплекс контроля конфигураций реализуется на базе решения Efros Defence Operations, модуль Network Access Control.

Комплекс централизованного управления доступом к активному сетевому оборудованию предназначен для централизованного предоставления и контроля доступа администраторов к сетевым устройствам.

Комплекс централизованного управления доступом к активному сетевому оборудованию обеспечивает выполнение следующих функций в рамках СОИБ:

– ролевое разграничение доступа администраторов при доступе к сетевому оборудованию;

– назначение минимально необходимых прав и привилегий администраторам при доступе к сетевому оборудованию;

– управление административным доступом к активному сетевому оборудованию;

– использование политик TACACS+ для доступа на сетевое оборудование;

– проверки/разграничения прав доступа администраторов на выполнение отдельных команд по управлению сетевыми устройствами;

– регистрация фактов доступа администраторов к сетевому оборудованию;

– регистрация выполнения конкретных команд управления на сетевом оборудовании.

Комплекс централизованного управления доступом к активному сетевому оборудованию входит в состав единого программного комплекса, реализующего функционал контроля безопасности конфигураций и централизованного управления доступом к активному сетевому оборудованию.

Комплекс централизованного управления доступом к активному сетевому оборудованию состоит из Сервера централизованного управления доступом, который входит в состав единого программного комплекса совместно с Комплексом контроля конфигураций и устанавливается на выделенный виртуальный сервер СОИБ, Сегмент СЗИ (титул 2201).

Для интеграции с решением, предварительно настраивается АСО для взаимодействия с Сервером централизованного управления доступом, с использованием механизмов AAA по протоколу TACACS+.

Для доступа к каталогу учетных записей администраторов, для их сверки, Сервер централизованного управления доступом подключается к Контроллеру СОИБ.

Решение обеспечивает составление списка набора команд для администраторов, работающих с оборудованием. Это позволяет контролировать выполняемые действия с контролируемым оборудованием.

Также решение обеспечивает настройку протоколов, которые могут использоваться во время проверки аутентификации при доступе.

В рамках решения обеспечивается профилирование сетевого оборудования и профили авторизации. Профилирование необходимо для назначения общих правил аутентификации и авторизации на оборудовании.

Решение обеспечивает управления доступом на оборудование на основе политик – списка наборов политик доступа на оборудование Наборы политик позволяют логически группировать политики аутентификации и авторизации в одном наборе.

Сервер централизованного управления доступом передает события информационной безопасности, собранные решением в SIEM-коллектор по протоколу syslog.

Сертификат ФСТЭК России № 4618 (действителен до 7 декабря 2027 года) удостоверяет, что программный комплекс по защите системно-технической инфраструктуры «Efros Defense Operations», является программным средством контроля (анализа) защищенности информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности

информации, установленным в документе «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 и технических условиях ТУ 58.2940-077-72410666-2021, при выполнении указаний по эксплуатации, приведённых в формуляре 643.72410666.00077-02 30 01.

4.2.11 Комплекс организационных мероприятий по обеспечению информационной безопасности

На этапе ввода в действие ИСУБ ПС250 и ОЗХ, разрабатываются организационно-распорядительные документы, регламентирующие:

– правила и процедуры идентификации и аутентификации;

– правила и процедуры управления доступом;

– правила и процедуры защиты машинных носителей информации;

– определение состава и содержания информации о событиях безопасности, подлежащих регистрации;

– правила и процедуры антивирусной защиты;

– правила и процедуры обеспечения целостности;

– правила и процедур обеспечения доступности;

– контроль предоставляемых вычислительных ресурсов и каналов связи;

– правила и процедуры защиты технических средств и систем;

– правила и процедуры защиты автоматизированных систем и их компонентов;

– правила и процедуры реагирования на компьютерные инциденты;

– правила и процедуры управления конфигурацией автоматизированных систем;

– правила и процедуры управления обновлениями программного обеспечения;

– правила и процедуры планирования мероприятий по обеспечению защиты информации;

– правила и процедуры обеспечения действий в нештатных ситуациях;

– правила и процедуры информирования и обучения персонала.

4.3 Инфраструктурные решения СОИБ

4.3.1 Активное сетевое оборудование

4.3.1.1 Общие принципы

Активное сетевое оборудование СОИБ предназначено для обеспечения компонентов СОИБ сетевой связностью с сетевой инфраструктурой ИСУБ ПС250 и ОЗХ.

Активное сетевое оборудование обеспечивает следующие функции:

– обеспечение доступа сегмента СОИБ к сети передачи данных ИСУБ ПС250 и ОЗХ;

– коммутация трафика между конечными устройствами внутри сегмента СОИБ;

– резервирование подключения конечных устройств СОИБ к сети передачи данных ИСУБ ПС250 и ОЗХ.

В рамках СОИБ коммутаторы устанавливаются в следующие сегменты сети:

– сегмент сети СОИБ;

– сегмент периметра АСУ (ядро периметра АСУ);

– сегмент периметра ЛСУ и управления ЛСУ Modbus (ядро периметра ЛСУ);

– сегмент сети управления (Out-of-Band).

Коммутаторы в каждой точке установки объединяются в одно логическое устройство посредством технологии стекирования, таким образом обеспечивая отказоустойчивость подключения конечных устройств СОИБ и сетевых устройств между собой.

Выход их строя одного из участников коммутаторов стека, каждого из сегментов СОИБ приводит только к деградации пропускной способности, но не к полной изоляции сегмента.

Активное сетевое оборудование СОИБ размещается в шкафу СОИБ Аппаратной.

Подключение активного сетевого оборудования к электропитанию выполняется по схеме с резервированием, каждый участник стека коммутаторов подключается в отдельный ввод, для обеспечения должного уровня отказоустойчивости. При наличии двух блоков питания на коммутаторах – каждый из блоков питания так же подключается в отдельный ввод.

Описание принципов сегментирования сети, прохождения и изоляции трафика как внутри сегментов, так и между остальными, описан в разделе 4.2.6.

4.3.1.2 Принципы функционирования сегмента сети СОИБ

Сегмент сети СИОБ состоит из двух коммутаторов 3 уровня модели OSI, обеспечивает подключение кластеров межсетевых экранов сегментов периметра АСУ и ЛСУ, серверного оборудования и оборудования системы хранения данных, а также выполняет агрегацию и коммутацию трафика между устройствами внутри сегмента сети СОИБ.

Подключение коммутаторов сегмента сети СОИБ к кластерам межсетевых экранов сегментов периметра АСУ и ЛСУ выполняется по схеме с резервированием для обеспечения должного уровня отказоустойчивости. Каждый участник стека коммутаторов сегмента СОИБ подключается как минимум одной линией связи на скорости не менее 10 Гбит/с к каждому участнику кластера межсетевых экранов сегментов периметра АСУ и ЛСУ.

Подключение серверного оборудования и оборудования системы хранения данных к коммутаторам сегмента сети СОИБ выполняется по схеме с резервированием. Каждое устройство подключается как минимум двумя линиями связи на скорости не менее 10 Гбит/с, по одной от каждого участника логического стека. Линии связи собираются в одну логическую сущность посредством агрегации.

Модели коммутаторов сегмента сети СОИБ и тип интерфейса подключения определяются рабочей документацией / на момент проведения пуско-наладочных работ.

Взаимодействие коммутаторов сегмента сети СОИБ с кластерами межсетевых экранов, серверным оборудованием и оборудованием системы хранения данных осуществляется на втором (канальном) уровне модели OSI, обеспечивая изоляцию трафика внутри сегмента на уровне виртуальных локальных сетей (VLAN). Коммутаторы сегмента сети СОИБ ставят в соответствие определенному VLAN определенную виртуальную таблицу коммутации, тем самым обеспечивая логическую изоляцию трафика на канальном уровне.

Сеть хранения данных реализуется на коммутаторах сегмента сети СОИБ, обеспечивая полную связность всех подключенных к ней устройств. Сеть хранения данных строится на основе технологии Ethernet со скоростью передачи данных не менее 10 Гбит/с.

Кластер межсетевых экранов периметра АСУ рассматриваются как «шлюз по умолчанию» для подключения серверного оборудования и оборудованием системы хранения данных.

В роли коммутаторов сегмента сети СОИБ используются модели Huawei CloudEngine S6730-H24X6C-V2 высотой 1U и глубиной 420 мм. Каждый коммутатор обеспечивает до 24-х подключений на скорости 10 Гбит/с через порты стандарта SFP+ и до 6-и подключений на скорости 40 Гбит/с (100 Гбит/с при наличии дополнительной лицензии) через порты стандарта QSFP+. Порты стандарта SFP+ имеют обратную совместимость со стандартом SFP, что позволяет подключать так же и оборудование на скорости 1 Гбит/с. Коммутаторы имеют 2 модульных блока питания мощностью 600 Вт каждый и 4 модульных вентилятора системы охлаждения, что обеспечивает должный уровень резервирования. Коммутаторы поддерживают работу на 3 уровне модели OSI и поддерживают все основные протоколы маршрутизации. Коммутаторы стекируются между собой по технологии iStack через Ethernet порты. Коммутаторы поставляются с кабелями питания под разъемы C13-C14.

4.3.1.3 Принципы функционирования ядра периметра АСУ

Ядро периметра АСУ состоит из двух коммутаторов 3 уровня модели OSI, обеспечивает подключение кластера межсетевых экранов сегмента периметра АСУ и оборудования локальной сети периметра АСУ, а также выполняет агрегацию и коммутацию трафика между устройствами внутри периметра АСУ.

Подключение коммутаторов ядра периметра АСУ к кластеру межсетевых экранов сегмента периметра АСУ выполняется по схеме с резервированием для обеспечения должного уровня отказоустойчивости. Каждый участник стека коммутаторов периметра АСУ подключается как минимум одной линией связи на скорости не менее 10 Гбит/с к каждому участнику кластера межсетевых экранов сегмента периметра АСУ.

Подключение коммутаторов ядра периметра АСУ к локальной сети АСУ выполняется по схеме с резервированием для обеспечения должного уровня отказоустойчивости. Каждый участник стека коммутаторов периметра АСУ подключается как минимум одной линией связи к коммутаторам локальной сети АСУ.

Модели коммутаторов ядра периметра АСУ и тип интерфейса подключения определяются рабочей документацией / на момент проведения пуско-наладочных работ.

Взаимодействие коммутаторов периметра АСУ с кластером межсетевых экранов периметра АСУ и активным сетевым оборудованием локальной сети осуществляется на втором (канальном) уровне модели OSI, обеспечивая изоляцию трафика внутри сегмента на уровне виртуальных локальных сетей (VLAN). Коммутаторы ядра периметра АСУ ставят в соответствие определенному VLAN определенную виртуальную таблицу коммутации, тем самым обеспечивая логическую изоляцию трафика на канальном уровне.

Кластер межсетевых экранов периметра АСУ рассматриваются как «шлюз по умолчанию» для подключенного активного сетевого оборудования периметра АСУ.

В роли коммутаторов сегмента сети АСУ используются модели Huawei CloudEngine S6730-H24X6C-V2 высотой 1U и глубиной 420 мм. Каждый коммутатор обеспечивает до 24-х подключений на скорости 10 Гбит/с через порты стандарта SFP+ и до 6-и подключений на скорости 40 Гбит/с (100 Гбит/с при наличии дополнительной лицензии) через порты стандарта QSFP+. Порты стандарта SFP+ имеют обратную совместимость со стандартом SFP, что позволяет подключать так же и оборудование на скорости 1 Гбит/с. Коммутаторы имеют 2 модульных блока питания мощностью 600 Вт каждый и 4 модульных вентилятора системы охлаждения, что обеспечивает должный уровень резервирования. Коммутаторы поддерживают работу на 3 уровне модели OSI и поддерживают все основные протоколы маршрутизации. Коммутаторы стекируются между собой по технологии iStack через Ethernet порты. Коммутаторы поставляются с кабелями питания под разъемы C13-C14.

4.3.1.4 Принципы функционирования ядра периметра ЛСУ

Ядро периметра ЛСУ состоит из двух коммутаторов 3 уровня модели OSI, обеспечивает подключение кластера межсетевых экранов сегмента периметра ЛСУ и оборудования существующей локальной сети периметра ЛСУ, а также выполняет агрегацию и коммутацию трафика между устройствами внутри периметра ЛСУ.

Подключение коммутаторов ядра периметра ЛСУ к кластеру межсетевых экранов сегмента периметра ЛСУ выполняется по схеме с резервированием для обеспечения должного уровня отказоустойчивости. Каждый участник стека коммутаторов периметра ЛСУ подключается как минимум одной линией связи на скорости не менее 10 Гбит/с к каждому участнику кластера межсетевых экранов сегмента периметра АСУ.

Подключение коммутаторов ядра периметра ЛСУ к локальной сети ЛСУ выполняется по схеме с резервированием для обеспечения должного уровня отказоустойчивости. Каждый участник стека коммутаторов периметра ЛСУ подключается как минимум одной линией связи к коммутаторам существующей локальной сети.

Модели коммутаторов ядра периметра ЛСУ и тип интерфейса подключения определяются рабочей документацией / на момент проведения пуско-наладочных работ.

Взаимодействие коммутаторов периметра ЛСУ с кластером межсетевых экранов периметра ЛСУ и активным сетевым оборудованием сегмента ЛСУ на втором (канальном) уровне модели OSI, обеспечивая изоляцию трафика внутри сегмента на уровне виртуальных локальных сетей (VLAN). Коммутаторы ядра периметра ЛСУ ставят в соответствие определенному VLAN определенную виртуальную таблицу коммутации, тем самым обеспечивая логическую изоляцию трафика на канальном уровне.

Для подключения портов управления оборудованием ЛСУ Modbus используются коммутаторы периметра ЛСУ в рамках отдельно выделенной виртуальной локальной сети (VLAN). В случае невозможности обеспечения требуемой скорости отклика между ЛСУ и ИСУБ допускается прямое подключение ЛСУ.

Кластер межсетевых экранов периметра ЛСУ рассматриваются как «шлюз по умолчанию» для подключенного активного сетевого оборудования периметра ЛСУ.

В роли коммутаторов сегмента сети ЛСУ используются модели Huawei CloudEngine S6730-H24X6C-V2 высотой 1U и глубиной 420 мм. Каждый коммутатор обеспечивает до 24-х подключений на скорости 10 Гбит/с через порты стандарта SFP+ и до 6-и подключений на скорости 40 Гбит/с (100 Гбит/с при наличии дополнительной лицензии) через порты стандарта QSFP+. Порты стандарта SFP+ имеют обратную совместимость со стандартом SFP, что позволяет подключать так же и оборудование на скорости 1 Гбит/с. Коммутаторы имеют 2 модульных блока питания мощностью 600 Вт каждый и 4 модульных вентилятора системы охлаждения, что обеспечивает должный уровень резервирования. Коммутаторы поддерживают работу на 3 уровне модели OSI и поддерживают все основные протоколы маршрутизации. Коммутаторы стекируются между собой по технологии iStack через Ethernet порты. Коммутаторы поставляются с кабелями питания под разъемы C13-C14.

4.3.1.5 Принципы функционирования сети управления Out-of-Band

Для подключения выделенных портов управления активного сетевого оборудования и выделенных портов управления серверного и оборудования системы хранения данных используется выделенный коммутатор Out-of-Band.

Коммутатор сети управления Out-of-Band подключается к существующей сети управления Out-of-Band предприятия посредством как минимум двух линий связи для обеспечения резервирования.

Выделенная сеть управления Out-of-Band используется в случае отказа основной сети управления оборудованием периметра СОИБ, АСУ и ЛСУ.

В роли коммутатора сегмента сети управления Out-of-Band используется модель Huawei CloudEngine S5735-S24T4X высотой 1U и глубиной 420 мм. Коммутатор обеспечивает до 24-х подключений на скорости 1 Гбит/с через порты стандарта 1000BASE-T и до 4-х подключений на скорости 10 Гбит/с через порты стандарта SFP+. Порты стандарта SFP+ имеют обратную совместимость со стандартом SFP, что позволяет подключать так же и оборудование на скорости 1 Гбит/с. Коммутатор имеет 2 модульных блока питания мощностью 180 Вт каждый и 1 модуль вентилятора системы охлаждения, что обеспечивает должный уровень резервирования. Коммутатор поддерживают работу на 3 уровне модели OSI и поддерживает все основные протоколы маршрутизации. Коммутатор поддерживает стекирование по

технологии iStack через Ethernet порты. Коммутатор поставляется с кабелями питания под разъемы C13-C14.

4.3.2 Контроллер домена

Контроллер домена обеспечивает возможность функционирования служб каталога пользователей и серверов с требуемым уровнем отказоустойчивости. Отказоустойчивость обеспечивается использованием встроенных средств резервирования на уровне контроллера домена.

Контроллер домена используется для управления учетными записями и политиками АРМ и серверов СОИБ и ИСУБ. Использование корпоративного домена sibur.local не допускается.

Используются базовые политики безопасности, расширяемые с использованием функционала Комплекса средств защиты от несанкционированного доступа. Состав базового набора политик представлен в таблице 3.2.

Таблица 3.2 – Состав базового набора политик контроллера домена

Параметр	Значение
Парольные политики	
Enforce password history	24 passwords remembered
Maximum password age	45 days
Minimum password age	0 days
Minimum password length	12 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Политики Kerberos	
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes
Audit Policy	
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit policy change	Success, Failure
Accounts	
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Audit	
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
Network Access	

Параметр	Значение
Network access: Allow anonymous SID/Name translation	Disabled
Network Security	
Network security: Do not store LAN Manager hash value on next password change	Disabled
Network security: Force logoff when logon hours expire	Disabled

Контроллер домена также выполняет функции NTP-сервера, используемого для синхронизации системного времени компонентов СОИБ.

Подключение АРМ и серверов СОИБ и ИСУБ, работающих под управлением ОС Linux, осуществляется с использованием рекомендуемого производителем соответствующей версии ядра, инструментария. Для ОС Astra Linux, рекомендуемым инструментом является SSSD.

Контроллер домена устанавливается на выделенном виртуальном сервере СОИБ, Сегмент инфраструктурных сервисов СОИБ (титул 2201).

4.3.3 Система виртуализации

Система виртуализации обеспечивает централизованное управление всеми аппаратными серверами, виртуальными машинами, хранилищами виртуальных машин и сетевой инфраструктурой виртуализации из единой консоли управления.

Система виртуализации обеспечивает отказоустойчивое функционирование виртуальных машин, за счет объединения серверов виртуализации в кластер и перезапуск виртуальных машин на ресурсах кластера в случае выхода из строя одного из аппаратных серверов виртуализации.

Система виртуализации строится на базе решения zVirt Max, обеспечивающим следующий функционал:

– перемещение виртуальных машин между серверами без выключения ОС виртуальной машины;

– автоматический перезапуск виртуальных машин на других физических серверах виртуализации, находящихся в одном кластере, в случае выхода из строя сервера, на котором они функционировали;

– проброс на виртуальные машины USB-устройств физического сервера, при необходимости;

– клонирование виртуальных машин без необходимости их выключения;

– динамическое добавление ресурсов: RAM, vCPU, дискового пространства, без остановки виртуальной машины;

– создание мгновенных снимков состояния виртуальных машин с возможностью возврата к ним;

– автоматическая балансировка нагрузки по CPU и RAM в рамках кластера высокой доступности;

– централизованная настройка сетевых компонентов на хостах виртуализации;

– присвоение IP-адресов с момента создания виртуального интерфейса – как при создании ВМ, так и при изменении конфигурации;

– экспорт списка виртуальных машин, хостов виртуализации, доменов хранения, пулов, событий в CSV формат через единый графический веб-интерфейс администратора системы;

– безагентское резервное копирование средствами Комплекса резервного копирования информационных ресурсов, ПО Кибер Бэкап.

Система виртуализация используется для размещения серверных компонентов СОИБ:

– сервер безопасности наложенных средств защиты Комплекса средств защиты от несанкционированного доступа;

– сервер управления решением Комплекса антивирусной защиты;

– SIEM-коллектор Комплекса сбора, анализа и корреляции событий безопасности;

– сервер управления решением Комплекса резервного копирования информационных ресурсов;

– файловый сервер;

– сервер обновления операционных систем;

– сервер централизованного управления МСЭ;

– сервер управления решением единого программного обеспечения Комплекса централизованного управления доступом к активному сетевому оборудованию и Комплекса контроля конфигураций;

– сервер Комплекса анализа защищенности инфраструктуры;

– контроллер домена.

Предварительные требования к вычислительным ресурсам для размещения виртуальных машин представлены в таблице 3.3.

Таблица 3.3 – Предварительные требования к вычислительным ресурсам для размещения виртуальных машин СОИБ

Сервер	Параметр	Значение
Комплекс средств защиты от несанкционированного доступа		
Сервер безопасности	OS	Windows Server 2022; Windows Server 2019; Windows Server 2016; Windows Server 2012 R2 Rollup Update
	vCPU	4
	RAM	16 ГБ
	SSD	150 ГБ
	NIC	1 × 100 Мбит/сек
Комплекс антивирусной защиты		

Сервер	Параметр	Значение
Сервер управления решением	OS	Debian GNU/Linux 12 (Bookworm) 64-разрядная; Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная; CentOS 7.x 64-разрядная; CentOS Stream 9 64-разрядная; Red Hat Enterprise Linux Server 9.x 64-разрядная; SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная; Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная; Альт СП Сервер 10 64-разрядная; Альт Сервер 10 64-разрядная; Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная; РЕД ОС 7.3 Сервер 64-разрядная; РЕД ОС 7.3 Сертифицированная редакция 64-разрядная; РОСА "КОБАЛЬТ" 7.9 64-разрядная
	vCPU	4
	RAM	4 ГБ
	SSD	100 ГБ
	NIC	1 × 100 Мбит/сек
Комплекса сбора, анализа и корреляции событий безопасности		
SIEM-коллектор	OS	Astra Linux Special Edition; РУСБ.10015-01 (2022-1110SE17 оперативное обновление 1.7.3)
	CPU	8
	RAM	16 ГБ
	SSD	500 ГБ
	NIC	1 * 100 Мбит/сек
Windows Agent	OS	Microsoft Windows Server 2012 Standard; Microsoft Windows Server 2012 R2 Standard; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2019 Standard; Microsoft Windows Server 2022 Standard
	CPU	8
	RAM	16 ГБ

Сервер	Параметр	Значение
	SSD	100 ГБ
	NIC	1 × 100 Мбит/сек
Комплекса резервного копирования информационных ресурсов		
Сервер управления СРК	OS	Microsoft Windows Server 2012 Standard; Microsoft Windows Server 2012 R2 Standard; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2019 Standard; Microsoft Windows Server 2022 Standard Astra Linux Special Edition 1.7.0, 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5, 1.8 Альт Сервер 10 Альт 8 СП РЕД ОС 7.3, 8 РОСА «КОБАЛЬТ» 7.9
	CPU	4
	RAM	32
	SSD	100
	NIC	1 × 1 Гбит/с
Агент резервного копирования	OS	Linux
	CPU	4
	RAM	8 ГБ
	SSD	50 ГБ
	NIC	1 × 10 Гбит/с
Комплекс управления обновлениями программного обеспечения		
Файловый сервер	OS	Microsoft Windows Server 2012 Standard; Microsoft Windows Server 2012 R2 Standard; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2019 Standard; Microsoft Windows Server 2022 Standard
	CPU	4
	RAM	4 ГБ
	SSD	200 ГБ
	NIC	1 × Гбит/с

Сервер	Параметр	Значение
Сервер обновления операционных систем Windows	OS	Microsoft Windows Server 2012 Standard; Microsoft Windows Server 2012 R2 Standard; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2019 Standard; Microsoft Windows Server 2022 Standard
	CPU	2
	RAM	4 ГБ
	SSD	500 ГБ
	NIC	1 × 100 Мбит/сек
Сервер обновления операционных систем Linux	OS	Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8); Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7), РУСБ.10015-10; Astra Linux Special Edition РУСБ.10015-17; Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7); Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6); Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7); Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6); Astra Linux Special Edition РУСБ.10015-16 исп. 1; Astra Linux Special Edition РУСБ.10015-16 исп. 2; Astra Linux Special Edition РУСБ.10265-01 (очередное обновление 8.1); Astra Linux Common Edition 2.12
	CPU	2
	RAM	4 ГБ
	SSD	500 ГБ
	NIC	1 × 100 Мбит/сек
Комплекс обеспечения сетевой безопасности		
Сервер централизованного управления МСЭ	OS	Virtual Appliance
	CPU	4
	RAM	8 ГБ
	SSD	350 ГБ
	NIC	2 × 1 Гбит/сек

Сервер	Параметр	Значение
Комплекс централизованного управления доступом к активному сетевому оборудованию и Комплекс контроля конфигураций		
Сервер управления решением	OS	Astra Linux Special Edition; РЕД ОС 7.3
	CPU	12
	RAM	16 ГБ
	SSD	600 ГБ
	NIC	1 × 100 Мбит/сек
Комплекс анализа защищенности инфраструктуры		
Сервер	OS	Microsoft Windows Server 2012 Standard; Microsoft Windows Server 2012 R2 Standard; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2019 Standard; Microsoft Windows Server 2022 Standard
	CPU	4
	RAM	10 ГБ
	SSD	300 ГБ
	NIC	1 × Гбит/сек
Инфраструктурные сервисы СОИБ		
Контроллер домена	OS	Microsoft Windows Server 2012 Standard; Microsoft Windows Server 2012 R2 Standard; Microsoft Windows Server 2016 Standard; Microsoft Windows Server 2019 Standard; Microsoft Windows Server 2022 Standard
	CPU	2
	RAM	4 ГБ
	SSD	100 ГБ
	NIC	1 × 100 Мбит/сек

На базе встроенных механизмов Системы виртуализации, осуществляются функции обеспечения информационной безопасности в среде виртуализации, перечисленные в пункте 4.2.7.

4.3.4 Серверное оборудование

В данном проекте используется 3 физических сервера, имеющих идентичную аппаратную конфигурацию и входят в состав единого кластера под управлением платформы виртуализации и один физический сервер для организации хранения и обработки резервных копий – узел хранения.

Для построения платформы виртуализации используются серверы СИЛА СР1-6326 высотой 1U со следующими параметрами:

а) два процессора 6326, 16 ядер каждый, частота 2,9 ГГц;

б) память 128 ГБ;

в) два SSD диска по 480 ГБ, имеющихся в сервере под установку ОС объединены в RAID1 для повышения отказоустойчивости;

г) сетевые интерфейсы:

1) один порт 1 Гб/с RJ-45 для удаленного мониторинга и управлением физическим состоянием сервера. Управление сервером осуществляется по протоколу HTTPS;

2) двухпортовая сетевая карта 10 Гб/с SFP+ в количестве одной шт. Используется для организации сетевого взаимодействия хостов виртуализации, ВМ, сети управления платформы виртуализацией.

   Для обеспечения отказоустойчивости и увеличения пропускной способности данные порты объединяются на стороне ОС сервера в NIC Teaming, а на стороне коммутаторов в LACP. Требуемые подсети подаются через TRUNK;

3) двухпортовая сетевая карта 10 Гб/с SFP+ в количестве одной шт.

   Используется для подключения к сети по протоколу iSCSI. Порты, используемые для iSCSI, не могут использоваться для прочего сетевого взаимодействия, кроме передачи данных из сети хранения. На портах со стороны коммутатора отключается маршрутизация и подаются необходимые подсети через TRUNK;

д) четыре коротковолновых трансивера SFP+ с пропускной способностью 10 Гб/с;

е) RAID контроллер 2ГБ кэш памяти;

ж) два блока питания;

з) кабели необходимые для подключения питания и сети передачи данных.

Для организации хранения и обработки резервных копий используется сервер СИЛА СР2-6327 высотой 2U со следующими параметрами:

а) один процессор 4310, 12 ядер, частота 2,1 ГГц;

б) память 64 ГБ;

в) два SSD диска по 480 ГБ, имеющихся в сервере под установку ОС объединены в RAID1 для повышения отказоустойчивости;

г) шесть HDD дисков по 8 ТБ, имеющихся в сервере для организации хранилища резервных копий;

д) сетевые интерфейсы:

1) один порт 1 Гб/с RJ-45 для удаленного мониторинга и управлением физическим состоянием сервера. Управление сервером осуществляется по протоколу HTTPS;

2) двухпортовая сетевая карта 10 Гб/с SFP+ в количестве одной шт.

   Используется для организации сетевого взаимодействия хостов виртуализации, ВМ, сети управления платформы виртуализацией.

Для обеспечения отказоустойчивости и увеличения пропускной способности данные порты объединяются на стороне ОС сервера в NIC Teaming, а на стороне коммутаторов в LACP. Требуемые подсети подаются через TRUNK;

е) два коротковолновых трансивера SFP+ с пропускной способностью 10 Гб/с;

ж) RAID контроллер 2ГБ кэш памяти;

з) два блока питания;

и) кабели необходимые для подключения питания и сети передачи данных.

4.3.5 Система хранения данных

В данном проекте используется СХД Dell PowerVault ME5024 высотой 2U с двумя контроллерами для организации отказоустойчивого хранения данных.

Дисковая подсистема СХД состоит из SSD накопителей в количестве шесть штук, объемом 1,92TB каждый, и объединенных в RAID5 для достижения наибольшей производительности, и отказоустойчивости систем. Один диск 1,92 ТБ используется в качестве горячей замены. Для организации хранения данных и доступа к ним используется классическая СХД с блочным уровнем доступа по протоколу iSCSI.

Каждый контроллер имеет, входящий в состав СХД имеет следующие сетевые интерфейсы:

- два 10 Гб/с порта SFP+ для подключения к сети передачи данных;
- один порт 1 Гб/с RJ-45 для удаленного мониторинга и управления СХД.

Управление СХД осуществляется по протоколу HTTP(s)/SSH.

Расчёт необходимых физических дисковых ресурсов был выполнен на основе Таблицы 3.3. Предварительные требования к вычислительным ресурсам для размещения виртуальных машин СОИБ. В ходе расчётов были получены требования в 3400 ГБ, а также учтён запас с учётом потенциального роста.

Система хранения данных обеспечивает реализацию следующего функционала:

- Thin Provisioning («Тонкое» выделение ресурсов) – распределение и использование физической емкости хранилища в пулах дисков по мере необходимости;

- SSD Read Cache – прирост в скорости выполнения приложений путем кэширования ранее считанных данных;

- Remote Replication (Удаленная репилкация) – репликация данных, в том числе зеркалирование «тонко» выделенных пулов;

- Volume Copy – полное клонирование тома, обеспечивает беспрерывное перемещение томов, резервное копирование и восстановление на базе дисков;

- Snapshots – восстановление файлов после случайного удаления или изменения с помощью копии данных на определенный момент времени.

4.3.6 Инженерные системы

Серверы и телекоммуникационное оборудование располагается в отдельном запираемом телекоммуникационном шкафу СОИБ, исключающим бесконтрольный доступ в отдельном помещении (Аппаратной, титул 2201), в котором обеспечивается необходимая степень климатической защиты от воздействия внешней среды.

Для защиты аппаратуры от бросков напряжения и коммутационных помех в общих электросетях применяются источники бесперебойного питания с двойным преобразованием, (онлайн-ИБП) в отказоустойчивой конфигурации.

Все оборудование с двумя блоками питания подключается к двум отдельным устройствам распределения электропитания (PDU), питание на которые подается от двух разных ИБП.

Все оборудование с одним блоком питания подключается к устройствам автоматического ввода резерва (ATS), питание на которые подается от двух разных ИБП.

Выход из строя ИБП не влияет на функционирование подсистем СОИБ. Каждый из ИБП рассчитан на 100% обеспечение питания подключенных к нему компонентов.

Размещаемое в шкафу СОИБ оборудование и его характеристики представлены в таблице 4.3.

Таблица 4.3 – Характеристики размещаемого в шкафу СОИБ оборудования

Компонент СОИБ	Производитель	Модель устройства	Размер в юнитах	Габаритные размеры (ШхГхВ), мм	Энергопотребление, Вт
МСЭ периметра АСУ	InfoWatch ARMA IF	2 * ARMA-19RACK-10G	2 * 1U	482x762x43,4	2 * 2 * 650
МСЭ периметра ЛСУ	InfoWatch ARMA IF	2 * ARMA-19RACK-10G	2 * 1U	482x762x43,4	2 * 2 * 650
Коммутаторы сегмента СОИБ	Huawei CloudEngine	2 * S6730-H24X6C-V2	2 * 1U	442x420x43.6	2 * 1200
Коммутаторы ядра периметра АСУ	Huawei CloudEngine	2 * S6730-H24X6C-V2	2 * 1U	442x420x43.6	2 * 600
Коммутаторы ядра периметра ЛСУ	Huawei CloudEngine	2 * S6730-H24X6C-V2	2 * 1U	442x420x43.6	2 * 600
Менеджмент коммутатор	Huawei CloudEngine	S5735-S24T4X	1U	442x420x43.6	2 * 180
Кластер серверов	СИЛА	СР1-6326	3 * 1U	433.4x748x43.6	3 * 2 * 1200
Узел хранения	СИЛА	СР2-6327	2U	433.4x748x87.6	2 * 1600
СХД	Dell PowerVault	ME5024	2U	483x547.8x8.79	2 * 580

В данном проекте оборудование устанавливается в шкаф Remer серии ШТК-М, размерами 800x1000мм и высотой 42U, черного цвета. Шкаф укомплектован всеми необходимы аксессуарами для монтажа оборудования. Активное оборудование подключается к двум устройствам распределения питания, установленным в шкафу – PDU 83401 (3ф, 16А) производства компании CyberPower. Каждое из устройств

распределения питания подключено к своему ИБП Huawei серии UPS2000-G мощностью 15 кВа, обеспечивающим не менее 15 минут автономии работы активного оборудования при полной нагрузке.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	–	автоматизированное рабочее место
ИБП	–	источник бесперебойного питания
МСЭ	–	межсетевой экран
ОС	–	операционная система
ПО	–	программное обеспечение
СЗИ	–	средство защиты информации
СХД	–	система хранения данных
AAA	–	описание процесса предоставления доступа и контроля над ним (Authentication, Authorization, Accounting)
DoS	–	атака типа «отказ в обслуживании» (Denial-of-service)
HDD	–	накопитель на жестких магнитных дисках (Hard disk drive)
HTTP/HTTPS	–	протокол передачи гипертекста, сетевой протокол прикладного уровня (HyperText Transfer Protocol)
iSCSI	–	протокол для установления взаимодействия и управления системами хранения данных (Internet Small Computer System Interface)
LACP	–	технология объединения нескольких параллельных каналов передачи данных в сетях Ethernet, агрегирование каналов (Link aggregation control protocol)
LDAP	–	протокол доступа к каталогам (Lightweight Directory Access Protocol)
Modbus	–	открытый коммуникационный протокол, основанный на архитектуре ведущий-ведомый
NTP	–	протокол сетевого времени (Network Time Protocol)
OPC	–	семейство программных технологий, обеспечивающих единый интерфейс для управления объектами автоматизации и технологическими процессами (Open Platform Communications)
OSI	–	сетевая модель стека сетевых протоколов OSI/ISO (Open Systems Interconnection model)
RAID	–	технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности (Redundant Array of Independent Disks)
SFP+	–	промышленный стандарт модульных компактных приёмопередатчиков (трансиверов), используемых для передачи данных в телекоммуникациях (Enhanced Small Form-factor Pluggable)

SIEM	–	класс программных продуктов, предназначенных для сбора и анализа событий безопасности (Security Information and Event Management)
SSD	–	твердотельный накопитель (Solid-State Drive)
SSH	–	сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (Secure Shell)
TACACS+	–	сеансовый протокол (Terminal Access Controller Access Control System plus)
TCP/IP	–	набор сетевых протоколов передачи данных, используемых в сетях, включая сеть интернет (Transmission Control Protocol and Internet Protocol)

ПЕРЕЧЕНЬ НОРМАТИВНОЙ ДОКУМЕНТАЦИИ

СОИБ соответствует действующему законодательству РФ и руководящим документам регулятора в области обеспечения информационной безопасности, а именно:

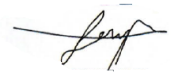
– Федеральный закон Российской Федерации от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;

– Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

– Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

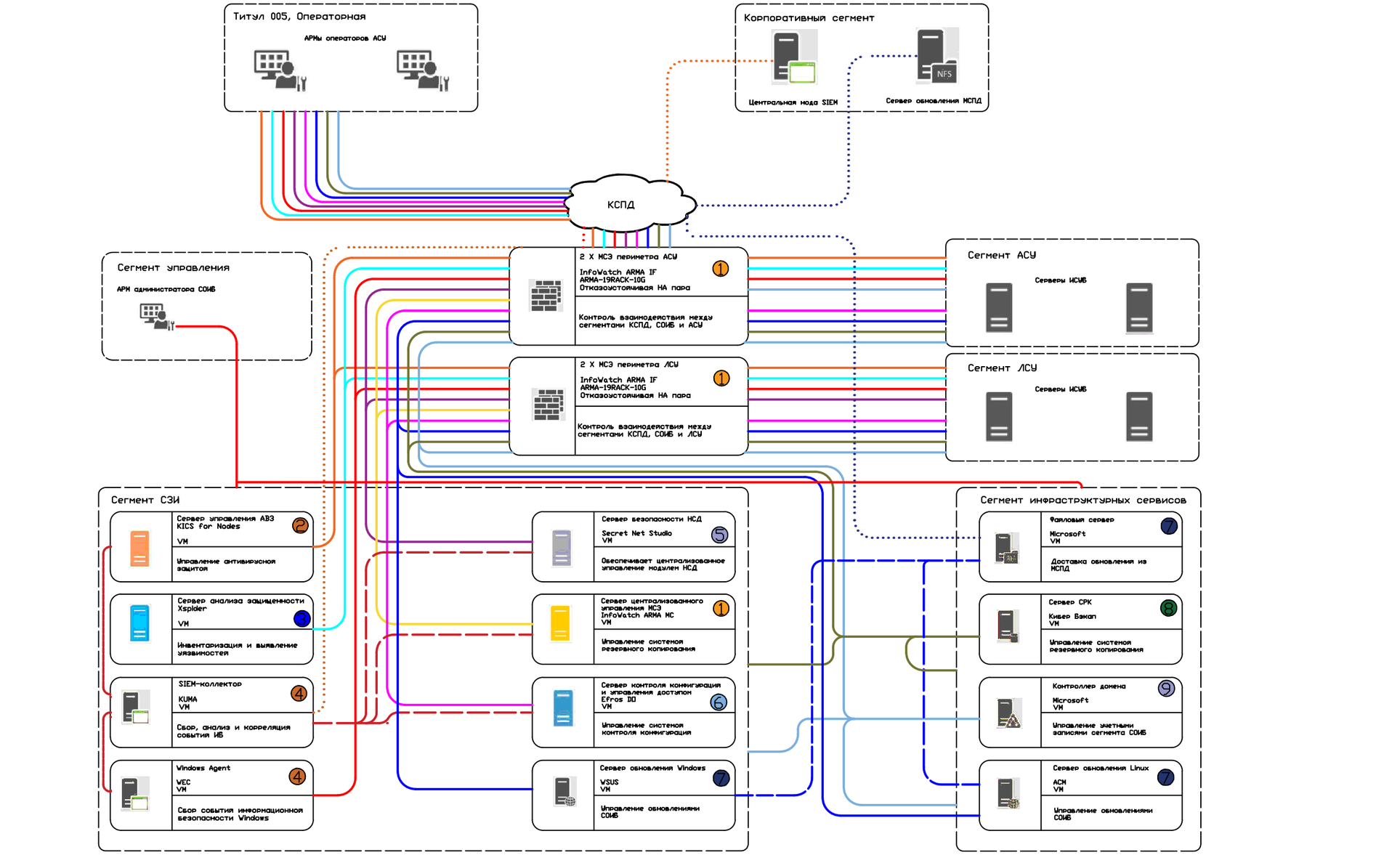
СПИСОК ИСПОЛНИТЕЛЕЙ

Выполненный раздел текстовой части	Отдел, должность, И.О. Фамилия	Подпись Дата
Раздел 1; 2 п. 3.1; 3.2; 3.2.1; 3.2.2; 3.2.4; 3.2.6; 3.2.7; 3.2.11	Департамент информационной безопасности Группа комплексных систем защиты информации Системный архитектор, Зац Константин Александрович	 11.10.2024
п. 3.2.3; 3.2.8; 3.2.10	Департамент информационной безопасности Группа комплексных систем защиты информации Системный архитектор, Турков Антон Сергеевич	 11.10.2024
п. 3.2.5; 3.3.3; 3.3.4; 3.3.5	Департамент комплексных решений Отдел инфраструктурного программного обеспечения Ведущий системный архитектор, Чуркин Сергей Валерьевич	 11.10.2024
п. 3.2.9; 3.3.2	Департамент комплексных решений Отдел инфраструктурного программного обеспечения Ведущий системный архитектор, Шацкий Дмитрий Анатольевич	 11.10.2024
3.3.1	Департамент комплексных решений Отдел сетей передачи данных и коммуникационных систем Системный архитектор, Сапрыкин Дмитрий Владимирович	 11.10.2024

Выполненный раздел текстовой части	Отдел, должность, И.О. Фамилия	Подпись Дата
3.3.6	Департамент комплексных решений Отдел инженерной инфраструктуры Системный архитектор, Сасковец Владимир Сергеевич	11.10.2024

Таблица регистрации изменений

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



Изм.	Кол.уч.	Лист	№док.	Подпись	Дата
Разраб.		Турков А.			11.10.2024
Н. контр.		Чекалёв Н.			11.10.2024
ГИП		Зац К.			11.10.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С2

Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

Стадия	Лист	Листов
П		1

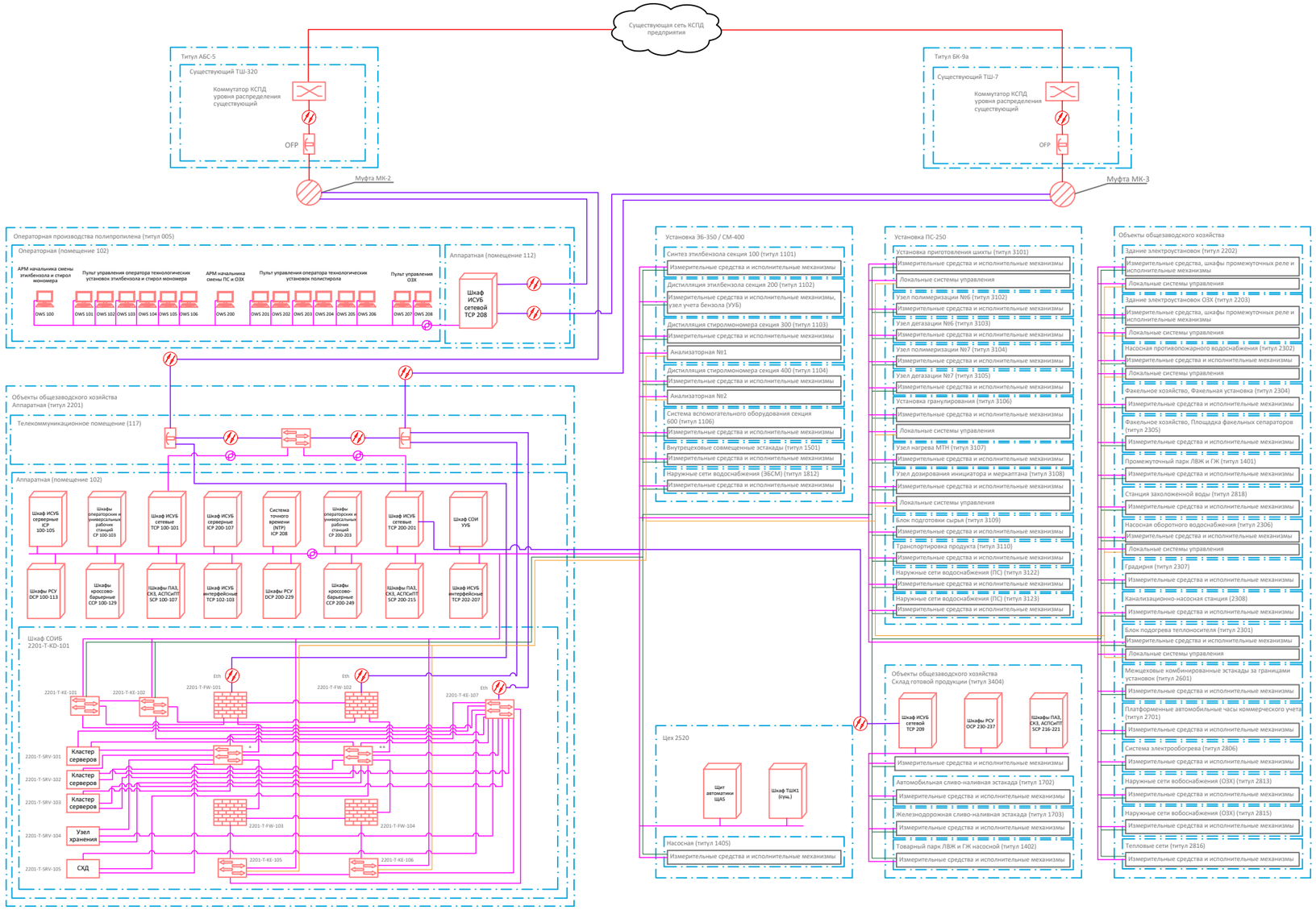
Схема функциональной структуры

Платформикс

Взам. инв. №

Подп. и дата

Инв. № подл.



Оборудование	Идентификатор
МСЭ периметра АСУ (устройство 1)	2201-T-FW-101
МСЭ периметра АСУ (устройство 2)	2201-T-FW-102
МСЭ периметра ЛСУ (устройство 1)	2201-T-FW-103
МСЭ периметра ЛСУ (устройство 2)	2201-T-FW-104
Коммутаторы ядра периметра АСУ (устройство 1)	2201-T-KE-101
Коммутаторы ядра периметра АСУ (устройство 2)	2201-T-KE-102
Коммутаторы сегмента СОИБ (устройство 1)	2201-T-KE-103
Коммутаторы сегмента СОИБ (устройство 2)	2201-T-KE-104
Коммутаторы ядра периметра ЛСУ (устройство 1)	2201-T-KE-105
Коммутаторы ядра периметра ЛСУ (устройство 2)	2201-T-KE-106
Менеджмент коммутатор	2201-T-KE-107
Кластер серверов (устройство 1)	2201-T-SRV-101
Кластер серверов (устройство 2)	2201-T-SRV-102
Кластер серверов (устройство 3)	2201-T-SRV-103
Устройство хранения	2201-T-SRV-104
СХД	2201-T-SRV-105

Маркировка оборудования

0001.2024-1806-T-BF-001 - маркировка оборудования, где:

- порядковый номер оборудования
- код оборудования
- код системы
- номер титула
- номер договора

0001.2024-1806-T-BA-001 - полная маркировка оборудования

1806-T-BA-001 - сокращенная маркировка оборудования

Условные обозначения

- коммутатор Ethernet
- оптический кросс
- межсетевой экран
- оптическая кабельная муфта существующая
- Стек коммутаторов уровня распределения существующие
- АРМ
- Телекоммуникационный шкаф
- существующее,запроектированное по другим проектам оборудования и кабельные линии
- волоконно-оптическая кабельная линия
- кабель парной скрутки
- проектируемое оборудование и кабельные линии
- сегмент ЛСУ
- сегмент АСУ

Коды оборудования

KD - телекоммуникационный шкаф
OFP - оптический кросс
FW - устройство межсетевого экрана
KE - коммутатор сети передачи данных
SRV - сервер/СХД

Код системы

T - система связи

Принятые сокращения

ТШ - телефонный шкаф
Eth - Ethernet
АРМ - автоматизированное рабочее место
КСПД - корпоративная сеть передачи данных

Примечание

* 2201-T-KE-103
** 2201-T-KE-104

Изм.	Кол.уч.	Лист	N°док.	Подпись	Дата
Разраб.		Зац К.			11.10.2024
Н.Контр.		Чекалёв Е.			11.10.2024
ГИП		Зац К.			11.10.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С1

Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

Стадия	Лист	Листов
П		1

Структурная схема комплекса технических средств СОИБ

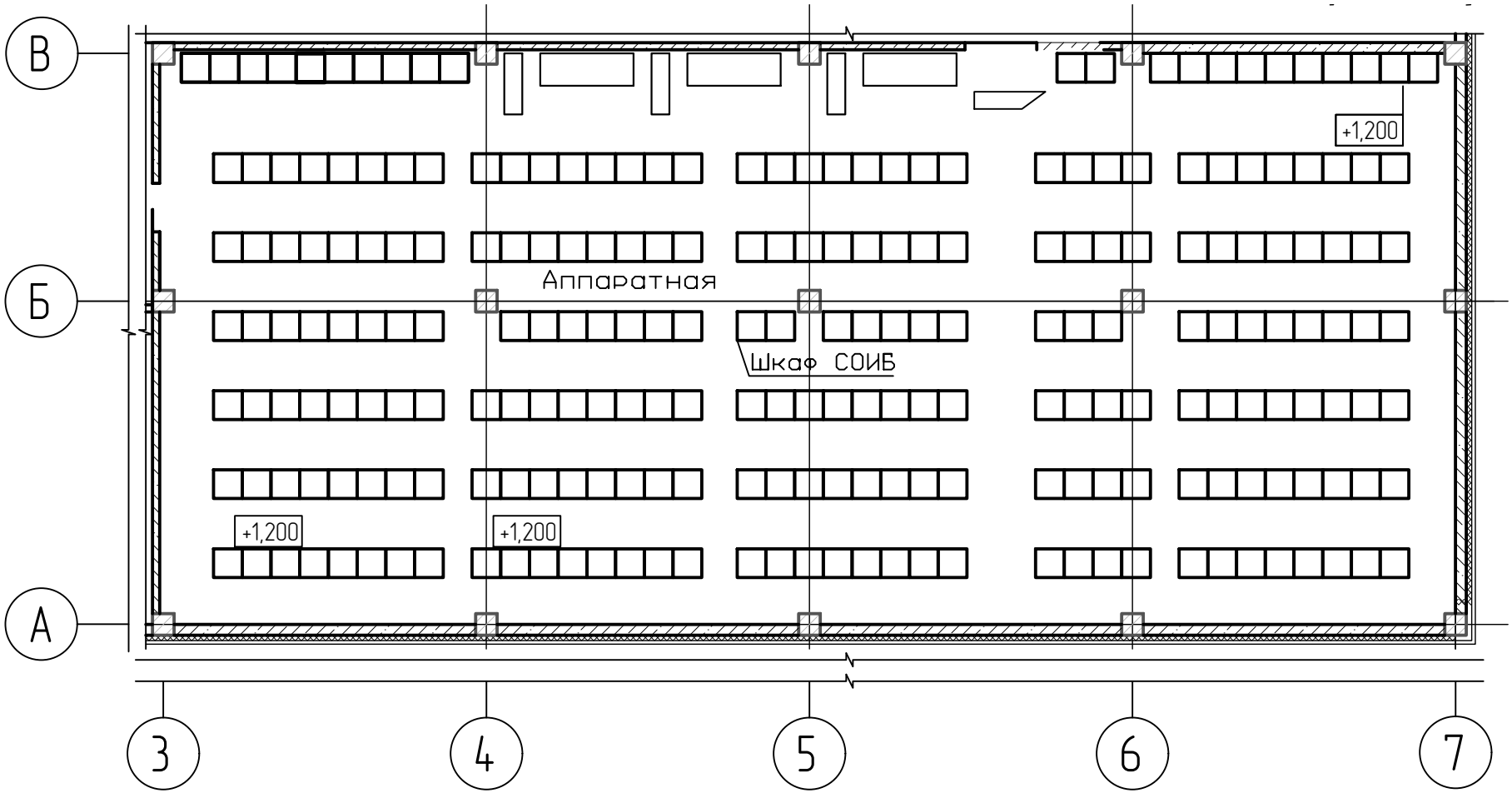
Платформикс

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С1_0_0_RU.dwg

Формат А3

Подл. и дата

Инв. N° подл.



Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№док.	Подпись	Дата
Разраб.		Зац К.			11.10.2024
Н. контр.		Чекалёв Е.			11.10.2024
ГИП		Зац К.			11.10.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С7

Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

Стадия	Лист	Листов
П		1

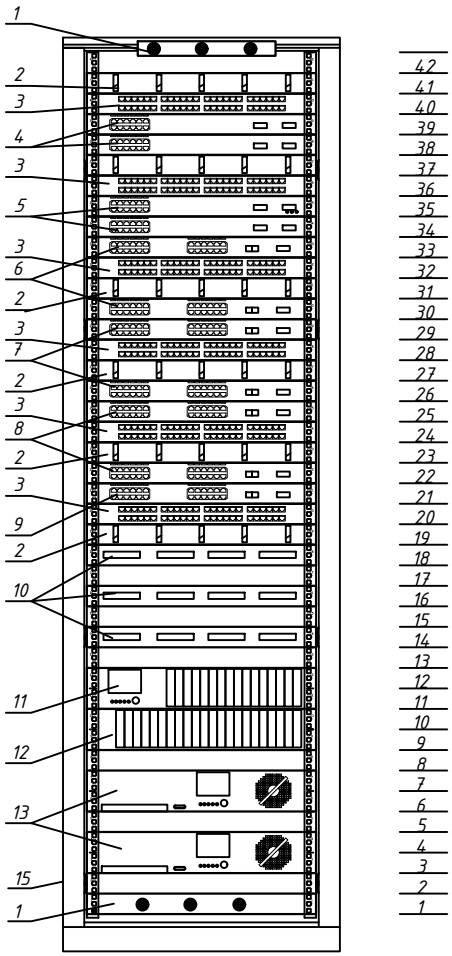
Схема расположения оборудования в Аппаратной

Платформикс

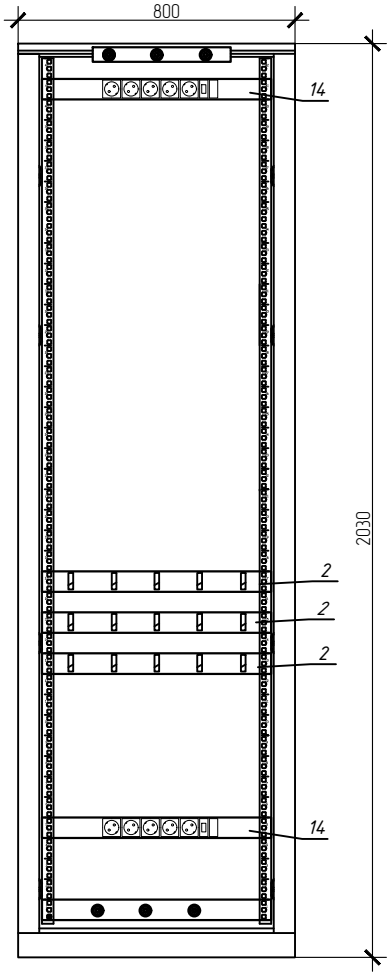
NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-С7_0_0_R.dwg

Формат А4

Фронтальный фасад



Задний фасад



Условные обозначения:

Поз.	Оборудование	Модель	Колл.
1	Блок вентиляторов	Уточнить в РД	2
2	Кабельный органайзер	Уточнить в РД	8
3	Патч-панель	Уточнить в РД	6
4	МСЭ периметра АСУ	InfoWatch ARMA IF ARMA-19RACK-10G	2
5	МСЭ периметра ЛСУ	InfoWatch ARMA IF ARMA-19RACK-10G	2
6	Коммутаторы сегмента СОИБ	Huawei CloudEngine S6730-H24X6C-V2	2
7	Коммутаторы ядра периметра АСУ	Huawei CloudEngine S6730-H24X6C-V2	2
8	Коммутаторы ядра периметра ЛСУ	Huawei CloudEngine S6730-H24X6C-V2	2
9	Менеджмент коммутатор	Huawei CloudEngine S5735-S24T4X	1
10	Кластер серверов	СИЛА СР1-6326	3
11	Узел хранения	СИЛА СР2-6327	1
12	СХД	Dell PowerVault ME5024	1
13	ИБП	Huawei UPS2000-G	2
14	Блок розеток	CyberPower PDU83401	2
15	Шкаф телекоммуникационный	Remer ШТК-М 800*1000*2030мм (ШхГхВ)	1

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	N°док.	Подпись	Дата
Разраб.		Яуров Л.			11.10.2024
Н. контр.		Чекалёв Е.			11.10.2024
ГИП		Зац К.			11.10.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-СА

«Строительство производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год», «Строительство производства полистирола мощностью 250 тыс. тонн в год и Строительство общезаводского хозяйства для производства полистирола мощностью 250 тыс. тонн в год и производства этилбензола мощностью 350 тыс. тонн в год и производства стирола мощностью 400 тыс. тонн в год»

Стадия	Лист	Листов
П		1

Чертежи установки технических средств

Платформикс

NKNH21002-ПС-ЭБСМ-ИОС5.4.1-0000-СА_0_0_RU.dwg

Формат А4