АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ И МОНИТОРИНГА АСУМ «АЛМАЗ»

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

Версия ПО 1.0

2025

АННОТАЦИЯ

Настоящий документ содержит ознакомительную и справочную информацию об автоматизированной системе управления и мониторинга «Алмаз» (далее — АСУМ «Алмаз»), версия программного обеспечения 1.0, предназначенной для эксплуатации в составе оборудования «Алмаз», выпускаемого ООО «Связной Альянс».

Предполагается, что лица, использующие данный документ, обладают следующим уровнем подготовки:

– знание основ сетевых технологий и соответствующей терминологии;

– понимание принципов функционирования технологии плотного волнового мультиплексирования (DWDM – Dense Wavelength Division Multiplexing).

СОДЕРЖАНИЕ

1 ОБЗОР

АСУМ «Алмаз» представляет собой систему централизованного управления оборудованием DWDM (Dense Wavelength Division Multiplexing), а также обеспечивает интеграцию с внешними IT-системами, такими как OSS/BSS.

АСУМ «Алмаз» предоставляет следующие функциональные возможности:

– управление топологией сети и трейлами (network management);

– контроль неисправностей (fault management);

– управление конфигурацией сетевых устройств (configuration management);

– мониторинг и управление рабочими характеристиками (performance management);

– журналирование событий (events);

– сбор и обработка инвентарной информации (inventory);

– управление программным обеспечением сетевых элементов (software management);

– обеспечение безопасности и управление доступом (security).

Для взаимодействия с OSS-системой АСУМ «Алмаз» поддерживает северный интерфейс, реализованный в соответствии с требованиями TM Forum (TMF) и использующий протокол REST.

Взаимодействие с сетевыми элементами осуществляется посредством протокола NETCONF. Система обеспечивает сбор данных о неисправностях с оборудования сторонних производителей.

Кроме того, предусмотрена возможность организации географического резервирования с балансировкой нагрузки. Это позволяет создать распределённую архитектуру системы с развёртыванием на серверах в различных физических локациях, что повышает отказоустойчивость и общую надёжность функционирования АСУМ «Алмаз».

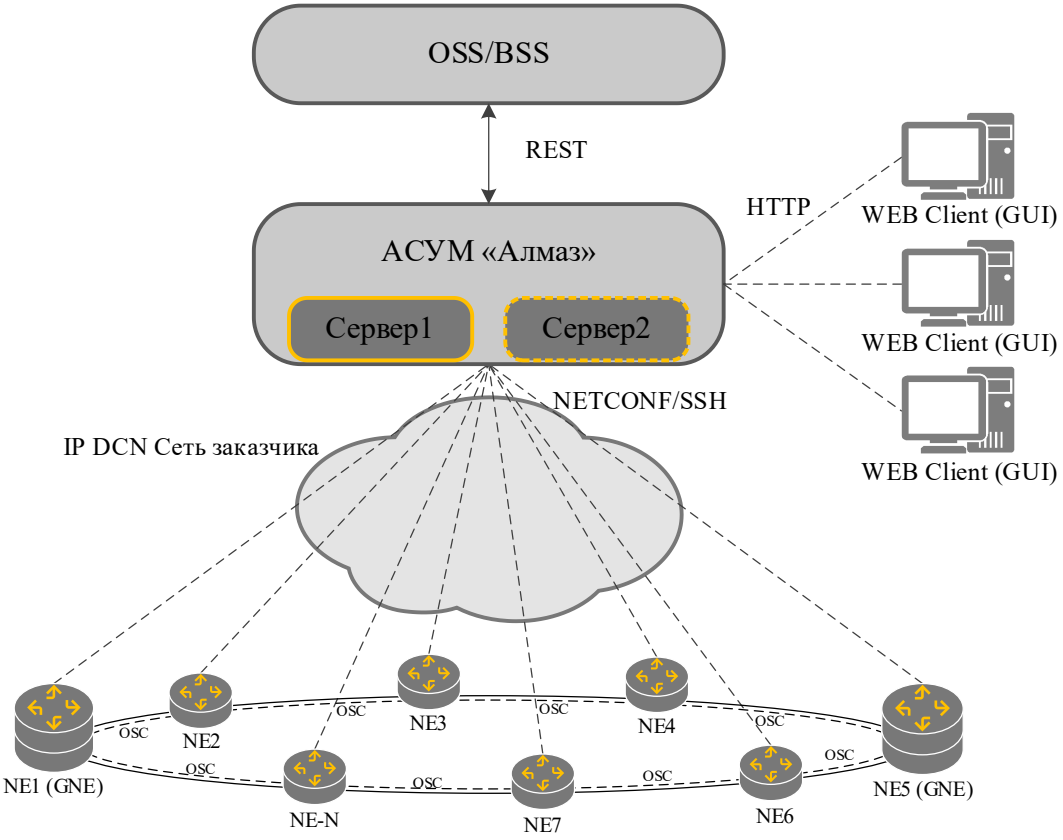

Рисунок 1 — Общая архитектура АСУМ

«Сервер 2» , указанный на схеме, является опциональным резервным сервером и может быть установлен на удалённой площадке с целью реализации географического резервирования.

Базовые технические характеристики АСУМ «Алмаз»:

– операционная система: Linux;

– аппаратная платформа: поддержка архитектуры x86;

– сетевое взаимодействие (SBI — Southbound Interface): протоколы Netconf/SSH;

– интеграция с OSS/BSS: интерфейс верхнего уровня (NBI) на основе REST API;

– обеспечение отказоустойчивости: распределённая архитектура с поддержкой балансировки нагрузки;

– организация хранения данных: использование нереляционной базы данных;

– пользовательский интерфейс: веб-интерфейс (WEB UI) с поддержкой многооконного режима.

2 ИНФОРМАЦИОННАЯ МОДЕЛЬ

АСУМ «Алмаз» соответствует базовым рекомендациям Международного союза электросвязи (ITU-T) в области управления телекоммуникационными сетями (Серия M).

В соответствии с базовой структурой TMN (Telecommunications Management Network), в системе реализованы следующие уровни управления:

а) Уровень сетевых элементов, предусматривающий сбор следующих категорий данных:

– информация о неисправностях;

– данные о рабочих показателях;

– события;

– конфигурации устройств;

– управление сетевыми элементами, включающее хранение, предоставление и обработку собранных данных, передаваемых каждым сетевым элементом.

б) Уровень управления сетью, включающий:

– маршрутизацию и организацию сетевого трафика;

– контроль взаимодействия между сетевыми элементами в рамках заданной топологии сети;

– агрегацию данных от сетевых элементов по всей сети.

Для всех управляемых объектов системы, включая физическое оборудование и логические интерфейсы, определены следующие состояния:

– административное состояние: locked (заблокировано), maintenance (техническое обслуживание), unlocked (разблокировано);

– операционное состояние: enabled (активно), disabled (неактивно).

АСУМ «Алмаз» взаимодействует с сетевыми элементами по протоколу NETCONF, загружает YANG-модели (в соответствии с RFC 6020) и использует их структуру и содержание для мониторинга и управления сетевыми элементами.

3 ЧАСТОТНЫЙ ПЛАН

В соответствии с рекомендацией ITU-T G.694.1, для технологии плотного волнового мультиплексирования (DWDM) определена частотная (канальная) сетка.

Оборудование «Алмаз» использует частотную сетку с межканальным интервалом 50 ГГц и применяет систему нумерации каналов, основанную на числовых значениях с возможным суффиксом «e» (even), обозначающим саб-канал шириной 50 ГГц , смещённый относительно центральной частоты основного канала. Например:

– «20» — канал с центральной частотой 192,00 ТГц ;

– «26e» — канал с центральной частотой 192,65 ТГц .

Система поддерживает диапазон каналов с номерами от 21 до 60e включительно.

Таблица 1 — Соответствие номеров каналов и частот / длин волн

Номер канала	Номинальная центральная частота, THz	Приблизительная длина волны, nm
C21	192,10	1560,61
C21e	192,15	1560,20
C22	192,20	1559,79
C22e	192,25	1559,39
C23	192,30	1558,98
C23e	192,35	1558,58
C24	192,40	1558,17
C24e	192,45	1557,77
C25	192,50	1557,36
C25e	192,55	1556,96
C26	192,60	1556,55
C26e	192,65	1556,15
C27	192,70	1555,75
C27e	192,75	1555,34
C28	192,80	1554,94
C28e	192,85	1554,54
C29	192,90	1554,13
C29e	192,95	1553,73

Номер канала	Номинальная центральная частота, THz	Приблизительная длина волны, nm
C30	193,00	1553,33
C30e	193,05	1552,93
C31	193,10	1552,52
C31e	193,15	1552,12
C32	193,20	1551,72
C32e	193,25	1551,32
C33	193,30	1550,92
C33e	193,35	1550,52
C34	193,40	1550,12
C34e	193,45	1549,72
C35	193,50	1549,32
C35e	193,55	1548,91
C36	193,60	1548,51
C36e	193,65	1548,11
C37	193,70	1547,72
C37e	193,75	1547,32
C38	193,80	1546,92
C38e	193,85	1546,52
C39	193,90	1546,12
C39e	193,95	1545,72
C40	194,00	1545,32
C40e	194,05	1544,92
C41	194,10	1544,53
C41e	194,15	1544,13
C42	194,20	1543,73
C42e	194,25	1543,33
C43	194,30	1542,94
C43e	194,35	1542,54
C44	194,40	1542,14
C44e	194,45	1541,75
C45	194,50	1541,35
C45e	194,55	1540,95
C46	194,60	1540,56
C46e	194,65	1540,16

Номер канала	Номинальная центральная частота, THz	Приблизительная длина волны, nm
C47	194,70	1539,77
C47e	194,75	1539,37
C48	194,80	1538,98
C48e	194,85	1538,58
C49	194,90	1538,19
C49e	194,95	1537,79
C50	195,00	1537,40
C50e	195,05	1537,00
C51	195,10	1536,61
C51e	195,15	1536,22
C52	195,20	1535,82
C52e	195,25	1535,43
C53	195,30	1535,04
C53e	195,35	1534,64
C54	195,40	1534,25
C54e	195,45	1533,86
C55	195,50	1533,47
C55e	195,55	1533,07
C56	195,60	1532,68
C56e	195,65	1532,29
C57	195,70	1531,90
C57e	195,75	1531,51
C58	195,80	1531,12
C58e	195,85	1530,72
C59	195,90	1530,33
C59e	195,95	1529,94
C60	196,00	1529,55
C60e	196,05	1529,16

4 ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

4.1 Общие функциональные возможности АСУМ

АСУМ «Алмаз» предоставляет следующие функциональные возможности:

4.1.1 Топология сети

АСУМ предоставляет сведения о структуре сети, общем состоянии её элементов и каналов связи между ними на разных уровнях организации сети.

4.1.2 Контроль неисправностей (Fault Management)

АСУМ агрегирует данные о возникновении нештатных ситуаций на оборудовании сетевых элементов DWDM-сети, полученные от КСЭ, и контролирует весь жизненный цикл аварийных сообщений.

4.1.3 Управление конфигурацией (Configuration Management)

АСУМ предоставляет следующие возможности:

– управление слотовыми устройствами: конфигурирование, получение информации по настройкам и данным измерений;

– создание резервных копий конфигураций сетевых элементов и настроек оборудования в автоматическом и ручном режимах;

– восстановление конфигурации из созданных копий;

– конфигурирование кросс-коммутации, резервирования ODU-соединений (защиты SNCP) и других параметров каналов связи;

– настройка резервирования блоков управления и стекирования шасси;

– поддержка SNMP.

4.1.4 Трейлы

АСУМ предоставляет по трейлам следующую информацию: инвентарные данные, данные по авариям, статистику измерений с интервалами 15 минут и 24 часа, а также список объектов, входящих в каждый трейл. Предусмотрено управление административным состоянием трейлов и входящих в их состав объектов, добавление клиентских трейлов и настройки их конфигурации.

4.1.5 Мониторинг и управление рабочими показателями (Performance Management)

АСУМ производит мониторинг сети и всех её элементов, собирая от КСЭ статистические данные по работе оборудования сетевых элементов DWDM-сети, их нагрузке и эффективности, что требуется для внесения корректировок в эксплуатацию, а также во вспомогательных функциях при планировании, развёртывании, техническом обслуживании и оценке качества работы.

4.1.6 Сбор и обработка инвентарной информации (Inventory)

АСУМ предоставляет сведения об актуальном составе оборудования сетевых элементов DWDM-сети и его инвентарных параметрах.

4.1.7 Поддержка возможностей холодной перезагрузки

АСУМ позволяет выполнить холодную перезагрузку отдельных устройств в шасси.

4.1.8 Управление ПО сетевых элементов (Software Management)

Поддерживается загрузка, установка и обновление программного обеспечения сетевых элементов.

4.1.9 Безопасность и управление доступом (Security)

Включает аутентификацию, авторизацию пользователей и управление доступом к функциям АСУМ на базе ролевой модели.

4.1.10 Системная информация (System)

АСУМ предоставляет следующие возможности:

– контроль состояния сетевых элементов и статуса их синхронизации (NE Control);

– просмотр списка найденных сетевых элементов, которые не находятся под контролем АСУМ, но связаны с узлами под контролем АСУМ (NE Discovered);

– просмотр списка IP-адресов сетевых элементов и их тестирование (IP Addresses);

– просмотр системных сообщений (Task Queue);

– просмотр общего журнала событий (Events);

– просмотр журнала событий по устройствам в сетевых элементах (Device Log);

– конфигурирование системных переменных (АСУМ Configuration).

4.1.11 Управление отчётами

Предоставляется возможность экспорта данных из таблиц разделов АСУМ в файлы формата CSV на локальный компьютер пользователя.

4.2 Топология сети

4.2.1 Общие сведения

Данные топологии содержат схему DWDM-сети, где отображается состояние сетевых элементов (NE) и каналов связи между ними.

Для формирования топологии сети используются OSC/OTS трейлы.

Предусмотрены следующие варианты просмотра топологии:

– по типу каналов связи: OSC, OTS, OMS;

– по доменам/узлам (Domains/Nodes);

– по заданным уровням организации сети («Основной» и т.п.).

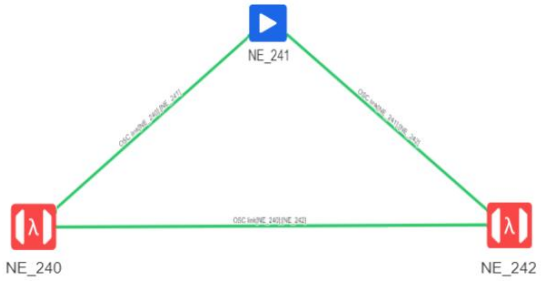

Рисунок 2 — Пример топологии DWDM-сети

4.2.2 Фоновое изображение топологии

АСУМ предоставляет возможность установки фонового изображения для отображения топологии сети. В качестве фона может быть загружено графическое изображение, например карта местности или схема расположения объектов, что позволяет визуализировать сетевые элементы в соответствующих географических или логических локациях.

АСУМ «Алмаз» предоставляет графическое отображение топологии DWDM-сети, включающее состояние сетевых элементов (NE) и каналов связи между ними.

4.2.3 Цветовая индикация объектов

Цветовая индикация объектов на схеме соответствует максимальному уровню критичности аварий, зарегистрированных на данных объектах. Также предусмотрена отдельная цветовая индикация для следующих состояний:

– административное состояние «locked»;

– потеря связи с объектом.

4.2.4 Доступные операции с сетевыми элементами

Для каждого сетевого элемента в интерфейсе топологии доступны следующие функции:

– управление административным состоянием;

– переход к интерфейсу управления сетевым элементом;

– просмотр данных по авариям и событиям;

– переход к настройкам мультиплексирования, кросс-коммутации и защиты SNCP;

– переход к данным ASAP (автоматизированного сбора параметров);

– настройка физических соединений портов;

– удаление сетевого элемента.

Удаление сетевого элемента возможно только при следующих условиях:

а) административное состояние элемента установлено в «locked»;

б) удалены все трейлы, связанные с данным сетевым элементом.

4.2.5 Доступные операции с каналами связи

Для каналов связи предусмотрены следующие действия:

– управление административным состоянием;

– переход к данным о связанных авариях;

– просмотр результатов измерений по OSC (оптическому каналу обслуживания);

– переход к конфигурации OTS (оптической транспортной секции) и OMS (оптической мультиплексной секции).

4.2.6 Управление структурой доменов сети

АСУМ поддерживает организацию сети в виде иерархической структуры доменов. Предусмотрены следующие возможности:

– создание и удаление дочерних доменов;

– добавление и удаление сетевых элементов в составе доменов;

– переход к просмотру и управлению топологии выбранного домена.

4.3 Контроль неисправностей

4.3.1 Общие положения

Функция контроля неисправностей (Fault Management) предусматривает:

– оперативное обнаружение и локализацию аварийных ситуаций;

– определение уровня серьёзности и возможных причин возникновения аварий;

– уведомление обслуживающего персонала;

– обработку и хранение записей о неисправностях с учётом изменения их состояния.

В соответствии с архитектурой АСУМ «Алмаз», контроль неисправностей реализован на трёх уровнях:

а) На уровне сетевых элементов:

– детектирование неисправностей на оборудовании.

б) На уровне управления сетевыми элементами:

– формирование записей об авариях с назначением уровня серьёзности через профиль ASAP;

– управление аварийными сообщениями:

- подтверждение аварий пользователем (acknowledgment);
- ручное и автоматическое закрытие аварий (close/auto close);
- ведение журнала текущих неисправностей;
- хранение архивного списка записей аварий.

в) На уровне управления сетью:

– агрегация данных по авариям со всех сетевых элементов;

– контроль обработки аварийных сообщений;

– бессрочное хранение записей об авариях (в зависимости от аппаратной конфигурации серверов, минимальный срок хранения — 1 год).

4.3.2 Классификация аварийных ситуаций

Аварийные ситуации классифицируются по следующим показателям:

– категория;

– уровень серьёзности;

– влияние на сервис.

Предусмотрены следующие категории неисправностей:

– EQPT (Equipment) — на оборудовании;

– COMM (Communication) — связаны с трафиком/трейлами;

– TCA (Threshold Crossing Alert) — значения наблюдаемых параметров эксплуатации вышли из допустимого диапазона.

Сообщения об аварийных ситуациях классифицируются по следующим уровням серьёзности, представленным в таблице 2.

Таблица 2 — Уровни серьёзности аварийных ситуаций

Уровень серьёзности	Определение	Обработка
Критический (Critical)	Сбой или событие, приводящее к полной потере работоспособности управляемого объекта	Немедленное реагирование
Серьёзный (Major)	Сбой или событие, вызывающее частичную потерю работоспособности управляемого объекта	Срочное выполнение корректирующих действий
Незначительный (Minor)	Сбой или событие, не влияющее на текущую работоспособность объекта, но способное повлиять на неё в будущем	Требуется внимание и планируемое устранение причины
Предупреждение (Warning)	Событие, не влияющее на работоспособность объекта, но несущее диагностическую информацию (например, информация о восстановлении оборудования после аварии)	Диагностика при необходимости и последующая корректировка
Без индикации (Not-alarmed)	Наличие неисправности без формирования аварийного сигнала (например, при административном состоянии объекта — Maintenance или через профиль ASAP)	Реакция не требуется

Дополнительно к уровню серьёзности для аварийных сообщений предусмотрена оценка влияния неисправности на сервис:

– SA (service-affecting) — аварийная ситуация влияет на сервис;

– NSA (non-service-affecting) — аварийная ситуация не влияет на сервис.

4.3.3 Управление аварийными сообщениями

4.3.3.1 Жизненный цикл аварийных сообщений

Для каждого сообщения о неисправности предусмотрен жизненный цикл, отражающий изменения состояния аварийной ситуации.

Состояние аварии определяется как автоматическими системными операциями, так и действиями оператора.

Возможные значения для состояния аварии, определяемые системой:

– авария активна;

– авария очищена.

Оператору доступны следующие действия над аварией:

– подтверждение аварии (alarm acknowledgement) — подтверждение аварийного сообщения указывает, что аварийный сигнал был принят и обработан пользователем.

– закрытие аварии (alarm close) — корректирующие действия были успешно завершены.

– сброс состояния аварии (unack/reopen) — отмена изменения состояния (например, при установке по ошибке или другой причине).

В соответствии с состоянием аварии и действиями оператора устанавливаются следующие статусы:

– текущая авария;

– закрытая авария.

Таблица 3 — Соответствие состояния авария, действий оператора и статуса аварии

Состояние аварии	Действие оператора	Статус аварии
Активна	нет	текущая авария (новая)
Активна	подтверждена (acknowledged)	текущая авария (корректирующие действия предпринимаются)
Активна	закрыта (closed)	текущая авария (новая)
Очищена	нет	текущая авария (очищена без участия оператора)

Состояние аварии	Действие оператора	Статус аварии
Очищена	подтверждена (acknowledged)	текущая авария (очищена в процессе корректирующих действий)
Очищена	закрыта (closed)	закрытая авария, повторная активация аварии приведёт к отмене данного статуса

Для аварийных сообщений в АСУМ ведутся следующие журналы:

– список текущих неисправностей (Current Alarms);

– история изменений по состоянию каждой аварии (Alarm log);

– архив — список закрытых аварий (Historical Alarms).

По каждой аварийной ситуации отсутствуют ограничения по глубине хранения записей (Alarm log).

Раз в сутки (в период 13:00-13:05 по системному времени) на КСЭ выполняется автоматический анализ списка текущих неисправностей на наличие записей, у которых со времени изменения состояния аварии на «очищена» (clear-time) прошло больше суток (24 ч). Найденным записям присваивается статус «закрыта», и они помещаются в архив АСУМ. Таким образом, количество текущих аварий уменьшается на 1, а закрытых — увеличивается на 1.

Архивные записи аварий хранятся бессрочно (зависит от аппаратной конфигурации серверов, базовые требования — 1 год). Они не удаляются ни автоматически, ни вручную.

4.3.3.2 Контроль отчётности об авариях

Пока сетевой элемент находится в состоянии ремонта, тестирования или настройки, он может генерировать большое количество аварийных сообщений, которые не содержат полезной информации для службы эксплуатации. В этом случае их можно скрыть, используя функцию ARC (Alarm Reporting Control) — контроля отчётности об авариях, используемую в соответствии с ITU-T-REC-M.3100.

Функция ARC работает в двух режимах:

– alarm-reporting — отчётность об авариях включена, обычная обработка аварийных ситуаций;

– no-alarm-reporting — отчётность об авариях выключена, сообщения о неисправностях не отображаются в КСЭ и не передаются в АСУМ.

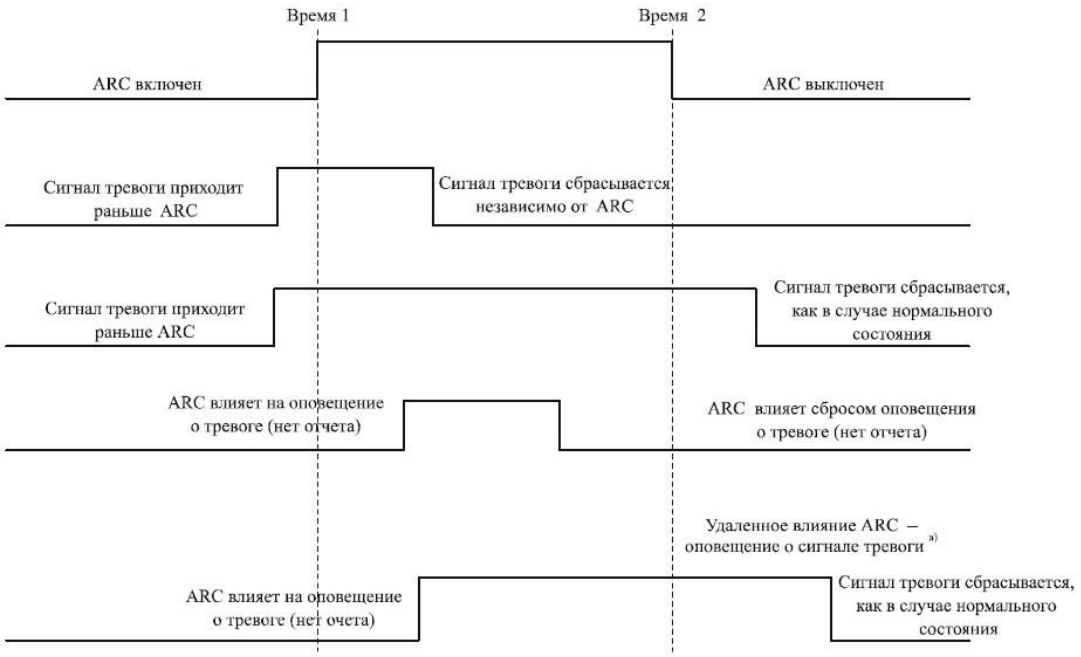

Рисунок 3 — Логика работы ARC при аварийных ситуациях (ITU-T-REC-M.3100)

4.4 Управление конфигурацией

4.4.1 Общие сведения

Функция управления конфигурацией сетевых элементов предусматривает следующие операции:

– управление слотовыми устройствами;

– резервное копирование и восстановление конфигурации;

– мультиплексирование и кросс-коммутация;

– резервирование блоков управления;

– резервирование ODU-соединений (SNCP);

– стекирование шасси;

– синхронизация времени;

– поддержка SNMP.

4.4.2 Синхронизация времени

Установка времени на сетевых элементах синхронизируется с внешними серверами по протоколу NTP (Network Time Protocol).

В качестве внешних серверов точного времени может использоваться АСУМ либо эталонные сервера в сети заказчика.

Предусмотрены следующие параметры NTP:

– IP-адрес основного NTP сервера (Primary NTP server IP address);

– IP-адрес резервного NTP сервера (Secondary NTP server IP address), указывается при необходимости.

Если при настроенном NTP по какой-либо причине возникнет потеря связи с основным или резервным NTP-сервером, в АСУМ будет передано соответствующее аварийное сообщение от КСЭ.

При использовании стекирования шасси настройки NTP производятся только на мастер-шасси, с которым синхронизируются подчинённые шасси. Если внешние NTP-сервера отсутствуют, то локальное время также устанавливается на мастер-шасси, по которому выполняется синхронизация подчинённых шасси.

4.4.3 Поддержка SNMP

Для мониторинга аварий и сбора данных по составу оборудования существует возможность использования протокола SNMPv2 (Simple Network Management Protocol версии 2).

Предусмотрен доступ к следующим данным:

– таблица аварийных ситуаций на сетевом элементе и извещения по её изменениям;

– таблица инвентарной информации по шасси и платам устройств сетевого элемента.

П р и м е ч а н и е — Информация, получаемая по SNMP, доступна только для чтения.

Таблица аварийных ситуаций, передаваемая по *SNMP*, содержит следующие параметры:

– класс объекта;

– объект;

– категория аварии на объекте;

– возможная причина аварии;

– уровень серьёзности;

– влияние на сервис;

– описание аварии;

– дополнительные данные;

– количество возникновений аварии;

– дата и время первого возникновения аварии;

– дата и время последнего возникновения аварии;

– дата и время изменения данных аварии;

– дата и время очистки аварии;

– название учётной записи оператора, обработавшего запись аварии;

– состояние аварии, назначенное оператором;

– комментарий оператора;

– дата и время действий оператора.

Извещения по изменениям в таблице аварий могут быть отправлены получателю с заданным IP-адресом и портом.

Таблица инвентарной информации содержит следующие параметры:

– AID объекта;

– название производителя устройства;

– модель устройства;

– серийный номер устройства;

– версия модели устройства;

– дата выпуска устройства;

– текущая версия ПО устройства;

– дата последнего обновления ПО устройства;

– уникальный номер;

– пользовательская метка.

4.5 Управление слотовыми устройствами

4.5.1 Общие сведения

Управление слотовыми устройствами предусматривает работу со следующим оборудованием, входящим в состав изделия «Алмаз»:

– шасси;

– блоки питания;

– блок вентиляторов;

– блоки управления;

– оптические мультиплексоры/демультиплексоры;

– оптические усилители;

– транспондеры/мукспондеры;

– спектроанализаторы;

– оптические рефлектометры.

Подробная информация доступна в документации на устройства.

Для сетевого элемента и входящих в его состав устройств предусмотрены следующие общие настройки конфигурации:

– административное состояние: undefined, unlocked, locked, maintenance;

– контроль отчётности об авариях: undefined, alarm-reporting, no-alarm-reporting;

– профиль ASA (ASAP);

– метка пользователя.

4.5.2 Резервное копирование и восстановление конфигурации

Операции резервного копирования и восстановления (Backup Restore) включает следующие:

а) просмотр сведений о сетевых элементах:

– проведение первого и последнего на текущий момент резервного копирования;

– название файла последней резервной копии;

– количество операций резервного копирования (общее, автоматические, ручные);

б) параметры автоматического резервного копирования конфигурации сетевого элемента:

– разрешение автоматического резервного копирования;

– количество дней, через которое повторяется операция;

– дата начала операции;

– максимальное число автоматических сохранений, после достижения которого будет удалено самое раннее, чтобы было проведено текущее резервное копирование;

– ручное резервное копирование конфигурации с указанием имени файла;

– восстановление конфигурации сетевого элемента из выбранной резервной копии (как из автоматической, так и сделанной вручную);

– удаление выбранной резервной копии.

4.5.3 Мультиплексирование и кросс-коммутация

Функция мультиплексирования позволяет настраивать схему ODU-мультиплексирования на линейных интерфейсах (NE Management). Схема мультиплексирования зависит от типа устройства.

В качестве примера, для платы агрегатора iTN15600-I-DTQ5DTC доступны следующие варианты настройки мультиплексирования:

ODU2 → ODU1

ODU2 → ODU1 → ODU0

Существует возможность разбить ODU2 на 4 контейнера ODU1, каждый из которых поддерживает разбиение на 2 контейнера ODU0.

С точки зрения информационной модели КСЭ в результате настройки схемы мультиплексирования происходит создание трибутарных портов (TP) на линейном интерфейсе.

Ниже приведён пример настроенной схемы мультиплексирования линейного порта (L1) платы, где на ODU2-интерфейсе созданы 4 ODU1 трибутарных порта (TP1, TP2, TP3, TP4), и первый ODU1 разбит на два ODU0 (TP1-TP1 ODU0, TP1-TP2 ODU0):

Line port L1

ODU-1-1-3-0-L1 ODU2

ODU-1-1-3-0-L1-TP1 ODU1

ODU-1-1-3-0-L1-TP1-TP1 ODU0

ODU-1-1-3-0-L1-TP1-TP2 ODU0

ODU-1-1-3-0-L1-TP2 ODU1

ODU-1-1-3-0-L1-TP3 ODU1

ODU-1-1-3-0-L1-TP4 ODU1

Перед удалением трибутарных портов следует удалить соответствующие ODU кросс-коннекты.

Созданные трибутарные порты возможно удалить.

Выделенные при мультиплексировании контейнеры используются для кросс-коммутации.

Для управления конфигурацией кросс-коннектов (ODU CrossConnections) предусмотрено:

– добавление/редактирование/удаление;

– изменение административного состояния (locked, maintenance, unlocked).

Особенности кросс-коммутации и мультиплексирования общие для мультисервисной платформы «iTN15600»:

– кросс-коммутация возможна только при нахождении клиентских портов (XPC) в административном состоянии unlocked;

– направленность (directionality) кросс-коннектов изменить нельзя. Конфигурация фиксированного кросс-коннекта запрещена;

– если кросс-коннект не поддерживается, то его операционное состояние становится disabled с соответствующим извещением об аварии MEA (mismatch of equipment and attributes);

– коммутация интерфейсов поддерживается только в рамках одного устройства. Поддерживается только коммутация один-к-одному.

Для агрегаторов с кросс-коммутацией:

– поддерживаются только двунаправленные ODU кросс-коннекты. Коммутация клиентских интерфейсов не поддерживается;

– если для HO (high order) ODU интерфейсов сконфигурированы LO (low order) ODU интерфейсы посредством мультиплексирования, то для таких HO ODU интерфейсов коммутация не поддерживается;

– не поддерживается кросс-коммутация ODU2 линейных интерфейсов. Не поддерживается коммутация интерфейсов разной скорости ODU;

– если на клиентском интерфейсе был изменён тип трафика, то клиентский ODU интерфейс может поменять скорость. При этом имеющийся кросс-коннект данного интерфейса будет разорван с извещением об аварии MEA;

– операционное состояние кросс-коннекта становится disabled только при возникновении аварии MEA.

4.5.4 Резервирование блоков управления

При установке на шасси двух блоков управления (CU) один из них будет использован в качестве основного (CU0), а другой — как резервный (CU1).

В случае, когда функцией самодиагностики оборудования обнаружена неисправность на основном блоке управления, производится автоматическое переключение на резервный блок. А после восстановления работоспособности основного блока — автоматическое обратное переключение с резервного блока, для чего требуется включение режима возврата в настройках.

Предусмотрены следующие настройки резервирования блоков управления (Reservation):

1) Режим переключения между блоками управления:

а) автоматический, установлен по умолчанию;

б) ручной, применяется для отладки и тестирования операции резервирования;

2) Режим возврата на основной блок управления при восстановлении его работоспособности:

в) автоматический возврат включён;

г) автоматический возврат выключен;

д) время задержки перед возвратом на основной блок управления при восстановлении его работоспособности;

е) время действия ручного режима переключения между блоками управления, по истечению которого восстанавливается автоматический режим;

ж) выбор основного блока управления при ручном режиме переключения.

4.5.5 Резервирование ODU-соединений (SNCP)

Функционал SNCP (Sub-Network Connection Protection) разработан на основе стандарта ITU-T G.873.1 и реализован как управление защитными группами ODU-интерфейсов.

Защитная группа ODU-интерфейсов состоит из основного и резервного ODU-соединений. Основное — между исходным клиентским портом и линейным портом основной линии трафика, резервное — между исходным клиентским портом и линейным портом, на который будет переключён трафик в случае аварии на основной линии.

Функционал SNCP предусматривает следующие операции:

– создание и настройка резервных ODU-соединений;

– изменение административного состояния защитной группы;

– ручное переключение между основным и резервным ODU-соединением;

– приоритетное переключение между основным и резервным ODU-соединением;

– снятие ручного/приоритетного переключения;

– удаление резервного ODU-соединения.

Особенности применения SNCP для мультисервисной платформы «iTN15600»:

Переключение на резервный ODU-интерфейс будет выполнено автоматически, если на основном интерфейсе возникло нарушение трафика, и поднялись

соответствующие аварии. При этом предусмотрена настройка задержки в мс (Hold-off), чтобы предотвратить переключение в случае кратковременных нарушений.

После очистки аварий на основной линии происходит автоматическое обратное переключение с резервного ODU-интерфейса, если установлен автоматический («revertive») режим возврата, и резервный интерфейс не выбран приоритетным.

- **основной интерфейс соединения (working) должен быть ODU-интерфейсом линейного порта устройства;**
- **создан кросс-коннект между основным интерфейсом и ODU-интерфейсом клиентского порта устройства;**
- **резервный интерфейс соединения (protecting) должен быть ODU-интерфейсом линейного порта устройства;**
- **резервный интерфейс не должен участвовать в кросс-коннекте; основной и резервный интерфейсы должны принадлежать разным портам устройства;**
- **основной и резервный интерфейсы должны принадлежать только одной группе защиты;**
- **скорости основного и резервного интерфейса должны быть одинаковыми; ODU-интерфейс не может быть включён в группу защиты, если для него сконфигурированы трибутарные интерфейсы.**

При установке неверных настроек конфигурации защитной группы или при нарушении условий применения SNCP будет поднята авария MEA.

Таблица 4 — Приоритеты переключения между ODU-интерфейсами в защитной группе

Запрос/состояние	Request/state	Приоритет
Приоритетное переключение	Force Switch (FS)	1 (высший)
Сбой связи	Signal Fail (SF)	2
Ухудшение связи	Signal Degrade (SD)	3
Ручное переключение	Manual Switch (MS)	4
Ожидание возврата на основной интерфейс	Wait-to-Restore (WTR)	5

Запрос/состояние	Request/state	Приоритет
Отсутствие возврата на основной интерфейс	Do Not Revert (DNR)	6
Без запроса	No Request (NR)	(низший)

4.5.6 Трейлы

Базовое определение структуры трейлов и иерархических связей между различными уровнями в оптической транспортной сети (OTN) приведено в рекомендации ITU-T G.709.

В рекомендации представлены логические уровни, которые используются в волоконно-оптических системах со спектральным разделением каналов для передачи различной полезной нагрузки и служебной информации по оптическим волокнам (физической среде).

Трейлы возможно условно разделить на следующие уровни:

– оптический;

– электрический.

Оптический уровень имеет следующую структуру:

Оптические каналы управления (OSC), которые организуются по схеме «точка-точка» между соседними сетевыми элементами вне полосы работы оптических усилителей. Данные трейлы используются для передачи служебной информации и аварийных сообщений по трейлам OTS/OMS/OTSi.

Оптические транспортные секции (OTS), представляют собой соединения «точка-точка» между соседними сетевыми элементами и связаны с групповыми оптическими сигналами вне оптического канала управления (OSC). Точки терминации трейлов OTS — порты оптических усилителей и/или линейные порты мультиплексоров/демультиплексоров.

Оптические мультиплексные секции (OMS), представляют собой логические связи между двумя соседними узлами ADN с точками терминации на линейных портах оптических мультиплексоров/демультиплексоров.

Оптические каналы (OCh/OTSi), представляют собой отдельные оптические несущие с точками терминации на OPT-интерфейсах линейных портов транспондеров узлов ADN.

Электрический уровень представлен набором транспортных контейнеров формата G.709 и уровнем клиентского трейла, а именно:

Трейлы различных транспортных блоков OTU, устанавливаются между линейными портами узлов ADN на OTU-интерфейсах. По скорости равны соответствующим трейлам ODU, при мультиплексировании — HO ODU.

Трейлы различных блоков ODU, устанавливаются между линейными портами узлов ADN на ODU-интерфейсах. Возможно применение мультиплексирования с образованием трейлов HO (High Order) ODU и LO (Low Order) ODU.

Трейлы различных блоков OPU (не используются в информационной модели АСУМ).

Клиентские трейлы — Client, устанавливаются на OPT-интерфейсах клиентских портов транспондеров узлов ADN (сторонах приёма и передачи клиенту).

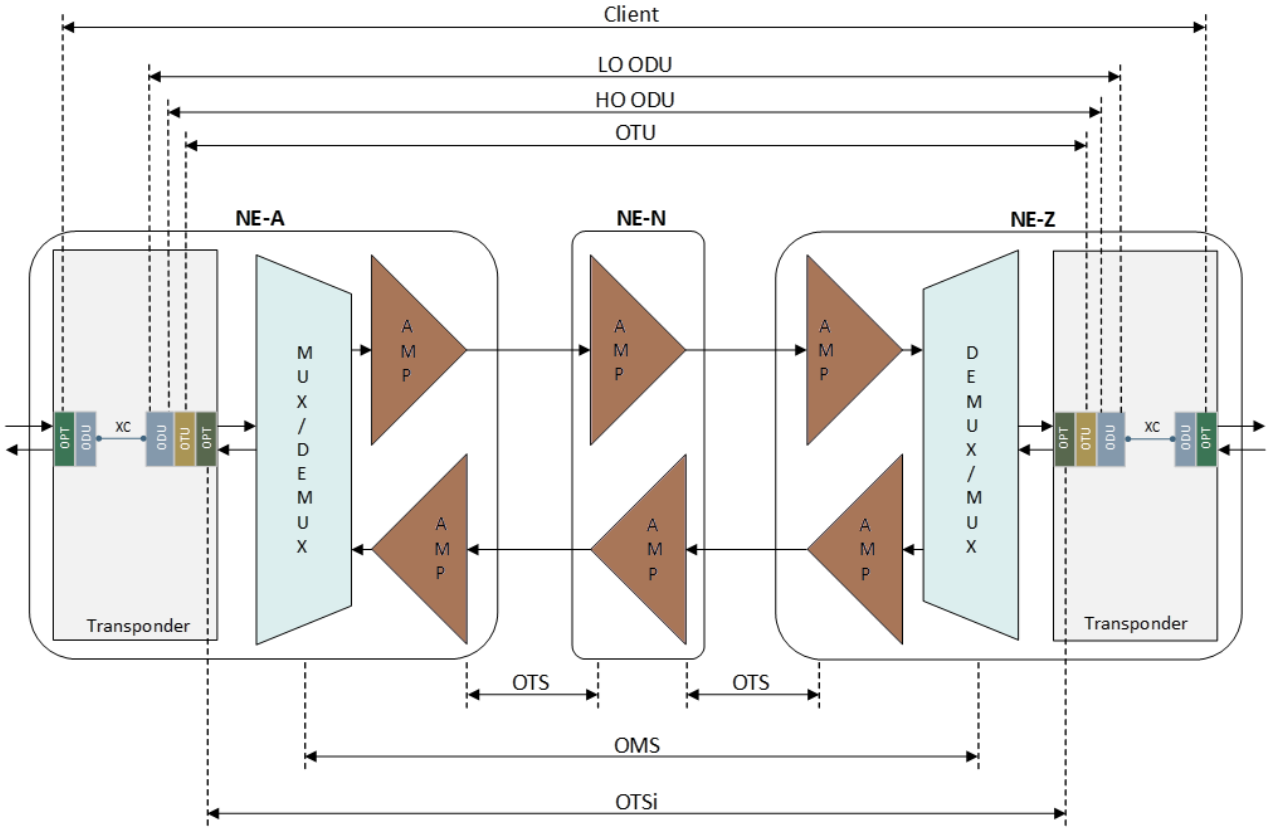

Рисунок 4 — Схема трейлов

Процесс создания трейлов в системе управления автоматизирован за счёт использования механизмов дискавери на уровне контроллера сетевого элемента «LCT». Создание трейлов для каждого из уровней имеет ряд особенностей:

OSC трейлы создаются автоматически (автоматическое определение на уровне оборудования) после настройки на оборудовании IP-адресов на OSC интерфейсах.

OTS трейлы создаются автоматически (автоматическое определение на уровне оборудования), пользователю требуется назначить точки терминации OTS трейлов на портах оборудования.

OMS трейлы создаются автоматически (автоматическое определение на уровне оборудования) после создания соединений OTS интерфейсов. Пользователю требуется назначить точки терминации OMS трейлов на портах оборудования.

OTSi трейлы создаются автоматически (автоматическое определение на уровне оборудования) после привязки линейных портов транспондеров к OTS направлениям.

OTU трейлы создаются автоматически (автоматическое определение на уровне оборудования) с использованием обмена метками в TTI заголовках OTU фрейма.

ODU-HO трейлы создаются автоматически средствами АСУМ (автоматическое определение на уровне системы управления).

ODU-LO трейлы создаются автоматически средствами АСУМ после настройки схемы ODU мультиплексирования на линейных портах транспондеров (автоматическое определение на уровне системы управления).

Client трейлы создаются по запросу со стороны оператора средствами АСУМ. Создание производится в автоматическом режиме для узлов NE-A и NE-Z (как представлено на примере схемы) с учётом доступного ресурса.

При создании клиентского трейла система управления выполняет:

– настройку административного состояния управляемых объектов, входящих в клиентский трейл;

– настройку типа клиентского трафика;

– создание кросс-коннектов.

По каждому трейлу доступны:

– инвенторная информация;

– управление административным состоянием;

– графическое отображение с возможностью управления и с отображением измерений в режиме реального времени;

– список текущих аварийных ситуаций на трейле;

– список объектов, входящих в трейл, с возможностью управления ими;

– статистические данные по трейлу с интервалами измерений 15 мин и 24 часа.

Для клиентских трейлов предусмотрены следующие сценарии:

– создание без использования защиты SNCP;

– создание с использованием защиты SNCP;

– преобразование клиентского трейла без защиты SNCP в трейл с защитой SNCP и наоборот.

Добавление/редактирование клиентского трейла включает следующую конфигурацию:

– режим трафика на трейле;

– тип SNCP (Off — защита SNCP не используется, SNCP-I, SNCP-N, SNCP-S);

– доступные клиентские порты на устройствах сетевых элементов, между которыми устанавливается трейл (A и Z);

– доступные линейные порты на устройствах сетевых элементов A и Z, с которыми производится кросс-коммутация соответствующих клиентских портов;

– резервные линейные порты на устройствах сетевых элементов A и Z для построения трейла с защитой SNCP;

– административное состояние трейла.

4.5.7 Мониторинг и управление рабочими показателями

Функция мониторинга и управления рабочими показателями оборудования (Performance Management) собирает их статистику, что позволяет выявить и устранить проблемы до того, как они окажут влияние на доступность каналов связи или приведут к повреждению оборудования.

К рабочим показателям относятся:

– параметры эксплуатации (например, напряжение, ток, температура, выходная мощность, усиление);

– показатели эффективности (например, продолжительность работы с момента включения/перезагрузки, BER);

– оповещения о выходе значений наблюдаемых параметров из диапазона допустимых значений (TCA — Threshold Crossing Alert).

Для определения источника нерегулярных ошибок, в частности, коротких всплесков битовых ошибок или потерянных фреймов, пакетов, требуется измерять количество таких ошибок в различных местах сети. Такие всплески вызывают высокие проценты ошибочных или потерянных блоков либо вызывают дефекты фрейминга. Контроль неисправностей не может обнаружить такие ошибки, потому что они длятся короткое время и не регистрируются как аварии.

АСУМ собирает с КСЭ статистику, полученную от сетевых элементов на следующих уровнях:

– результаты измерений с сенсоров оборудования;

– параметры работоспособности OTN интерфейсов.

Порядок мониторинга:

Сбор статистики производится с интервалами по 15 минут (recent-15m) с регистрацией минимального, максимального и среднего значения за период.

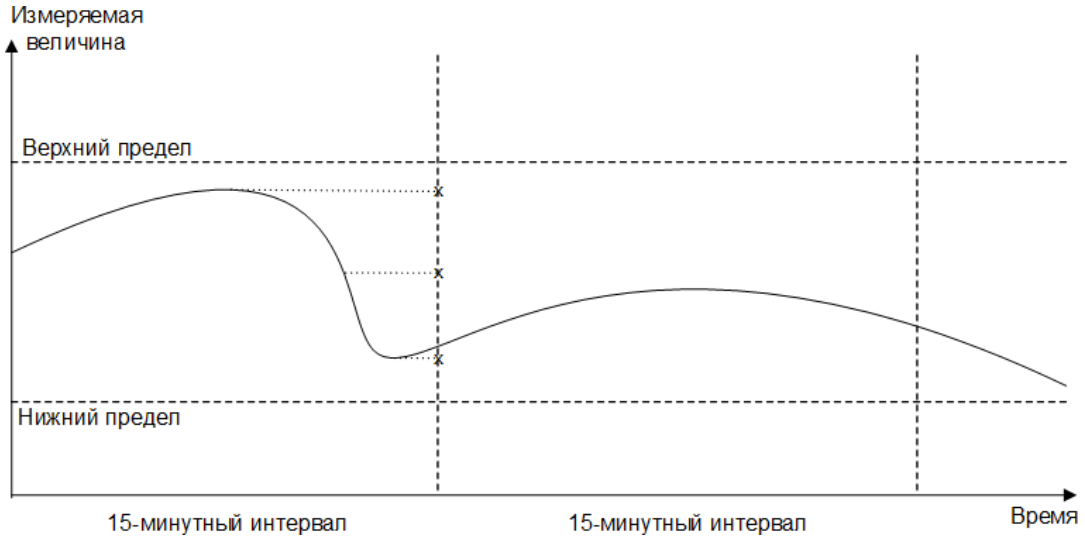

Рисунок 5 — Схема сбора статистики измерений через 15-минутные интервалы

Из данных 15-минутных интервалов формируются интервалы за 24 часа (recent-24h).

Временная сетка 15-минутных интервалов: начало интервала в XX:00, XX:15, XX:30, XX:45 каждого часа.

Временная сетка 24-часовых интервалов: начало интервала в 00:00 ч. по местному времени или UTC.

Началом следующего интервала является конец предыдущего.

Статистика интервалов по 15 минут хранится в течение трёх последних суток, интервалов за 24 часа — бессрочно (зависит от аппаратной конфигурации серверов, базовые требования — 1 год).

4.5.8 Результаты измерений с сенсоров оборудования

Считывание измерений с сенсоров производятся для контроля параметров работы оборудования.

В случае значительного отклонения значений измеряемых величин от их номинальных (паспортных) значений требуется провести техническое обслуживание.

Данные с сетевых элементов передаются в КСЭ, а от них агрегируются в АСУМ.

Предусмотрены следующие измерения:

– сенсоры физических блоков сетевого элемента;

– сенсоры портов и логических интерфейсов сетевого элемента.

4.5.9 Параметры сенсоров физических блоков

а) шасси (CHS):

– доступный запас мощности (power-reserve), Вт;

б) слот в шасси (Slot):

– потребляемая мощность (power-consumption), Вт;

в) блок питания (PS):

– входное напряжение (input-voltage), В;

– выходной ток (output-current), А;

– выходное напряжение (output-voltage), В;

– входной ток (input-current), A;

г) блок вентиляторов (FU):

– ток 3v3 (current-3v3), мА;

– скорость 1-го вентилятора (fan-1-speed), %;

– скорость 2-го вентилятора (fan-2-speed), %;

– скорость 3-го вентилятора (fan-3-speed), %;

– скорость 4-го вентилятора (fan-4-speed), %;

– скорость 5-го вентилятора (fan-5-speed), %;

– скорость 6-го вентилятора (fan-6-speed), %;

– ток 12v (current-12v), мА;

д) блок управления (CU):

– загрузка процессора (cpu-load), %;

– ток 12v (current-12v), мА;

– ток 3v3 (current-3v3), мА;

– загрузка постоянной памяти (disk-space-usage), %;

– текущая продолжительность работы микроконтроллера с момента включения / перезагрузки (mcu-uptime), сек;

– загрузка оперативной памяти (mem-load), %;

– текущая продолжительность работы с момента включения/перезагрузки (uptime), сек;

– напряжение 12v (voltage-12v), В;

– напряжение 3v3 (voltage-3v3), В;

– напряжение батареи (voltage-battery), В;

– температура корпуса (case-temperature), °C;

е) блок транспондера (XPDR), блок агрегатора/блок агрегатора с кросс-коммутацией (MPDR):

– температура FPGA (fpga-temperature)[1], °C;

[1] Параметр зависит от типа устройства, может отсутствовать на некоторых типах.

– текущая продолжительность работы с момента включения/перезагрузки (uptime), сек;

– температура корпуса (case-temperature), °C;

– Плата оптического усилителя (OAMP):

– температура 1-го модуля усилителя EDFA (edfa-module-1-temperature), °C;

– текущая продолжительность работы с момента включения/перезагрузки (uptime), сек;

– температура корпуса (case-temperature), °C;

ж) Модуль усилителя (EA):

– отклонение от референсной входной мощности (delta-from-reference-input-power), дБ;

– усиление (gain), дБ;

– текущее значение тока накачки первого лазера (pump-1-current), мА;

– температура накачки первого лазера (pump-1-temperature), °C;

– текущее значение тока накачки второго лазера (pump-2-current), мА;

– температура накачки второго лазера (pump-2-temperature), °C;

– затухание (attenuation), дБ;

з) оптические мультиплексоры с функцией измерения и программно-управляемыми аттенюаторами:

– температура модуля мультиплексора, °C;

– текущая продолжительность работы с момента включения/перезагрузки (uptime), сек;

– температура корпуса (case-temperature), °C;

и) перестраиваемые мультиплексоры с функцией измерения и программно-управляемыми аттенюаторами:

– температура корпуса (case-temperature), °C;

– текущая продолжительность работы с момента включения/перезагрузки (uptime), сек;

– температура wss модуля мультиплексора, °C;

к) сменные оптические модули (PPM):

– текущее значение тока смещения накачки лазера (pump-bias-current), мА;

– текущее значение тока накачки лазера (pump-current)[1], мА;

– температура накачки лазера (pump-temperature), °C;

– температура корпуса (case-temperature), °C.

Пассивные платы не имеют встроенных средств измерения.

4.5.10 Параметры сенсоров портов и логических интерфейсов

а) OSC:

– выходная мощность (output-power), дБ на мВт;

– входная мощность (input-power), дБ на мВт;

б) EA OAIN:

– входная мощность (input-power), дБ на мВт;

в) EA OAOUT:

– выходная мощность (output-power), дБ на мВт;

– полная выходная мощность (full-output-power), дБ на мВт;

г) XPL:

– выходная мощность (output-power), дБ на мВт;

– входная мощность (input-power), дБ на мВт;

д) XPC:

– выходная мощность (output-power), дБ на мВт;

– входная мощность (input-power), дБ на мВт;

е) OTU:

– утилизация FEC (fec-utilization), %;

[1] Параметр зависит от типа устройства, может отсутствовать на некоторых типах.

4.5.11 Уровень битовых ошибок (BER). Параметры работоспособности OTN интерфейсов

Параметры работоспособности OTN интерфейсов содержат следующие данные по ODU и OTU интерфейсам оборудования:

– *n-es*

– *n-ses*

– *n-bbe*

– *n-uas*

– *f-es*

– *f-ses*

– *f-bbe*

– *f-uas*

– *uas*

– *n-bip8*

– *f-bei*

– *n-ebc*

– *f-ebc*

– *fec-corr-err*

– *fec-uncorr-err*

– *fec-util-min*

– *fec-util-max*

– *ber-min*

– *ber-max*

4.6 Журналирование событий

4.6.1 Общие сведения

Журналирование событий (Events) в АСУМ представляет результаты сбора зарегистрированных на КСЭ и полученных со всех сетевых элементов следующих данных:

– событие старта системы управления;

– события изменения базы данных управляемых объектов:

– автономные события изменения состояния объектов (из журнала исключены события, связанные с историческими авариями);

– изменение конфигурации (по инициативе пользователя);

– действия пользователя (RPC).

Журнал событий хранится в постоянном хранилище (на сервере), глубина хранения не ограничена.

4.6.2 Категории и типы событий

Таблица 5 — Категории и типы событий

Категория	Описание класса	Событие
system-state	Изменение состояния системы управления	system-startup — старт системы управления (КСЭ), формируется на блоках управления (CU) после установки внутреннего управляющего соединения, т.е. не соответствует событию начала старта ПО КСЭ, а сообщает о готовности ПО КСЭ к работе. Предназначено в основном для логирования, т.к. в момент старта системы нет активных подписок на события
database-change	Изменение базы данных. Включает изменения конфигурации в результате действий пользователя и автономные изменения в состоянии управляемого объекта	object-created — создание объекта object-deleted — изменение объекта attribute-value-change — изменение значения атрибута state-change — изменение значения атрибута-состояния
action	Пользовательские действия над управляемыми объектами	action-invoke — вызов процедуры action-success — успешное завершение процедуры action-failure — ошибка при выполнении процедуры

4.6.3 Формат записи о событии

Журнал событий составляют записи, состоящие из следующих параметров:

– *identity* — уникальный идентификатор записи;

– *time* — время наступления события;

– *source* — источник события:

– *resource* — автономное событие;

– *management* — действия пользователя;

– *unknown* — неизвестно;

– *source-user* — имя пользователя (только для действий пользователя);

– *source-address* — адрес, откуда была произведена операция (только для действий пользователя);

– *source-protocol* — протокол, через который была произведена операция (только для действий пользователя);

– *category* — категория события;

– *type* — тип события;

– *object-class* — класс управляемого объекта;

– *object* — управляемый объект;

– *attributes* — таблица атрибутов операции для предоставления пользователям со следующими характеристиками:

– *index* — индекс атрибута;

– *name* — имя атрибута;

– *value* — значение атрибута;

– *description* — текстовое описание события;

– *data* — структурированные данные системных сообщений.

4.7 Сбор и обработка инвентарной информации

АСУМ предоставляет пользователю следующие виды инвентарной информации по всей поддерживаемой сети DWDM:

– по оборудованию сетевых элементов — слотовым устройствам и устройствам *PPM*;

– по трейлам.

По оборудованию доступны следующие данные:

– тип и модель устройства;

– наименование производителя;

– серийный номер;

– версии аппаратного и программного обеспечения.

По трейлам доступны следующие данные:

– тип трейла;

– сетевые элементы на ближнем и дальнем концах трейла;

– порты устройств сетевых элементов, между которыми установлен трейл;

– устройства на сетевых элементах, между которыми установлен трейл;

– в соответствии с типом трейла: скорость/режим трафика/гранулярность мультиплексирования/тип SNCP/FEC/канальная сетка, номер канала и длина его волны.

4.8 Управление ПО сетевых элементов

Функция управления ПО (SWM) сетевых элементов предусматривает следующие операции:

– загрузка/удаление файлов пакетов и бандлов с обновлениями ПО сетевых элементов;

– хранение загруженных пакетов и бандлов в соответствующих репозиториях;

– запуск установки обновлений: как бандла ПО для всех устройств сетевого элемента, так и пакетов ПО для отдельных устройств из бандла.

Контроль состояния обновлений.

В АСУМ предусмотрена возможность загрузки обновлений ПО как для отдельных сетевых элементов и их компонентов, так и для нескольких сетевых элементов одновременно

Файл пакета обновления представляет собой zip-архив, содержащий соответствующий файл прошивки с именем в следующем формате: <имя пакета>-<версия пакета>-<класс устройства>.<расширение>, где:

– *имя пакета* — уникальное для класса устройства имя пакета обновления;

– *версия пакета* — версия ПО, содержащаяся в пакете обновления;

– *класс устройства* — SWM-класс устройства;

– *расширение* — расширение файла, соответствующее типу прошивки, например, *s19*.

Файл бандла обновления — zip-архив, содержащий json-файл с данными обновления и с именем в формате: bundle-<версия>.json, где *версия* - ревизия/версия бандла ПО.

При загрузке файл скачивается во временную папку, затем выполняются следующие автоматические операции:

1) Распаковка zip-архива.

2) Проверка целостности содержимого архива.

3) Перенос пакета/бандла в репозиторий после успешной распаковки и проверки целостности.

4) Обновление информации о пакете/бандле на уровне северного интерфейса.

Если в базе уже есть данный пакет/бандл, то его повторная загрузка не допускается. Для проведения повторной загрузки требуется удалить его из репозитория.

Информация о пакетах ПО, доступных для установки на оборудование сетевых элементов, представлена в виде таблицы с записями вида: <имя пакета>-<версия пакета>-<целевая платформа пакета>. Например: *cne-1.3-sa-rc1-1-g17e8095ea.*

Информация о бандлах ПО представлена в виде таблицы со следующими параметрами:

– имя бандла, формируется как: cne-bundle-<имя бандла>; например: *cne-bundle-v1.1.1*;

– имя пакета, например: *cne-sa*;

– версия пакета;

– класс устройства, к которому принадлежит данный пакет, например: *n2ucpu*;

– имя пакета ПО для данного модуля;

– версия пакета ПО для данного модуля;

Статус бандла:

– *active* — бандл активен, т.е. его ПО успешно установлено и используется;

– *standby* — бандл не используется;

– *installing* — для бандла запущена установка обновления ПО, идёт процесс установки пакетов;

– *installed* — для бандла запущена установка обновления ПО, процесс установки пакетов завершён;

– *activating* — для бандла запущена установка обновления ПО, идёт процесс активации пакетов;

– *active-waiting-for-cfm* — для бандла запущена установка обновления ПО, процесс активации пакетов завершён, ожидается подтверждение активации для завершения процесса установки;

– *failed* — операция с бандлом завершилась ошибкой;

– *rollingback* — производится откат установки данного бандла;

– *corrupted* — файл описания бандла повреждён и не может быть использован для операций обновления, подлежит удалению;

– дополнительная информация о статусе бандла;

– имя родительского бандла — информация о пакетах, отсутствующая в текущем бандле, наследуется из бандла, имя которого указано в данном параметре.

Информация об установленных версиях ПО содержит следующие параметры:

– класс устройства, на котором запущено ПО;

– класс объекта, на котором запущено ПО;

– идентификатор объекта, на котором запущено ПО;

– UUID объекта, на котором запущено ПО;

– название пакета ПО;

– версия пакета ПО;

– хэш версии ПО, значение зависит от реализации;

– дата и время сборки, значение зависит от реализации;

– комбинация варианта/позиции пакета (primary или backup) и его состояния активности (active или standby), например: primary_active или backup_standby.

4.9 Безопасность и управление доступом

Предусмотрены следующие варианты авторизации в АСУМ:

– только локально;

– только посредством RADIUS-сервера;

– если не удалось локально, то через RADIUS-сервер;

– если не удалось через RADIUS-сервер, то локально.

Для авторизации через RADIUS-сервер требуется задать список серверов, каждый из которых конфигурируется со следующими настройками:

– IP-адрес;

– порт;

– ключ аутентификации (secret).

Безопасность и управление доступом (Security *and* Access Management) в АСУМ предусматривает следующие операции:

– контроль подключений к АСУМ;

– ведение журнала безопасности;

– создание/редактирование/удаление учётных записей пользователей;

– назначение прав доступа пользователей.

4.9.1 Безопасность

Функция безопасности предусматривает следующий контроль подключений к АСУМ:

– срок действия учётных записей пользователей;

– срок действия заданного пользователем пароля, по истечению которого потребуется установить новый;

– допускаемое количество неверных попыток авторизации подряд, после которых авторизация будет заблокирована на заданное время;

– допускаемое время неактивности в рабочей сессии пользователя, после которого сессия будет автоматически завершена, и потребуется повторная авторизация для продолжения работы;

– допускаемое количество одновременных сессий пользователя (в разных окнах/закладках интернет-обозревателя);

– разрешённые IP (маски) для подключения по учётной записи.

В установках учётных записей пользователей предусмотрен флаг активности, снятие которого блокирует подключение с использованием учётной записи.

Имя пользователя и пароль назначаются системным администратором. При первом подключении пользователю будет предложено изменить пароль.

Журнал безопасности АСУМ содержит следующую информацию:

– дату и время последнего подключения;

– продолжительность рабочей сессии;

– IP, по которому произведено подключение;

– интернет-обозреватель и ОС, на которых произведено подключение;

– разделы, к которым обращался пользователь.

4.9.2 Управление доступом

Управление доступом в АСУМ осуществляется в соответствии с ролевой моделью.

Учётные записи пользователей распределены по группам (ролям). Предусмотрены роли по умолчанию, и системные администраторы могут создавать произвольные роли.

Таблица 6 — Роли пользователей по умолчанию в АСУМ

Роль	Права доступа
Мониторинг (MonitoringEngineer)	Только просмотр следующих данных: • топология сети, состав сетевых элементов и трейлы; • текущие и архивные записи аварий; • конфигурация сетевых элементов; • рабочие показатели; • журнал событий; • инвенторная информация; • установленные обновления ПО сетевых элементов
Контроль (NetworkEngineer)	Права роли «Мониторинг» + управление следующими данными: • настройка топологии и трейлов; • изменение состояния текущих аварийных сообщений; • изменение конфигурации каналов связи; • настройка TCA в рабочих показателях; • просмотр списка пользователей и ролей
Сетевое администрирование (NetworkAdmin)	Права роли «Контроль» + управление следующими данными: • загрузка, установка и контроль обновлений ПО сетевых элементов; • управление конфигурацией сетевых элементов и трейлов; • просмотр очередей задач; • просмотр логов системы
Администрирование безопасности (SecurityAdmin)	Права роли «Мониторинг» + управление следующими данными: • добавление/редактирование/удаление учётных записей пользователей, присвоение ролей; • добавление/редактирование/удаление ролей; • просмотр журналов системы; • просмотр журналов безопасности; • изменение состояния текущих аварийных сообщений

В АСУМ созданы учётные записи пользователей по умолчанию, представленные в таблице 7.

Таблица 7 — Учётные записи пользователей по умолчанию в АСУМ

Имя пользователя	Роль	Назначение
monitor	MonitoringEngineer	Получение данных о состоянии сети и сетевых элементах, авариях, рабочих показателях, событиях и обновлениях ПО
Neteng	NetworkEngineer	Общие настройки сетевых элементов, управление аварийными сообщениями
netadmin	NetworkAdmin	Полная настройка сети и сетевых элементов, управление обновлением ПО оборудования
Admin	SecurityAdmin	Управление учётными записями пользователей и их ролями, просмотр системных журналов и журналов безопасности

Роли и учётные записи по умолчанию не могут быть удалены.

5 СТЕКИРОВАНИЕ ШАССИ

Цель стекирования — создание сетевого элемента с функционалом, расширенным за счёт добавления устройств в подчинённых шасси. Определение сетевого элемента и его функции подробно представлено в рекомендациях ITU-T M.3010, ITU-T G.874. В сети DWDM такой сетевой элемент имеет один IP-адрес для подключения внешней системы управления, так же, как и сетевые элементы из одного шасси.

В сетевом элементе может использоваться до шести шасси. При этом одно шасси получает роль мастера, остальные — подчинённых, которые управляются через мастер-шасси.

Для стекирования, в зависимости от реализуемой схемы, используются порты L1 и L2 блока управления и порты 9-16 блока iTN15600-E-D8U.

В случаях, когда стекирование не применяется, OSC каналы терминируются на портах L1/L2 блоков управления мастер шасси. При стекировании шасси, OSC-каналы терминируются на портах на портах 1-8 блока iTN15600-E-D8U (либо двух блоков при необходимости резервирования).

Для организации стекирования используются интерфейсы 1000 Base-T. Для этого в блоки управления устанавливаются модули SFP-T, подключения выполняются медными патчкордами.

Последовательность действий для организации стекирования:

1) До выполнения действий по стекированию:

– порты L1 и/или L2, в зависимости от реализуемой схемы стекирования (с резервированием или без) на блоках управления переводятся в режим trun;

– выполнить физическое подключение шасси в стек в соответствии с требуемой схемой.

2) После соединения в стек производится настройка конфигурации каждого шасси по отдельности локально в LCT, используя LCT-порт:

– устанавливается тип шасси: мастер/подчинённое;

– задаются параметры номера стойки/шасси (rack/subrack) локального агента (local-agent);

– управление данными конфигурации всего сетевого элемента производится на мастер-шасси;

– конфигурация каждого шасси задаётся в соответствии с его номером стойки/шасси (rack/subrack);

– на мастер-шасси устанавливаются параметры связи с подчинёнными шасси (remote-agents);

– на подчинённых шасси устанавливаются параметры связи с мастер-шасси (master-agent).

3) Выполнить настройку физических линков в LCT.

Подключение двух портов блока управления в один iTN15600-E-D8U не допускается.

Шасси в стек подключаются по схеме «звезда». Каждый блок управления (включая резервный при его наличии на шасси) соединяется с каждым iTN15600-E-D8U. Если в мастер-шасси только один блок iTN15600-E-D8U, то для соединения используется только один L-порт блока управления.

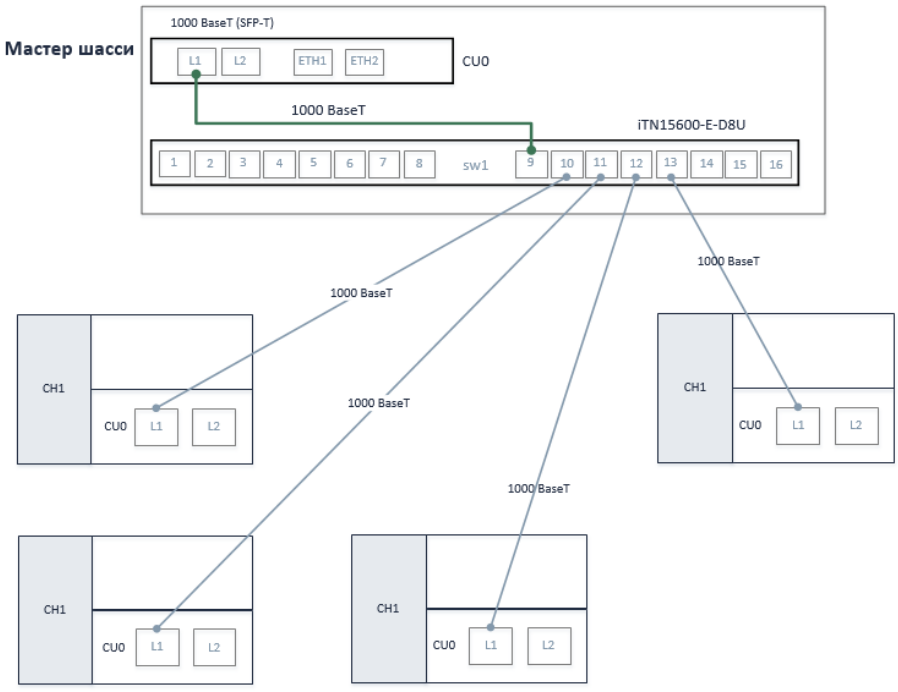

Рисунок 6 — Схема соединения шасси в стек без резервирования

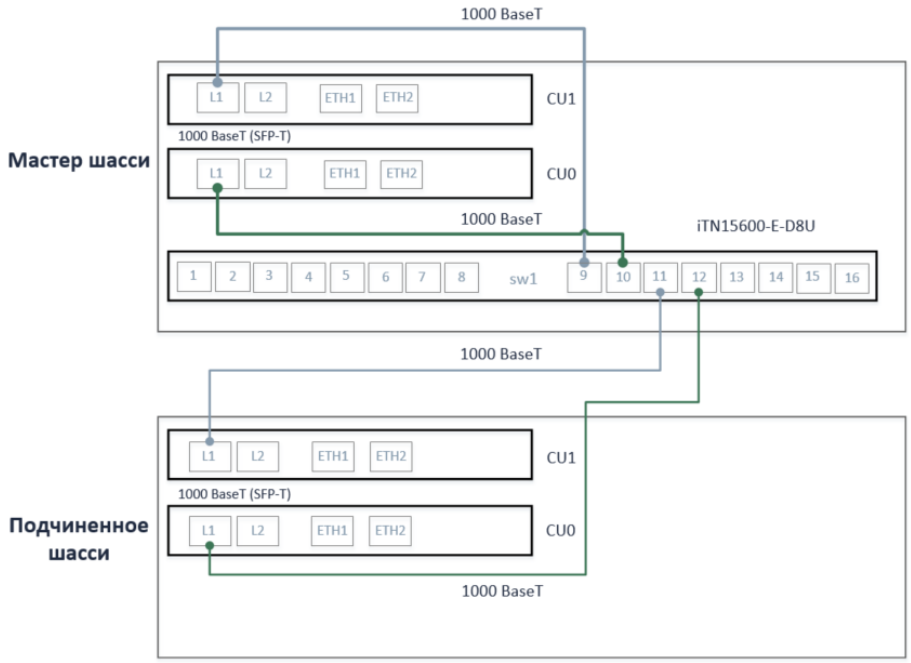

Рисунок 7 — Схема соединения шасси в стек с резервированием

Ниже приведён пример организации стекирования шасси с резервированием внутренних соединений:

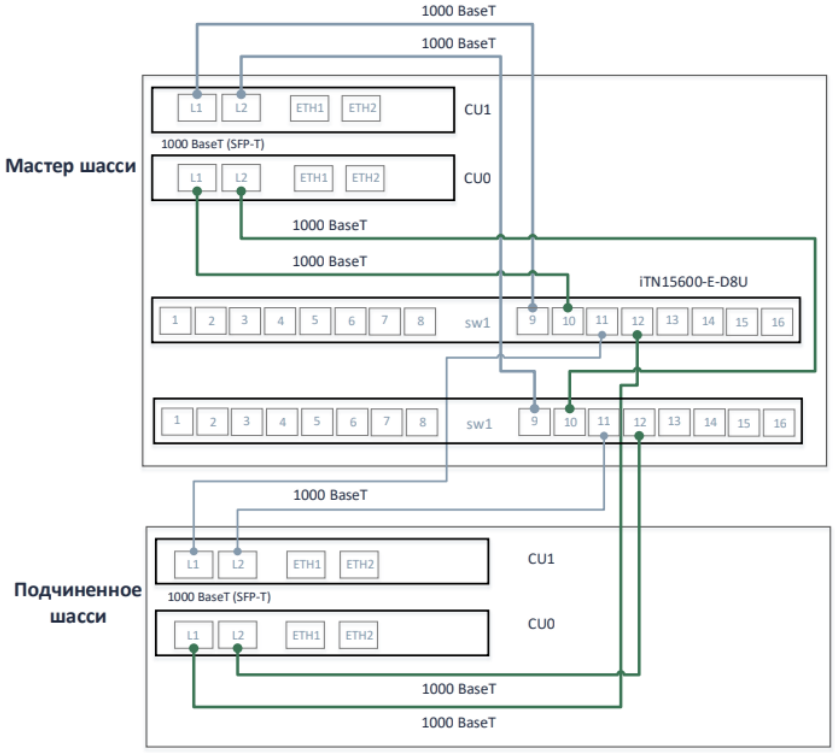

Рисунок 8 — Схема соединения шасси в стек с резервированием внутренних соединений

После соединения шасси в стек согласно выбранной схеме коммутации следует перейти непосредственно к настройке стекирования шасси в Алмаз-ТУ.

Подробное описание и последовательность процесса настройки стекирования шасси приводится в разделе 5 Руководства пользователя ПО «Алмаз», Версия 1.0.

6 ПРОГРАММНАЯ АРХИТЕКТУРА

АСУМ использует открытую архитектуру программного обеспечения с модульной структурой под управлением операционной системы Linux.

Для работы с АСУМ рекомендуется использовать интернет-обозреватели на базе Chromium (такие как Google Chrome, Yandex Browser, Opera, Microsoft Edge и др.).

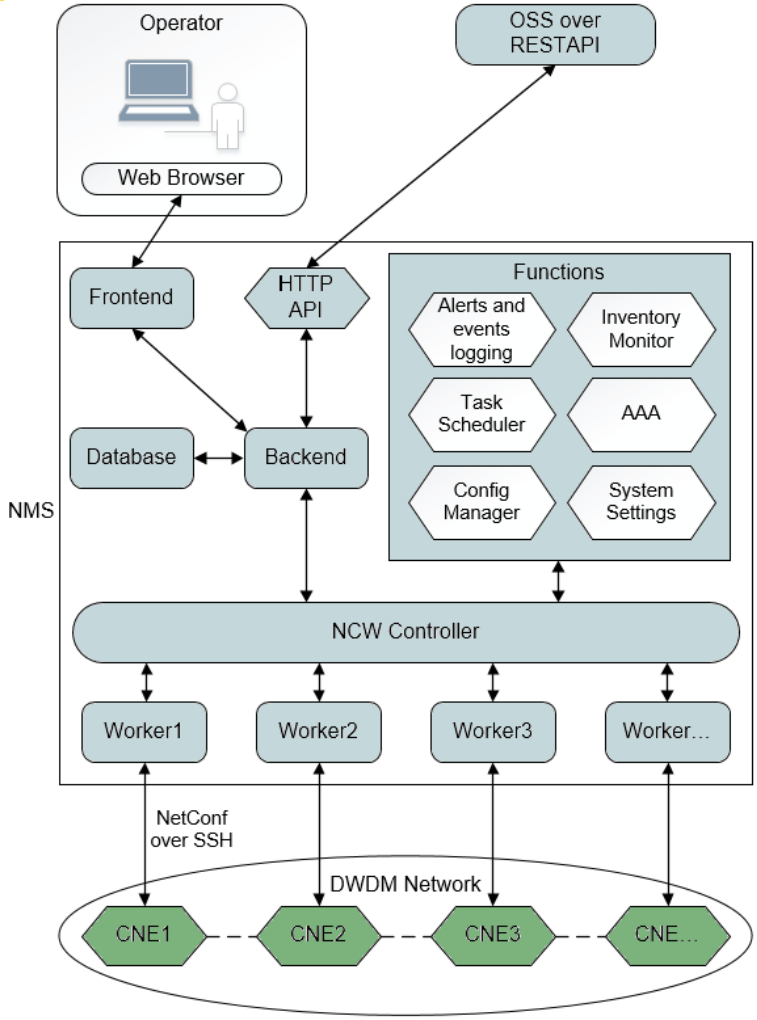

Рисунок 9 — Программная архитектура АСУМ

Содержание схемы:

Operator, Web Browser — рабочая станция оператора с интернет-обозревателем, который используется для подключения к АСУМ;

OSS over RESTAPI — северный интерфейс для подключения OSS/BSS систем;

Структура АСУМ:

Frontend — клиентский пользовательский web-интерфейс;

HTTP API — интерфейс взаимодействия с OSS/BSS системами на базе протокола HTTP;

Backend — сервисы взаимодействия с функционалом АСУМ, контроллером NCW и базой данных;

Database — распределённая база данных;

NCW Controller — контроллер *NCW*, управляющий модулями Worker, взаимодействующими с контроллерами сетевых элементов сети DWDM;

Worker — модуль, собирающий данные с назначенного ему КСЭ и обрабатывающий очередь соответствующих задач;

Функционал:

Alerts and events logging — логирование неисправностей, рабочих показателей и событий;

Inventory Monitor — сбор инвентарных данных физических и логических объектов;

Task Scheduler — контроль очередей системных задач;

AAA — модуль аутентификации и авторизации для контроля доступа пользователей при подключении по протоколам HTTP и SSH;

Config Manager — управление конфигурацией;

System Settings — системные настройки;

CNE — КСЭ сетевого элемента в DWDM-сети, подключенный к *АСУМ* посредством протокола SSH, обеспечивающего шифрование, сжатие и контроль передаваемых данных.

7 ТРЕБОВАНИЯ К АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

7.1 Серверное оборудование

Для корректного функционирования АСУМ предусмотрены следующие минимальные требования к серверному оборудованию:

Таблица 8 — Минимальные требования к серверному оборудованию

Оборудование	Минимальные требуемые характеристики
Процессор	Intel Xeon или аналогичный AMD с 4-мя ядрами
Оперативная память	Объём 16 Гб
Накопитель SSD	2×500 Гбайт
Жёсткий диск	4×1 Тбайт
Внешний интерфейс	Ethernet с пропускной способностью 1 Гбит/с

Приведённой конфигурации сервера достаточно для обслуживания от 1 до 25 сетевых элементов.

7.2 Клиентское оборудование

Для корректного функционирования АСУМ предусмотрены минимальные требования к клиентскому оборудованию, представленные в таблице 9.

Таблица 9 — Минимальные требования к клиентскому оборудованию

Оборудование	Минимальные требуемые характеристики
Процессор	Intel Core i5 или аналогичный AMD с 2-мя ядрами
Оперативная память	Объём 8 Гб
Внешний интерфейс	Ethernet с пропускной способностью 100 Мбит/с

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

ПО	—	программное обеспечение
DWDM	—	технологии плотного волнового мультиплексирования (Dense Wavelength Division Multiplexing)
АСУМ	—	автоматизированная система управления и мониторинга
SSH	—	сетевой протокол прикладного уровня (Secure Shell)
HTTP	—	протокол передачи гипертекста (HyperText Transfer Protocol)
SNCP	—	резервирование/защита на уровне соединения подсетей с внутренним контролем (Sub-Network Connection Protection)
OTDR	—	оптический рефлектометр (Optical Time Domain Reflectometer)
ARC	—	контроль отчётности об авариях (Alarm Reporting Control)

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводи тельного докум. и дата	Подп.	Дата
	измененн ых	замененны х	новых	аннулиров анных					