Помещение электромеханика
АРМ ШЧИ
UPS
RS-232
Помещение ДЦ
АРМ
ДЦ «Метроком-М»
Существующие сети связи
метрополитена
Помещение ДСЦП
АРМ ДСЦП
(резервный)
АРМ ДСЦП
(основной)
Стойка системных
блоков
UPS
RS-232
Eth
UDP
Opt
EDS-305-T
Optic
Релейная
АТДП
Оборудование
ДЦ-ММ
АРМ ШН(резервный)
АРМ ШН(основной)
Eth/UDP
Positive Technologies
Industrial Security Incident Manager (PT ISIM)
АРМ PT ISIM
АРМ ИБ PT ISIM
Сервер анализа
wan
Router R1
Router R2
EDR-G902-T
Инфодиод 3
Инфодиод 1
Инфодиод 2
СТДМ
Router R3
EDR-810-2GSFP-T
Коммутатор
К3
Span-
port
EDS-518-
E-MM-ST-T
Коммутатор
К1
Коммутатор
К2
EDS-518-E-MM-ST-T
МСПУ
(Шкаф ШФГП)
СТМ МСПУ
Router R
Стойка №13
УСОД 2 (СТМ)
Сервер МПЦ1
Сервер МПЦ2
UPS1
UPS2
УСОД 1 (СТМ)
ССОД (СТМ)
ЦВМ-М
Стойка ЦМА
Сеть СТМ
RS-485
Сеть ОК
RS-422
К стойкам МПЦ-СМ с ОК стрелок, светофоров, ЦМ КРЦ-М

Сокращения:
АРМ ДСЦП – рабочее место дежурного по станции
АРМ ИБ PT ISIM – рабочее место специалиста по инф-ой безопасности
АРМ ШН – рабочее место электромеханика
АРМ ШЧИ – рабочее место дежурного инженера СЦБ
АРМ PT ISIM - рабочее место системы PT ISIM
АСДУ – автоматизированная система диспетчерского управления
МСПУ – установка питающая модульная совмещенная
ОК – объектные контроллеры
СТМ – средства технического мониторинга
УСОД – устройство сбора и обработки данных
ССОД – сервер сбора и обработки данных
ЦВМ-М – центральный вычислительный модуль для метрополитенов
ЦМА - цифровой модуль управления объектами автоматики
ЦМ КРЦ-М – цифровой модуль контроля рельсовых цепей для метрополитенов
Opt – медиаконвертер
Router – роутер
Eth – сеть Ethernet 100Base-TX, протокол TCP/IP
PT ISIM — программно-аппаратный комплекс глубокого анализа технологического трафика
UPS – источник бесперебойного питания

Структура сети МПЦ-СМ

Ст. Новокосино

Изм.	Кол.уч.	Лист	№ док.	Подп.	Дата	ЕИУС.468333.003-2317ТР	Лист 1

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

Описание структуры сети МПЦ-СМ

1. Перечень сокращений

АРМ ДСЦП – автоматизированное рабочее место дежурного по станции

АРМ ШН – автоматизированное рабочее место электромеханика СЦБ

АРМ ШЧИ – автоматизированное рабочее место дежурного инженера

АСУ – автоматизированная система управления

ГосСОПКА – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак

ДЦ – диспетчерская централизация

ИБ – информационная безопасность

МПЦ – микропроцессорная централизация

МПЦ-СМ – микропроцессорная централизация для метрополитенов

МСПУ – модульная совмещенная питающая установка

ОК – объектные контроллеры

ПАК – программно-аппаратный комплекс

ПК – персональный компьютер

ПО – программное обеспечение

Сенсор – сервер анализа сетевого трафика

ССОД – сервер сбора и обработки данных

СТМ – средства технического мониторинга

УСОД – устройство сбора и обработки данных

ЦВМ-М – центральный вычислительный модуль для метрополитенов

ЦМ КРЦ-М – цифровой модуль контроля рельсовых цепей для метрополитенов

2. Описание структуры сети МПЦ-СМ

2.1. АРМ ДСЦП предназначено для организации пользовательского интерфейса по управлению и контролю объектами электрической централизации на станции.

В состав АРМ ДСЦП входят два идентичных аппаратно-программных комплекса, которые работают в режиме горячего резервирования с выделением

одного активного, и различаются как «АРМ ДСЦП (основной)» и «АРМ ДСЦП (резервный)». В качестве аппаратной платформы АРМ ДСЦП служат ПК промышленного исполнения.

Основной и резервный АРМ ДСЦП осуществляют взаимодействие с ЦВМ-М по дублированным каналам связи через коммутаторы К1, К2.

Взаимодействие с СТМ основной и резервный АРМ ДСЦП осуществляют по каналам связи через коммутатор К3.

2.2. АРМ ШН предназначено для организации пользовательского интерфейса по контролю за объектами электрической централизации на станции и обеспечения персонала визуальной оперативной информацией о состоянии системы МПЦ-СМ.

В состав АРМ ШН входят два идентичных аппаратно-программных комплекса, которые работают в режиме горячего резервирования с выделением одного активного, и различаются как «АРМ ШН (основной)» и «АРМ ШН (резервный)». В качестве аппаратной платформы АРМ ШН служат ПК промышленного исполнения.

Основной и резервный АРМ ШН осуществляют взаимодействие с ЦВМ-М по дублированным каналам связи через коммутаторы К1, К2.

Взаимодействие с СТМ основной и резервный АРМ ШН осуществляют по каналам связи через коммутатор К3.

2.3. Сервера МПЦ1, МПЦ2 обеспечивают:

- обработку и долгосрочное сохранение данных архива МПЦ-СМ;
- обмен данными и передачу команд через коммутаторы К1, К2;
- обмен данными с внешней системой ДЦ.

Также на серверах сохраняется архив журнала событий, данные о текущем состоянии полевого оборудования и устройств МПЦ-СМ.

В качестве аппаратной платформы Серверов МПЦ1, МПЦ2 служат ПК промышленного исполнения.

2.4. АРМ ШЧИ предназначено для организации пользовательского интерфейса по контролю за объектами электрической централизации на станции и обеспечения дежурного инженера визуальной оперативной информацией о состоянии системы МПЦ-СМ.

2.5. Сопряжение устройств МПЦ-СМ с аппаратурой ДЦ-ММ осуществляется при помощи промышленных маршрутизаторов безопасности R1, R2 и программных модулей увязки с ДЦ-ММ, которые входят в состав ПО Серверов МПЦ-СМ 1, 2. Промышленные маршрутизаторы используются для логического ограждения внутренней сети МПЦ-СМ, а также защиты при помощи сетевого экрана.

2.6. Связь между серверами ДЦ-ММ и МПЦ-СМ организована посредством двух каналов по сети стандарта Ethernet с использованием стека протоколов TCP/IP.

2.7. Коммутатор К3 предназначен для организации технологической сети. Эта сеть обеспечивает связь между составляющими частями МПЦ-СМ и внешней системой СТДМ.

2.8. Сопряжение устройств МПЦ-СМ с внешней СТДМ осуществляется при помощи промышленного маршрутизатора безопасности R3 и программных модулей увязки с СТДМ, которые входят в состав ПО ССОД. Промышленный маршрутизатор R3 используется для логического ограждения внутренней сети МПЦ-СМ, а также защиты при помощи сетевого экрана.

Связь с внешней СТДМ осуществляется по сети стандарта Ethernet с использованием стека протоколов TCP/IP.

Передача информации от СТМ о текущем состоянии МПЦ-СМ во внешнюю СТДМ производится по протоколу MQTT.

2.9. ПАК PT ISIM предназначен для обеспечения промышленной кибербезопасности системы МПЦ-СМ.

Взаимодействие PT ISIM с МПЦ-СМ осуществляется через аппаратные Инфодиоды 1-3, обеспечивающие на физическом уровне однонаправленную передачу данных с портов зеркалирования (SPAN-port) сетевых коммутаторов К1-К3 МПЦ-СМ в ПАК PT ISIM.

ПАК PT ISIM состоит из следующих компонентов: Сервер анализа, АРМ PT ISIM и административный АРМ ИБ PT ISIM.

2.9.1. Сервер анализа, с установленным ПО netView Sensor, использует для анализа копию трафика сети, детектируя события кибербезопасности, и позволяет:

– автоматически собирать необходимую информацию об активных элементах

сети (коммутаторах, маршрутизаторах, АРМ, ПЛК), представлять ее в удобном пользователю виде, выявлять потенциально опасные изменения (нарушения сегментации, неправомерный доступ) и вовремя реагировать на них;

- выявлять внутренние угрозы, такие как потенциально опасные действия персонала и ошибки конфигурации;
- выполнять непрерывный мониторинг сетевой активности и выявлять уязвимости и хакерские атаки на сеть;
- анализ сохраненной копии трафика и расследование инцидента;
- выполнять контроль несанкционированного подключения к сети, подбор паролей к компонентам системы, неправомерное исполнение управляющих команд, подмену конфигураций и прошивок оборудования;
- выстроить эффективное взаимодействие с ведомственными и корпоративными центрами системы ГосСОПКА для обеспечения мониторинга и реагирования на инциденты ИБ.

В качестве аппаратной платформы Сервера служит ПК промышленного исполнения.

2.9.2. АРМ PT ISIM предназначено для отображения элементов сетевой топологии, оперативного предоставления информации об инцидентах в системе и располагает минимальным набором инструментов, необходимых для поддержки административных регламентов.

В качестве аппаратной платформы служит сенсорный ПК промышленного исполнения.

2.9.3. АРМ ИБ PT ISIM предназначено для отображения элементов сетевой топологии и обеспечивает полный доступ к информации об инцидентах для их расследования.

В качестве аппаратной платформы служит ПК промышленного исполнения.

3. Используемое ПО сторонних производителей

МПЦ-СМ использует следующее ПО сторонних производителей:

№ п.п.	Назначение ПО	Название	Лицензии
АРМ ДСЦП, АРМ ШН, АРМ ШЧИ			
1.	Операционная система (ОС)	Astra Linux	Лицензии ФСТЭК и ФСБ
2.	База данных (БД)	MySQL	Универсальная общественная лицензия GNU (GNU General Public License, GPL)
СТМ (ССОД, УСОД)			
1.	Операционная система (ОС)	Astra Linux	Лицензии ФСТЭК и ФСБ
2.	База данных (БД)	MySQL	Универсальная общественная лицензия GNU (GNU General Public License, GPL)
3.	Веб сервер	Nginx	Лицензия открытого программного обеспечения BSD (Berkeley Software Distribution)
4.	MQTT брокер	Mosquitto	Лицензия открытого программного обеспечения Eclipse Public License.
PT ISIM			
1.	Операционная система (ОС)	Astra Linux	Лицензии ФСТЭК и ФСБ
2.	Сенсор	netView Sensor	PT ISIM