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 2. Производство этилбензола и стирола-мономера

NKNH21002-ПС-ЭБСМ-ИОС5.4.2

Том 5.5.4.2

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 2. Производство этилбензола и стирола-мономера

NKNH21002-ПС-ЭБСМ-ИОС5.4.2

Том 5.5.4.2

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

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

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 2. Производство этилбензола и стирола-мономера

NKNH21002-ПС-ЭБСМ-ИОС5.4.2

Том 5.5.4.2

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

Обозначение	Наименование	Примечание
NKNH21002-ПС-ЭБСМ-СП	Состав проектной документации	Выпускается отдельным томом 0
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-С	Содержание тома 5.5.4.2	Лист 2
	Раздел 5. Сведения об инженерном оборудовании, о сетях и системах инженерно-технического обеспечения	
	Подраздел 5. Сети связи	
	Часть 4. Информационная безопасность	
NKNH21002-ПС-ЭБСМ-ИОС5.4.2	Книга 2. Производство этилбензола и стирола-мономера	
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-В	Ведомость проекта	Лист 3

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.2-С		
Разраб.		Зац			12.09.24	Содержание тома	Стадия	Лист	Листов
							П		1
Н. контр.		Чекалёв			12.09.24		Платформикс		
ГИП		Зац			12.09.24				

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-ИОС5.4.2-В

2024

ВЕДОМОСТЬ ПРОЕКТА

Обозначение	Формат	Наименование	Приме-чание
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П1	А4	Концепция СОИБ	Лист 5
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П2	А4	Пояснительная записка по СОИБ	Лист 36
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-С2	А3	Схема функциональной структуры	Лист 86
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-С1	А3	Структурная схема комплекса технических средств СОИБ	Лист 87
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-С7	А4	Схема расположения оборудования в Аппаратной	Лист 88
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-СА	А4	Чертежи установки технических средств	Лист 89

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.2-В		
Разраб.		Зац			12.09.2024	Ведомость проекта	Стадия	Лист	Листов
							П		1
Н. контр.		Чекалёв			12.09.2024		Платформикс		
ГИП		Зац			12.09.2024				

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

Концепция СОИБ

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П1

2024

СОДЕРЖАНИЕ

Лист

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П1		
Разраб.		Зац			12.09.2024	Концепция СОИБ	Стадия	Лист	Листов
							П	1	30
Н. контр.		Чекалёв			12.09.2024		Платформикс		
ГИП		Зац			12.09.2024				

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 система 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.

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 проекта Раковым С.Г..

В данном томе представлена концепция технических решений СОИБ ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ.

Настоящая книга разработана 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 ЭБСМ и ПС250 и ОЗХ, как объекты управления, представляют собой технологический комплекс на площадке ПАО «Нижнекамскнефтехим».

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

ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ обеспечивают 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 ЭБСМ и ИСУБ ПС250 и ОЗХ представляют собой распределенные (по функциям и территориально), многофункциональные, информационно-измерительные и управляющие системы, построенные по иерархическому принципу, с использованием стандартных протоколов межуровневого обмена данными, способные к расширению интеграции с другими системами, а также с вышестоящим уровнем управления.

ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ, каждая, состоят 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 ЭБСМ и ИСУБ ПС250 и ОЗХ, каждая, взаимодействуют со следующими системами, не входящими в их состав:

– стационарной системой мониторинга динамического оборудования (ССМД);

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

– 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.

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 ЭБСМ и 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 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

3.1 Реализация требований по обеспечению информационной безопасности системы

ИСУБ ЭБСМ включает в свой состав автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (АСУ) и не являются значимыми объектами критической информационной инфраструктуры Российской Федерации. Согласно «Актам классификации АСУ», необходимо обеспечить требования по 3-му классу защищенности автоматизированных систем управления.

Базовый набор мер защиты информации, подлежащий реализации в рамках СОИБ, а также описание порядка реализации представлены 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	Регламентация правил и процедур 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; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.2	Идентификация и аутентификация устройств	Функционал Комплекса средств защиты от несанкционированного доступа
ИАФ.3	Управление идентификаторами	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.4	Управление средствами аутентификации	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.5	Идентификация и аутентификация внешних пользователей	Не применимо

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
ИАФ.7	Защита аутентификационной информации при передаче	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
2 Управление доступом (УПД)		
УПД.0	Регламентация правил и процедур управления доступом	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
УПД.1	Управление учетными записями пользователей	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.2	Реализация модели управления доступом	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.4	Разделение полномочий (ролей) пользователей	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.5	Назначение минимально необходимых прав и привилегий	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	Функционал Комплекса средств защиты от несанкционированного доступа
УПД.10	Блокирование сеанса доступа пользователя при неактивности	Функционал Комплекса средств защиты от несанкционированного доступа
УПД.11	Управление действиями пользователей до идентификации и аутентификации	Функционал Комплекса средств защиты от несанкционированного доступа
УПД.13	Реализация защищенного удаленного доступа	Не применимо
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	Не применимо

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
4 Защита машинных носителей персональных данных (ЗНИ)		
ЗНИ.0	Регламентация правил и процедур 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	Функционал Комплекса средств защиты от несанкционированного доступа
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации	Функционал Комплекса средств защиты от несанкционированного доступа
ЗНИ.7	Контроль подключения съемных машинных носителей информации	Функционал Комплекса средств защиты от несанкционированного доступа
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	Функционал Комплекса средств защиты от несанкционированного доступа
5 Аудит безопасности (АУД)		
АУД.0	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	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 правил и процедур антивирусной защиты	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
АВЗ.1	Реализация антивирусной защиты	Функционал Комплекса антивирусной защиты
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	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 правил и процедур обеспечения целостности	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
ОЦЛ.1	Контроль целостности программного обеспечения	Функционал Комплекса средств защиты от несанкционированного доступа
9 Обеспечение доступности (ОДТ)		
ОДТ.0	Регламентация правил и процедур обеспечения доступности	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
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	Регламентация правил и процедур 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

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
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 правил и процедур 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.19	Защита информации при ее передаче по каналам связи	Не применимо, информация передается в пределах контролируемой зоны
ЗИС.20	Обеспечение доверенных канала, маршрута	Не применимо, информация передается в пределах контролируемой зоны
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.32	Защита беспроводных соединений	Не применимо
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	Не применимо
ЗИС.35	Управление сетевыми соединениями	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.38	Защита информации при использовании мобильных устройств	Не применимо
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Функционал Комплекса защиты среды виртуализации

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
12 Реагирование на компьютерные инциденты (ИНЦ)		
ИНЦ.0	Регламентация правил и процедур 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	Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
УКФ.2	Управление изменениями	Функционал Комплекса контроля безопасности конфигураций
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
14 Управление обновлениями программного обеспечения (ОПО)		
ОПО.0	Регламентация правил и процедур 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
ОПО.2	Контроль целостности обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
ОПО.3	Тестирование обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
ОПО.4	Установка обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
15 Планирование мероприятий по обеспечению безопасности (ПЛН)		
ПЛН.0	Регламентация правил и процедур 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	Регламентация правил и процедур 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
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 правил и процедур 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.3	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

3.2 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.

3.2.1 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 ЭБСМ и ИСУБ ПС250 и ОЗХ;

– настройка встроенных механизмов защиты прикладного ПО;

– настроек встроенных механизмов защиты активного сетевого оборудования.

3.2.1.1 Решение наложенных средств защиты от несанкционированного доступа

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 ЭБСМ и ИСУБ ПС250 и ОЗХ и выделенном сервере управления комплексом:

– клиентская часть решения;

– сервер безопасности;

– центр управления решением.

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.

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

Программа управления используется для централизованного управления серверами безопасности и клиентами в сетевом режиме функционирования и устанавливается на АРМ администратора информационной безопасности СОИБ, Сегмент управления (титул 2201).

3.2.1.2 Встроенные механизмы защиты прикладного ПО

Встроенные механизмы прикладного ПО предназначены для обеспечения защищенного режима функционирования прикладного ПО ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ.

С помощью встроенных средств защиты прикладного ПО ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ предусматривается принятие ряда мер, в соответствии с Описанием порядка реализации мер защиты информации, представленном в таблице 3.1.

3.2.1.3 Встроенные механизмы защиты активного сетевого оборудования

Встроенные механизмы активного сетевого оборудования (АСО) предназначены для обеспечения защищенного режима функционирования сетевого оборудования ЛВС ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ.

С помощью встроенных средств защиты АСО ЛВС ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ предусматривается принятие ряда мер, в соответствии с Описанием порядка реализации мер защиты информации, представленном в таблице 3.1.

3.2.2 Комплекс антивирусной защиты

Комплекс антивирусной защиты обеспечивает:

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

– контроль запуска программ;

– защиту от шифрования;

– мониторинг файловых операций;

– защиту от эксплойтов;

– 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 ЭБСМ и ИСУБ ПС250 и ОЗХ, серверах СОИБ и выделенном сервере управления комплексом:

– клиентская часть решения;

– 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.

Сервер управления решением 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 информационной безопасности СОИБ, Сегмент управления (титул 2201), при подключении к консоли Сервера управления решением.

3.2.3 Комплекс анализа защищенности инфраструктуры

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

Комплекс анализа защищенности инфраструктуры обеспечивает выполнение следующих функций:

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

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

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

– определение рекомендаций по устранению выявленных уязвимостей.

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

3.2.4 Комплекс сбора, анализа и корреляции событий безопасности

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 представляет собой SIEM-коллектор, обеспечивающий сбор событий безопасности с АРМ, серверов ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ, серверов СОИБ, по протоколу syslog.

Передача событий осуществляется в одностороннем порядке с инициацией отправки событий от источника.

SIEM-коллектор СОИБ отправляет нормализованные и агрегированные события в Центральную ноду SIEM, расположенную в МСПД.

SIEM-коллектор устанавливается на выделенном виртуальном сервере СОИБ, Сегмент СЗИ (титул 2201).

3.2.5 Комплекс резервного копирования информационных ресурсов

Комплекс резервного копирования предназначен для резервного копирования и восстановления данных АРМ и серверов ИСУБ ЭБСМ и 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.

Комплекс резервного копирования состоит из следующих программных пакетов, устанавливаемых на АРМ, серверах ИСУБ ЭБСМ и ИСУБ ПС250 и ОЗХ, серверах СОИБ и выделенном сервере управления комплексом:

– агенты резервного копирования;

– сервер управления решением.

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

Управление решением осуществляется с АРМ администратора информационной безопасности 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 ЭБСМ и ИСУБ ПС250 и ОЗХ, с передачей резервных копий в Систему хранения данных;

– с выгрузкой резервных копий на съемный носитель, при отсутствии технической возможности установки Агента, и последующей передачей в Систему хранения данных.

3.2.6 Комплекс обеспечения сетевой безопасности

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

Комплекс обеспечения сетевой безопасности обеспечивает следующие функции в рамках СОИБ:

– 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, функционирующего в режиме Active/Passive. МСЭ периметра АСУ обеспечивают контроль и фильтрацию трафика между СОИБ и внешними по отношению к СОИБ системами и сетями связи.

Межсетевые экраны периметра ЛСУ устанавливаются в виде отказоустойчивого кластера аппаратных межсетевых экранов, функционирующего в режиме Active/Passive. МСЭ периметра ЛСУ обеспечивают контроль и фильтрацию трафика между СОИБ и технологическим сегментом ЛСУ.

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

3.2.7 Комплекс защиты среды виртуализации

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

Комплекс защиты среды виртуализации обеспечивает следующие функции:

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

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

в) регистрация событий безопасности в виртуальной инфраструктуре;

г) разбиение виртуальной инфраструктуры на сегменты:

1) Сегмент СЗИ;
2) Сегмент инфраструктурных сервисов СОИБ.

3.2.8 Комплекс контроля конфигураций

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

Комплекс контроля конфигураций выполняет следующие функции в рамках СОИБ:

- контроль изменения конфигураций сетевого оборудования;
- контроль изменения конфигураций МЭ;
- проверки соответствия безопасности сетевого оборудования;

– проверки соответствия безопасности МЭ;

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

– контроль целостности и оперативное восстановление конфигураций;

– моделирование трафика на основе маршрутов и правил МЭ;

– контроль изменения конфигураций операционных систем, элементов сред виртуализации, прикладного программного обеспечения;

– 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 ЭБСМ и 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 МЭ, управляет агентами и консолидирует информацию в единой централизованной системе.

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

3.2.9 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;

– компоненты Комплексов СОИБ, обеспечивающие централизованную установку обновлений.

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.

Сервер обновления 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).

Сервер обновления операционных систем устанавливается на выделенном виртуальном сервере СОИБ, Сегмент инфраструктурных сервисов СОИБ (титул 2201).

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

3.2.10 Комплекс централизованного управления доступом к активному сетевому оборудованию

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 рамка 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 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).

3.2.11 Комплекс организационных мероприятий по обеспечению информационной безопасности

На этапе ввода в действие ИСУБ ЭБСМ и 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.

3.3 Инфраструктурные решения СОИБ

3.3.1 Активное сетевое оборудование

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

Активное сетевое оборудование обеспечивает следующие функции:

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

– коммутация трафика между конечными устройствами внутри сегмента СОИБ;

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

В рамках СОИБ коммутаторы устанавливаются в следующие сегменты сети:

– сегмент периметра АСУ (ядро периметра АСУ);

– сегмент сети СОИБ;

– сегмент периметра ЛСУ (ядро периметра ЛСУ).

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.

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.

Подключение активного сетевого оборудования сегментов СОИБ к существующей локальной сети выполняется по схеме с резервированием для обеспечения должного уровня отказоустойчивости. Каждый участник стека коммутаторов сегментов СОИБ подключается как минимум одной линией связи к коммутаторам существующей локальной сети.

Подключение серверного оборудования к активному сетевому оборудованию выполняется по схеме с резервированием. Каждый сервер подключается как минимум

двумя линиями связи, по одной от каждого участника логического стека. Линии связи собираются в одну логическую сущность посредством агрегации.

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

3.3.2 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.

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

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

3.3.3 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 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.

На базе встроенных механизмов Системы виртуализации, осуществляются функции обеспечения информационной безопасности в среде виртуализации, перечисленные в пункте 3.2.7.

3.3.4 Серверное оборудование

Расчёт требований осуществляется в рамках разработки Пояснительной записки по СОИБ (NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П2).

3.3.5 Система хранения данных

Расчёт требований осуществляется в рамках разработки Пояснительной записки по СОИБ (NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П2).

3.3.6 Инженерные системы

Серверы и телекоммуникационное оборудование располагается в отдельном запираемом телекоммуникационном шкафу (шкафах) СОИБ, исключающим бесконтрольный доступ в отдельном (отдельных) помещении (помещениях) (Аппаратной АСУ, 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 2-мя блоками питания подключается к двум отдельным устройствам распределения электропитания (PDU), питание на которые подается от двух разных ИБП.

Все оборудование с 1-м 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.

Расчёт требований осуществляется в рамках разработки Пояснительной записки по СОИБ (NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П2)

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

– 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
Разделы 1; 2 п. 3.1; 3.2.1; 3.2.2; 3.2.4; 3.2.7; 3.2.11	Департамент информационной безопасности Группа комплексных систем защиты информации Системный архитектор, Зац Константин Александрович	12.09.2024
п. 3.2.3; 3.2.6; 3.2.8; 3.2.10	Департамент информационной безопасности Группа комплексных систем защиты информации Системный архитектор, Жуков Андрей Игоревич	12.09.2024
п. 3.2.5; 3.2.9; 3.3.2; 3.3.3	Департамент комплексных решений Отдел инфраструктурного программного обеспечения Ведущий системный архитектор, Шацкий Дмитрий Анатольевич	12.09.2024
п. 3.3.1	Департамент комплексных решений Отдел сетей передачи данных и коммуникационных систем Системный архитектор, Сапрыкин Дмитрий Владимирович	12.09.2024

Таблица регистрации изменений

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

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

Изм.	Кол.уч.	Лист	№док	Подп.	Дата

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-ИОС5.4.2-П2

2024

СОДЕРЖАНИЕ

Лист

Взам. инв. №

Подп. и дата

Инв. №подл.

Изм.	Кол.уч	Лист	№док.	Подп.	Дата	NKNH21002-ПС-ЭБСМ-ИОС5.4.2-П2		
Разраб.		Зац			12.09.2024	Пояснительная записка	Стадия	Лист	Листов
							П	1	49
Н. контр.		Чекалёв			12.09.2024		Платформикс		
ГИП		Зац			12.09.2024				

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 этилбензола мощностью 350 тыс. тонн 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 ЭБСМ, как объекты управления, представляют собой технологический комплекс на площадке ПАО «Нижнекамскнефтехим».

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

ИСУБ ЭБСМ 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 ЭБСМ 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 ЭБСМ 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 ЭБСМ 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 ЭБСМ 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 ЭБСМ 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).

3 ОСНОВНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

3.1 Реализация требований по обеспечению информационной безопасности системы

ИСУБ ЭБСМ включает в свой состав автоматизированные системы управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (АСУ) и не являются значимыми объектами критической информационной инфраструктуры Российской Федерации. Согласно «Актам классификации АСУ», необходимо обеспечить требования по 3-му классу защищенности автоматизированных систем управления.

Базовый набор мер защиты информации, подлежащий реализации в рамках СОИБ, а также описание порядка реализации представлены 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; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.2	Идентификация и аутентификация устройств	Функционал Комплекса средств защиты от несанкционированного доступа
ИАФ.3	Управление идентификаторами	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.4	Управление средствами аутентификации	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
ИАФ.5	Идентификация и аутентификация внешних пользователей	Не применимо

Условное обозначение и номер меры	Содержание меры защиты информации	Описание порядка реализации меры защиты информации
ИАФ.7	Защита аутентификационной информации при передаче	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
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; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.2	Реализация политик управления доступа	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.4	Разделение полномочий (ролей) пользователей	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.5	Назначение минимально необходимых прав и привилегий	Функционал Комплекса средств защиты от несанкционированного доступа; Функционал Комплекса централизованного управления доступом к активному сетевому оборудованию
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	Функционал Комплекса средств защиты от несанкционированного доступа
УПД.10	Блокирование сеанса доступа пользователя при неактивности	Функционал Комплекса средств защиты от несанкционированного доступа
УПД.11	Управление действиями пользователей до идентификации и аутентификации	Функционал Комплекса средств защиты от несанкционированного доступа
УПД.13	Реализация защищенного удаленного доступа	Не применимо
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	Не применимо

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
ЗНИ.7	Контроль подключения съемных машинных носителей информации	Функционал Комплекса средств защиты от несанкционированного доступа
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	Функционал Комплекса средств защиты от несанкционированного доступа
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.2	Антивирусная защита электронной почты и иных сервисов	Не применимо

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
9 Обеспечение доступности (ОДТ)		
ОДТ.0	Регламентация политики обеспечения доступности	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности
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.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.19	Защита информации при ее передаче по каналам связи	Не применимо, информация передается в пределах контролируемой зоны
ЗИС.20	Обеспечение доверенных канала, маршрута	Не применимо, информация передается в пределах контролируемой зоны
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	Функционал Комплекса обеспечения сетевой безопасности
ЗИС.32	Защита беспроводных соединений	Не применимо
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.38	Защита информации при использовании мобильных устройств	Не применимо
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	Функционал Комплекса защиты среды виртуализации
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
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
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
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
ОПО.2	Контроль целостности обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
ОПО.3	Тестирование обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
ОПО.4	Установка обновлений программного обеспечения	Функционал Комплекса управления обновлениями программного обеспечения
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
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.3	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	Посредством Комплекса организационных мероприятий по обеспечению информационной безопасности

3.2 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.

3.2.1 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 ЭБСМ;

– настройка встроенных механизмов защиты прикладного ПО;

– настроек встроенных механизмов защиты активного сетевого оборудования.

3.2.1.1 Решение наложенных средств защиты от несанкционированного доступа

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 ЭБСМ и выделенном сервере управления комплексом:

– клиентская часть решения;

– сервер безопасности;

– центр управления решением.

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.

Сервер безопасности 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).

Программа управления используется для централизованного управления серверами 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.

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.

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.

3.2.1.2 Встроенные механизмы защиты прикладного ПО

Встроенные механизмы прикладного ПО предназначены для обеспечения защищенного режима функционирования прикладного ПО ИСУБ ЭБСМ. 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.

3.2.1.3 Встроенные механизмы защиты активного сетевого оборудования

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

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;

– ограничение времени действия неиспользуемых открытых консолей управления АСО;

– ограничение количества неудачных попыток входа в консоль управления АСО;

– 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.

3.2.2 Комплекс антивирусной защиты

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 ЭБСМ, серверах СОИБ и выделенном сервере управления комплексом:

– клиентская часть решения;

– 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.

Сервер управления решением 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 Сервера управления решением.

Задача постоянной защиты файлов 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.

Компонент контроля запуска программ 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, могут выступать: сертификаты, хеш-сумма, путь к файлу.

Компонент защиты от эксплойтов защищает память исполняемых процессов от эксплуатации уязвимостей. Специальная служба внедряет агента защиты в защищаемые процессы, который контролирует их целостность. Список программ, которые защищает компонент от эксплуатации уязвимостей в них, ограничен техническими решениями производителя Комплекса антивирусной защиты.

Задача защиты от шифрования 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.

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

3.2.3 Комплекс анализа защищенности инфраструктуры

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

Комплекс анализа защищенности инфраструктуры обеспечивает выполнение следующих функций:

– затирание удаляемой информации;

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

– сканирование доступности сетевых портов компонентов ИСУБ ЭБСМ и СОИБ;

– автоматический поиск (анализ) уязвимостей компонентов ИСУБ ЭБСМ 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 в трех режимах: в режиме пентеста, режиме аудита и режиме соответствия требованиям.

Сканирование в режиме пентеста направлено на получение оценки защищенности контролируемого узла и отличается использованием минимальных привилегий в сканируемой системе. С помощью данного сканирования выявляются уязвимости программного обеспечения, проверка стойкости паролей и отсутствующие обновления ОС.

Сканирование в режиме аудита предполагает использование специальной учетной записи для более глубокой проверки безопасности операционной системы и приложений контролируемого узла.

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

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

Анализ защищенности контролируемых узлов производится при сканировании в режимах пентеста и аудита. Результаты сканирования представляются в отчете о найденных уязвимостях.

При сканировании в режиме пентеста 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 в режиме пентеста, содержит перечень протоколов, доступных для взаимодействия с контролируемым узлом, и выявленные уязвимости в реализации данных протоколов.

При сканировании в режиме аудита, выявляются уязвимости, которые могут эксплуатироваться как внешним нарушителем, так и нарушителем, имеющим полный или ограниченный доступ к операционной системе и прикладному ПО контролируемого узла. Отчет об уязвимостях, выявленных в режиме аудита, содержит

перечень программ, функционирующих на контролируемом узле, и выявленные в них уязвимости.

Контроль соответствия требованиями безопасности производится при сканировании в режиме соответствия требованиям. При этом результаты одного сканирования могут использоваться для оценки соответствия просканированных узлов нескольким техническим стандартам.

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

3.2.4 Комплекс сбора, анализа и корреляции событий безопасности

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, обеспечивающий сбор событий безопасности с АРМ, серверов ИСУБ ЭБСМ, 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, 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 Центральную ноду SIEM, расположенную в МСПД.

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

3.2.5 Комплекс резервного копирования информационных ресурсов

Комплекс резервного копирования предназначен для резервного копирования и восстановления данных АРМ и серверов ИСУБ ЭБСМ, 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 ЭБСМ;

– контроллер домена СОИБ.

Комплекс резервного копирования информационных ресурсов состоит из программных пакетов, устанавливаемых на АРМ, серверах ИСУБ ЭБСМ, серверах СОИБ, выделенном сервере управления и медиа-сервере:

– сервер управления решением;

– медиа-сервер;

– 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).

Медиа-сервер — 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 медиа-сервера 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.

Медиа-сервер 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 ЭБСМ, с передачей резервных копий в Систему хранения данных.

3.2.1 Комплекс обеспечения сетевой безопасности

Комплекс обеспечения сетевой безопасности предназначен для обеспечения защиты компонентов ИСУБ ЭБСМ 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, 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, 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), 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.

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.

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

Межсетевые экраны периметра 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.

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

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

3.2.2 Комплекс защиты среды виртуализации

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

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.

Управление доступом внутри виртуальных машин реализуется при помощи функционала разграничения доступа наложенных средств защиты от несанкционированного доступа Комплекса средств защиты от несанкционированного доступа.

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.

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.

Политиками безопасности системы виртуализации обеспечивается:

– ограничение длительности сессии пользователей;

– управление сроком действия паролей;

– управление сложностью паролей.

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

3.2.3 Комплекс контроля конфигураций

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

Функционал Комплекса контроля конфигураций состоит из следующих модулей:

– модуль контроля сетевых устройств: 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: предназначен для контроля целостности файлов операционной системы и контроля их конфигураций.

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 ЭБСМ, 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 и прикладного программного обеспечения.

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

3.2.4 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;

– сервер обновления операционных систем Linux;

– Компоненты Комплексов СОИБ, обеспечивающие централизованную установку обновлений.

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).

3.2.5 Комплекс централизованного управления доступом к активному сетевому оборудованию

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 рамка 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.

3.2.6 Комплекс организационных мероприятий по обеспечению информационной безопасности

На этапе ввода в действие ИСУБ ЭБСМ, разрабатываются организационно-распорядительные документы, регламентирующие:

– затирание удаляемой информации;

– 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.

3.3 Инфраструктурные решения СОИБ

3.3.1 Активное сетевое оборудование

3.3.1.1 Общие принципы

Активное сетевое оборудование СОИБ предназначено для обеспечения компонентов СОИБ сетевой связностью с сетевой инфраструктурой ИСУБ ЭБСМ.

Активное сетевое оборудование обеспечивает следующие функции:

– обеспечение доступа сегмента СОИБ к сети передачи данных ИСУБ ЭБСМ;

– коммутация трафика между конечными устройствами внутри сегмента СОИБ;

– резервирование подключения конечных устройств СОИБ к сети передачи данных ИСУБ ЭБСМ.

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 3.2.1.

3.3.1.2 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.

3.3.1.3 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.

3.3.1.4 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.

3.3.1.5 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.

3.3.2 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	
Network access: Allow anonymous SID/Name translation	Disabled
Network Security	
Network security: Do not store LAN Manager hash	Disabled

Параметр	Значение
value on next password change	
Network security: Force logoff when logon hours expire	Disabled

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

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

3.3.3 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 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 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

Сервер	Параметр	Значение
	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
	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 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
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 3.2.2.

3.3.4 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 – медиа-сервер.

Для построения платформы виртуализации используются серверы 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 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) четыре коротковолновых трансивера SFP+ с пропускной способностью 10 Гб/с;

з) RAID контроллер 2ГБ кэш памяти;

и) два блока питания;

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

3.3.5 Система хранения данных

В данном проекте используется СХД 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.

3.3.6 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.

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	 12.09.2024
п. 3.2.3; 3.2.8; 3.2.10	Департамент информационной безопасности Группа комплексных систем защиты информации Системный архитектор, Турков Антон Сергеевич	 12.09.2024
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	 12.09.2024
п. 3.2.9; 3.3.2	Департамент комплексных решений Отдел инфраструктурного программного обеспечения Ведущий системный архитектор, Шацкий Дмитрий Анатольевич	 12.09.2024
3.3.1	Департамент комплексных решений Отдел сетей передачи данных и коммуникационных систем Системный архитектор, Сапрыкин Дмитрий Владимирович	 12.09.2024

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	12.09.2024

Таблица регистрации изменений

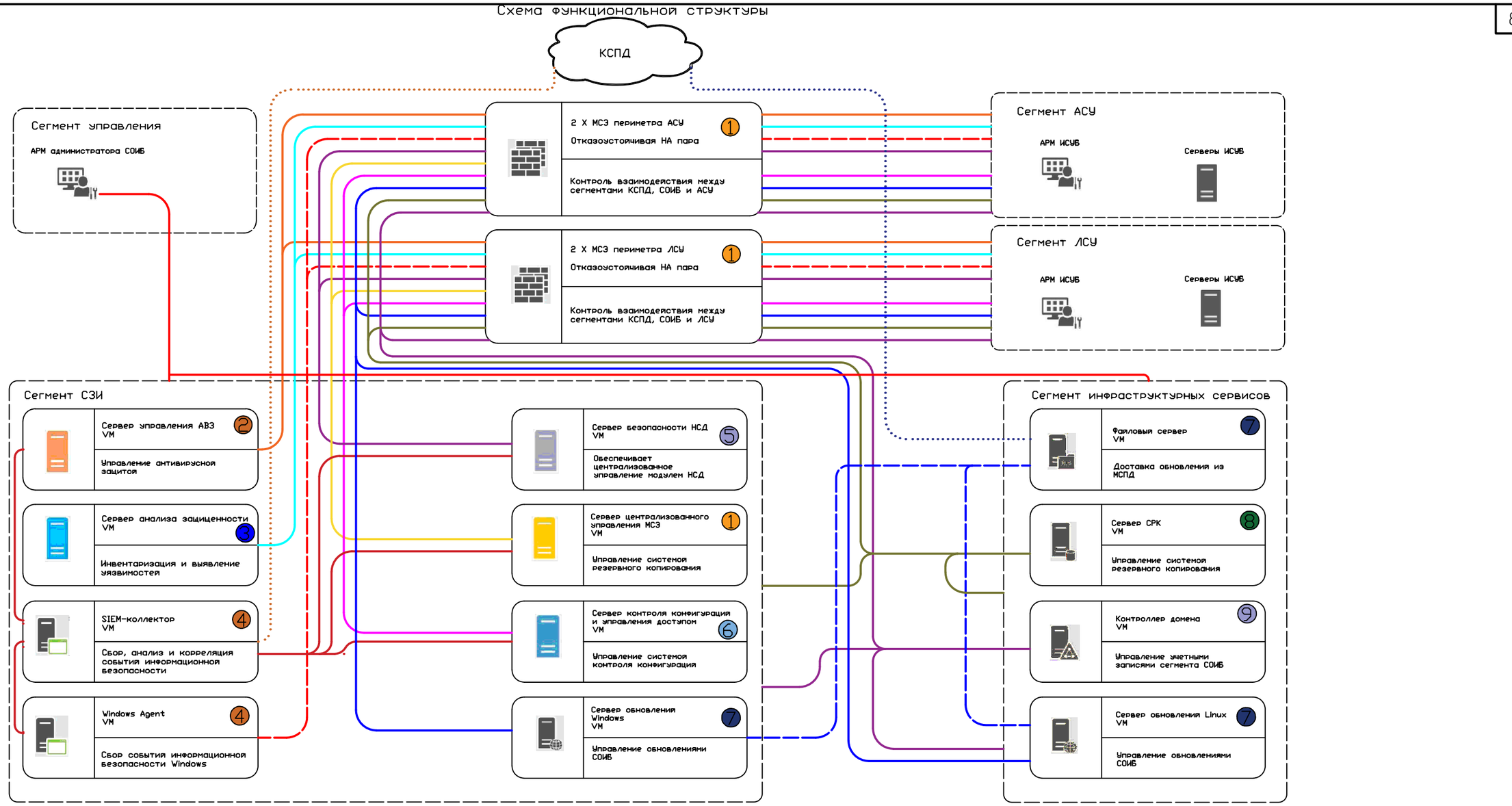
Изм.	Номера листов (страниц)				Всего листов (страниц) в док.	Номер док.	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных				

Взам. инв. №

Подп. и дата

Инв. № подл.

Схема функциональной структуры



Обозначение программных и технических средств в составе системы

Графическое изображение технического (программного) средства	Тип, количество Режим работы ○
	Основное назначение технического (программного) средства

Обозначение внешних систем

Графическое изображение системы

Наименование системы

Обозначение подсистем

1. Комплекс обеспечения сетевой безопасности
2. Комплекс антивирусной защиты
3. Комплекс анализа защищенности инфраструктуры
4. Комплекс сбора, анализа и корреляции события
5. Комплекс защиты от НСД
6. Комплекс контроля конфигурация и управления доступом
7. Комплекс управления обновлениями ПО
8. Комплекс резервного копирования информационных ресурсов
9. Контроллер домена

Обозначение взаимодействия

- Управление СОИБ
- Взаимодействие 1 с ИСУБ
- Взаимодействие 2 с ИСУБ
- Взаимодействие 3 с ИСУБ
- Взаимодействие 4 с КСПД
- Взаимодействие 4 с ИСУБ
- Взаимодействие 4 с СОИБ
- Взаимодействие 5 с ИСУБ
- Взаимодействие 6 с ИСУБ
- Взаимодействие 7 с КСПД
- Взаимодействие 7 с СОИБ
- Взаимодействие 7 с ИСУБ
- Взаимодействие 8 с ИСУБ
- Взаимодействие 9 с ИСУБ

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	№док.	Подпись	Дата
Разраб.		Турков А.			12.09.2024
Н. контр.		Чекалёв Н.			12.09.2024
ГИП		Зац К.			12.09.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-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

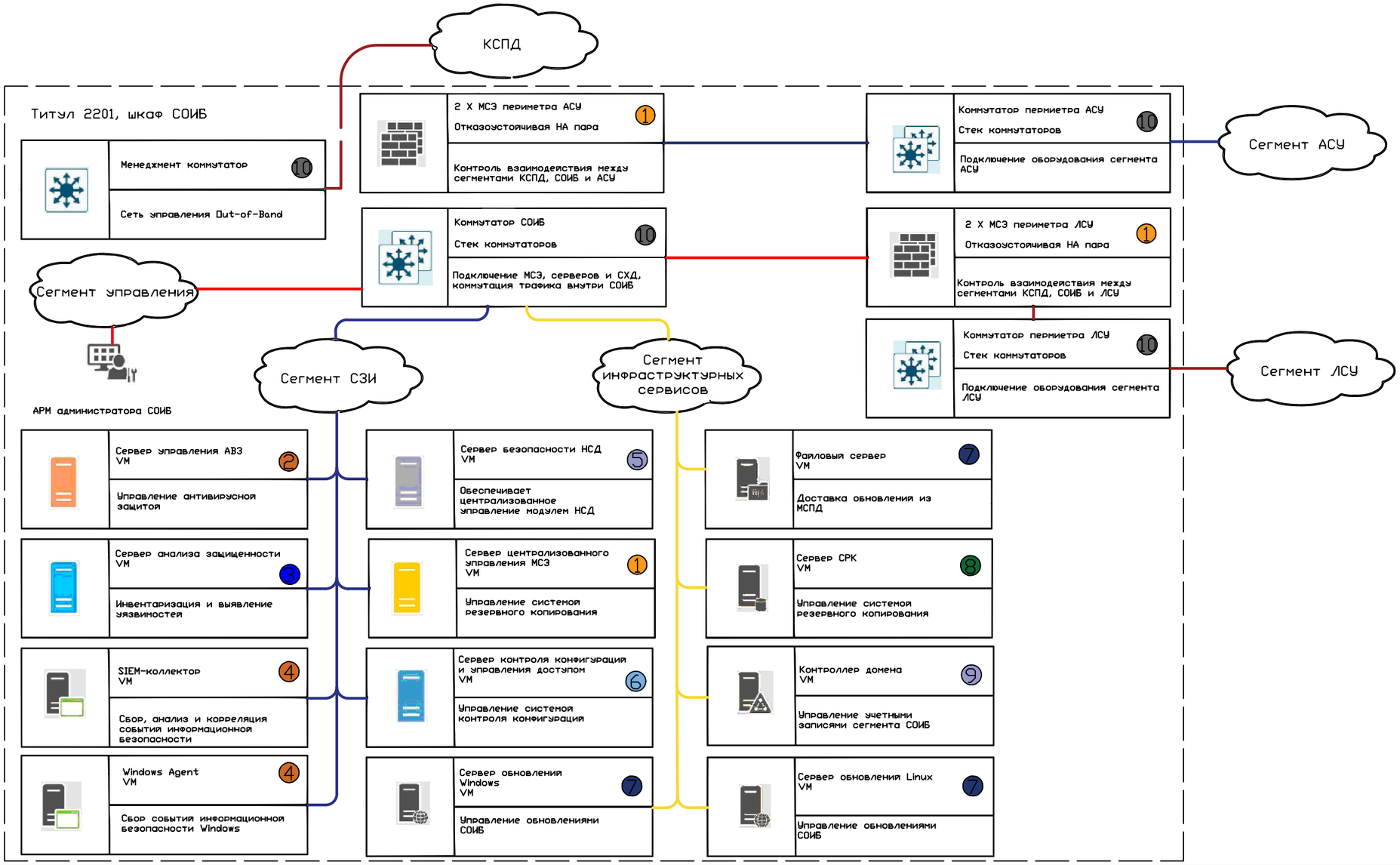
Схема функциональной структуры

Платформикс

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-С2_0_0_RU.dwg

Формат А3

Структурная схема комплекса технических средств СОИБ



Обозначение программных и технических средств в составе системы

Графическое изображение технического (программного) средства	Тип, количество Режим работы ○
	Основное назначение технического (программного) средства

Обозначение внешних систем

Графическое изображение системы
Наименование системы

Обозначение подсистем

1. Комплекс обеспечения сетевой безопасности
2. Комплекс антивирусной защиты
3. Комплекс анализа защищенности инфраструктуры
4. Комплекс сбора, анализа и корреляции события
5. Комплекс защиты от НСД
6. Комплекс контроля конфигурации и управления доступом
7. Комплекс управления обновлениями ПО
8. Комплекс резервного копирования информационных ресурсов
9. Контроллер домена
10. Активное сетевое оборудование

Обозначение взаимодействия

- Сеть Out-of-Band
- Сегмент инфраструктурных сервисов
- Сегмент СЗИ
- Сегмент управления
- Сегмент АСУ
- Сегмент ЛСУ

Примечание:
Цвета линия – наименование соответствующего сегмента

Изм.	Кол.уч.	Лист	№док.	Подпись	Дата
Разраб.		Зац К.			12.09.2024
Н.Контр.		Чекалёв Е.			12.09.2024
ГИП		Зац К.			12.09.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-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

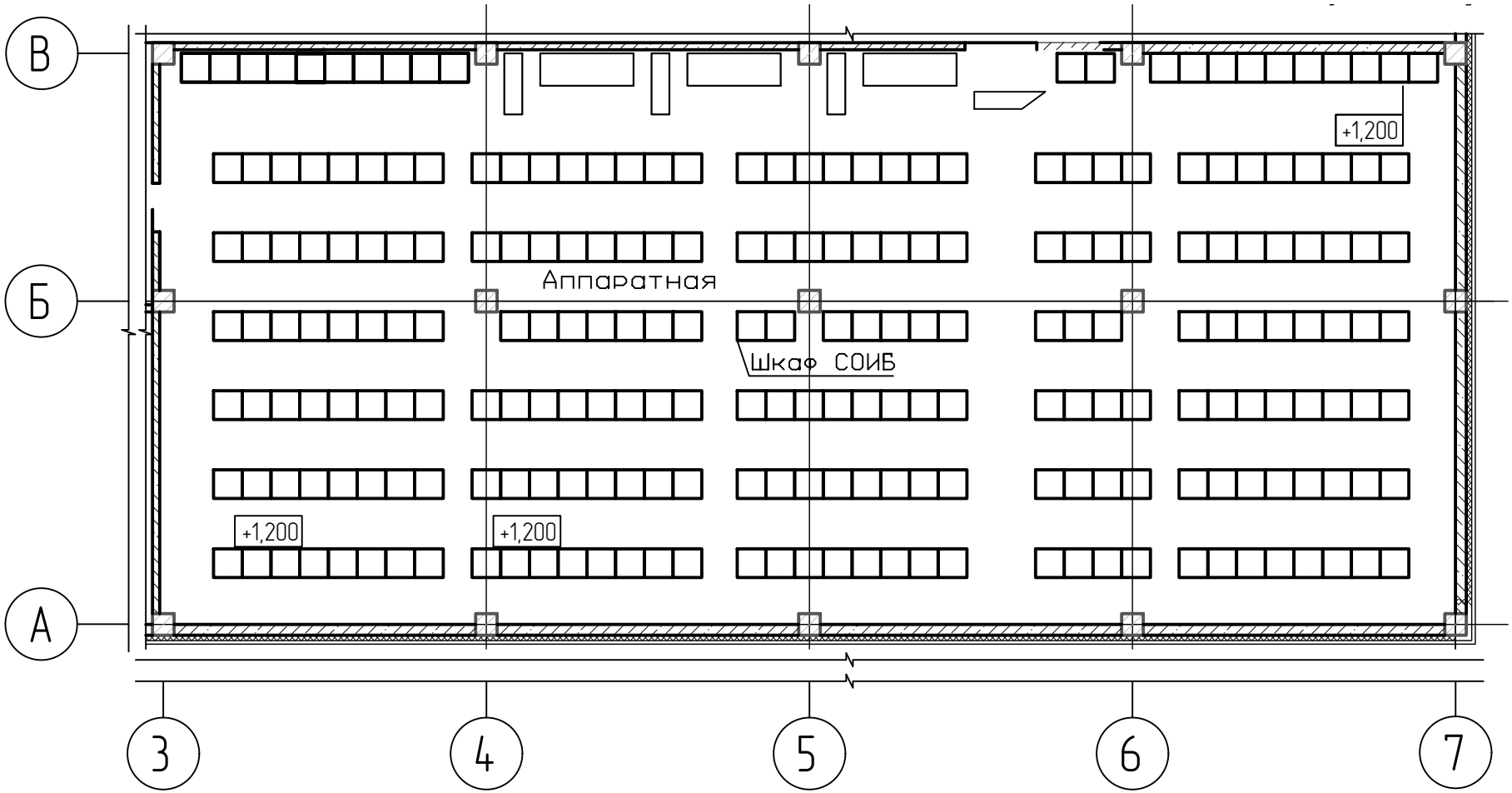
Взам. инв. №

Подп. и дата

Инв. № подл.

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-С1_0_0_RU.dwg

Формат А3



Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	N°док.	Подпись	Дата
Разраб.		Зац К.			12.09.2024
Н. контр.		Чекалёв Е.			12.09.2024
ГИП		Зац К.			12.09.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-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

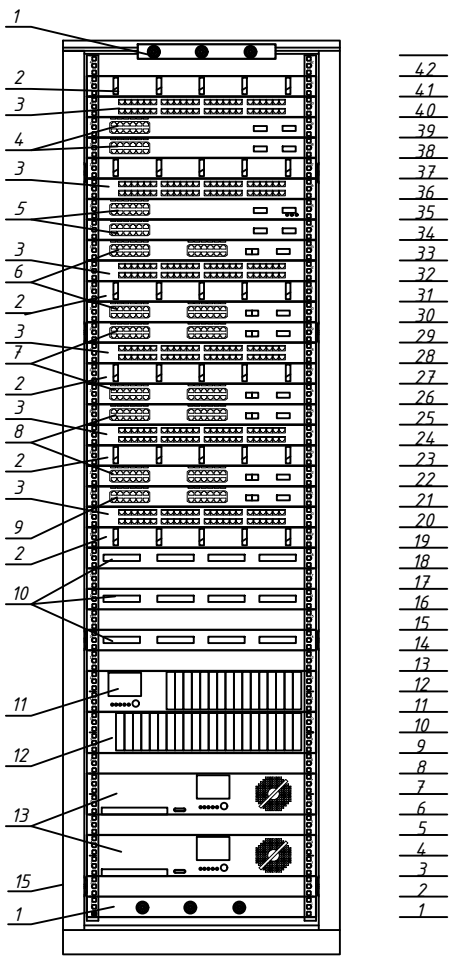
Схема расположения оборудования в Аппаратной

Платформикс

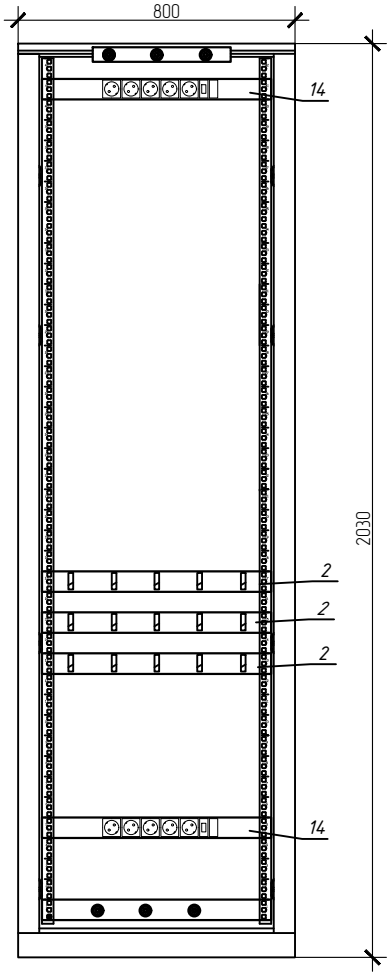
NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-С7_0_0_R.dwg

Формат А4

Фронтальный фасад



Задний фасад



Условные обозначения:

1 – Блок вентиляторов
2 – Кабельный органайзер
3 – Патч-панель
4 – МСЭ периметра АСУ
5 – МСЭ периметра ЛСУ
6 – Коммутаторы сегмента СОИБ
7 – Коммутаторы ядра периметра АСУ
8 – Коммутаторы ядра периметра ЛСУ
9 – Менеджмент коммутатор
10– Кластер серверов
11 – Медиа-сервер
12– СХД
13– ИБП
14– Блок розеток
15– Шкаф телекоммуникационный 800х800х2030 мм (ШхГхВ)

Взам. инв. №

Подп. и дата

Инв. № подл.

Изм.	Кол.уч.	Лист	N°док.	Подпись	Дата
Разраб.		Яуров Л.			12.09.2024
Н. контр.		Чекалёв Е.			12.09.2024
ГИП		Зац К.			12.09.2024

NKNH21002-ПС-ЭБСМ-ИОС5.4.2-0000-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