

1. Назначение программы

ПУМ должна обеспечивать:

- Взаимодействие компонентов ККП, управление процессом передачи данных и управление сетевым распределением ключей ККП;
- Автоматизированную диагностику ККП, сбор статистики о её функционировании, состоянии ПКРК и ПДУ, в том числе с использованием мониторинга посредством протокола SNMP.
- ПУМ должна передавать исходные данные о всех событиях (выход значений параметров системы за пределы допустимого) с использованием брокеров сообщений в зонтичную систему индустриального партнёра. Формирование необходимых действий по событиям выполняет зонтичная система индустриального партнёра.
- ПУМ должна передавать исходные данные об использовании ресурсов с использованием брокера сообщений в систему биллинга индустриального партнёра. Формирование действий на основе данных ПУМ выполняет система биллинга индустриального партнёра.
- Выдачу команд в ПДУ на формирование и распределение квантово-защищенных ключей (КЗК) в автоматизированном режиме с помощью графической системы управления.
- Централизованный мониторинг заданных параметров ККП, с возможностью подачи сигналов в случае возникновения любых нештатных ситуаций в сфере ответственности ПУМ.
- Централизованное хранение программных компонент ПУМ (программы, конфигурационные файлы, описания) и

| | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Име. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
| | | | | |
| | | | | |
| | | | | |

| | | | | | |
|------|------|----------|-------|------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Лист |
| | | | | | 4 |

2. Условия применения ПУМ

ПУМ должна устанавливаться как на выделенные серверы на основе архитектуры x86_64, так и в виртуальной среде.

Средства вычислительной техники ПУМ должны поддерживать следующие режимы:

- Рабочий – плановое функционирование в соответствии с назначением;
- Тестовый (или сервисный) – проверочный режим, когда выполняется тестирование ПО и/или оборудования;
- Аварийный – режим, в котором некоторые части функционала могут быть недоступны, хотя в целом функционирование продолжается. Например, при выходе из строя одного из двух блоков питания функционирование может продолжаться.
- Загрузка ОС в локальный сервер управления – по сети.
- Управление и мониторинг в ПУМ – по каналу, защищенному СКЗИ.

Рабочие места администраторов модулей ПУМ должны содержать средства обеспечения защищенного канала управления и мониторинга для обмена информацией между АРМ администратора ПУМ и другими модулями ПУМ.

Каждый пользователь ПУМ должен иметь свой ключевой контейнер.

Аппаратные компоненты ПУМ должны функционировать в условиях для группы 4 ГОСТ 15150-69 исполнения УХЛ и группы 2 ГОСТ 21552-84, в частности:

- температуры окружающей среды: от +5°C до +40°C;
- относительной влажности до 80% при температуре +20°C;
- атмосферного давления от 84 до 107 кПа (от 630 до 800 мм рт. ст.) при отсутствии в воздухе хранилища агрессивных примесей.

| | | | | | | | | | | | | | | |
|------|------|----------|-------|------|------|------|----------|-------|------|------|------|----------|-------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Изм. | Лист | № докум. | Подп. | Дата | Изм. | Лист | № докум. | Подп. | Дата |
| | | | | | | | | | | | | | | |

3. Описание задачи ПУМ

3.1. Подсистема управления

3.1.1. Модуль управления ПДУ и КРК

Функционально модулем решаются следующие задачи:

- Взаимодействие с ПДУ и КРК;
- Управление ПДУ и КРК;
- Производится запись событий в электронный журнал.

3.1.2. Модуль управления трафиком, топологией и технологическими параметрами ККП

Функционально модулем решаются следующие задачи:

- Обеспечивается доступ к сетевым и вычислительным устройствам системы для осуществления процесса управления ими;
- Обеспечивается безопасность передачи данных в соответствии с уровнем необходимой защищенности;
- Формируется топология сети и вычислительных устройств системы в представлении, соответствующем контексту использования, в достаточной мере обеспечивающем технологический процесс;
- Производится автоматический расчет емкости сети передачи данных с оценкой возможности построения канала передачи пользовательских данных в необходимом объеме;
- Производится оценка технической возможности подключения новых потребителей без ухудшения параметров и уровня обслуживания для подключённых ранее потребителей;
- Реализуется выдача диагностических сообщений;
- Производится запись событий в электронный журнал.

| | | | | | | | | | | | | | | |
|------|------|----------|-------|------|------|------|----------|-------|------|------|------|----------|-------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Изм. | Лист | № докум. | Подп. | Дата | Изм. | Лист | № докум. | Подп. | Дата |
| | | | | | | | | | | | | | | |

- прием данных о результатах обработки событий в привязке к инцидентам и работам для информирования администратора ПУМ. ВС направляет в модуль мониторинга данные о всех работах и/или инцидентах, связанных с событиями, которые модуль мониторинга оборудования ранее отправил в ВС.

Для взаимодействия с ВС используется API интерфейс через брокер сообщений Kafka (служебный модуль коммутации данных) и Apache ServiceMix.

3.3. Подсистема технического учёта

3.3.1. Модуль учета оборудования

Модуль учета оборудования решает следующие задачи:

- сбор данных учета оборудования;
- заполнение места расположения, координат, номеров коммерческих заказов и прочей дополнительной информации;
- составление базы знаний по возникающим проблемам;
- создание объектов, загруженных из ВС с возможностью внесения описания.

Для решения данных задач решено использовать заимствованную систему GLPI. Для обнаружения состава оборудования ККП и его загрузки в GLPI использовался плагин Fusioninventory.

В качестве языка разработки дополнений к программному обеспечению использовался python в среде Linux. Для создания объектов в GLPI, загруженных из ВС, использовался программный пакет для python «glpi-sdk- python».

Модуль учета оборудования взаимодействует с ВС, которая предназначена для обеспечения единого непрерывного жизненного цикла управления технологическими сетями передачи данных. Компоненты,

| | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Изн. № подл. | Подп. и дата | Взам. инв. № | Изн. № дубл. | Подп. и дата |
| | | | | |

| | | | | | |
|------|------|----------|-------|------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Лист |
| | | | | | 10 |

оборудование, соединения компонентов описываются во ВС. Все описания из ВС реплицируются в модуле учета оборудования. Модуль учета оборудования постоянно отслеживает реальный состав оборудования и соединений с базой оборудования и соединений и в случае расхождения формировать событие в модуле мониторинга оборудования ККП.

Модуль учета оборудования обеспечивает передачу следующих данных во ВС:

- регулярно передачу инвентаризационных данных, полученных с оборудования.

Модуль учета оборудования обеспечивает прием следующих данных из ВС:

- прием данных о типах, моделях и экземплярах конфигурационных единиц, соединениях между конфигурационными единицами.

Для взаимодействия с ВС используется API интерфейс через брокер сообщений Kafka (служебный модуль коммутации данных ВС) и Apache ServiceMix.

3.3.2. Модуль учета логических ресурсов

Модуль учета логических ресурсов решает следующие задачи:

- сбор данных учета логических ресурсов;
- заполнение дополнительной информации;
- получение актуального статуса установленного программного обеспечения и лицензий;
- создание объектов, загруженных из ВС с возможностью внесения описания.

| | |
|--------------|--------------|
| Инв. № подл. | Подп. и дата |
| Взам. инв. № | Инв. № дубл. |
| Подп. и дата | Подп. и дата |

| | | | | | |
|------|------|----------|-------|------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Лист |
| | | | | | 11 |

3.4.2. Модуль обработки запросов API в реальном времени

Модуль обработки API в реальном времени должен работать по следующей схеме:

- Прием запроса в формате REST (HTTP GET/POST, JSON) от ВС.
- Обработка запроса с использованием диагностической информации с соответствующих подсистем и компонентов .
- Возврат полученных в ходе обработки данных инициатору запроса.

Модуль выполняет прием запросов от ВС, его обработку с использованием информации подсистем и компонентов ККП, возврат полученных в ходе обработки данных инициатору запроса. При этом взаимодействие осуществляется через очередь сообщений AMQP брокера RabbitMQ. Очередь входящих сообщений прослушивается модулем на предмет поступающих запросов, в теле которого содержится идентификатор ответной очереди, в которую направляется результат обработки.

В качестве языка разработки используется python 3 в среде Linux. Для взаимодействия с брокером RabbitMQ используется библиотека pika для python 3.

3.5. Подсистема контроля доступа

Подсистема контроля доступа ПУМ обеспечивает:

- аутентификацию, авторизацию и аудит учетных записей.
- валидацию доверенных устройств – взаимодействие между АРМ и серверами ПУМ, серверами ПУМ и серверами ПДУ, серверами ПДУ и аппаратной частью ПДУ, устройствами для консольного доступа к компонентам в аварийных.
- доступ пользователей в систему через графический интерфейс автоматизированного рабочего места;

| | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Име. № подл. | Подп. и дата | Взам. инв. № | Име. № дубл. | Подп. и дата |
| | | | | |

| | | | | | |
|------|------|----------|-------|------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Лист |
| | | | | | 13 |

- регистрацию пользователя (администратора) в системе с использованием подтверждения со стороны администратора и назначения группы, в которую включён пользователь. Данные пользователя автоматически вносятся в OpenLDAP;
- контроль учетных данных пользователей;
- внесение изменений в учётные данные пользователей через графический интерфейс;
- определение принадлежности пользователей к группам;
- запись событий входа и взаимодействия с системой в системные логи;
- блокировка и разблокировка пользователей;
- автоматизация создания учетных данных в системах OpenLDAP и Kerberos для дальнейшего использования устройствами системы;
- интеграция в модули управления и мониторинга квантовой коммуникационной платформы;
- единую точку входа по протоколу CAS 2.0, в которой используются данные из OpenLDAP.

3.6. ЛСУ и агенты ЛСУ

Операционная система на базе ОС Linux на ЛСУ решает задачи предоставления среды выполнения для агентов ЛСУ. Агенты ЛСУ решают задачи выполнения локального мониторинга, управления подсистемами ПДУ и КРК, инвенторизации оборудования а так же контроля доступа, и по сути являются компонентами соответствующих подсистем, выполняющимися на ЛСУ:

- Агент модуля управления ПДУ и КРК описан в п. 3.1.1
- Агент модуля мониторинга п 3.2.1 и 3.2.2
- Агент модуля технического учета описан в п 3.3.1 и 3.2.2
- Агент подсистемы контроля доступа описан в п 3.5

| | | | | |
|------|------|----------|-------|------|
| Изм. | Лист | № докум. | Подп. | Дата |
| Изм. | Лист | № докум. | Подп. | Дата |
| Изм. | Лист | № докум. | Подп. | Дата |
| Изм. | Лист | № докум. | Подп. | Дата |
| Изм. | Лист | № докум. | Подп. | Дата |

3.7. ПО АРМ Администратора

Автоматизированное рабочее место администратора (АРМ администратора) реализует функции взаимодействия с администраторами с помощью графического интерфейса. Графический интерфейс реализуется в браузере администратора и может быть выполнен на рабочем месте – ПК, имеющем доступ к сети управления. Серверная часть ПО АРМ администратора выполняется на ЦУМ и позволяет производить авторизацию пользователей, отображать окна графического интерфейса с учётом доступных ролей в системе за счёт использования подсистемы контроля доступа.

ПО АРМ администратора обеспечивает:

- генерацию окон графического интерфейса
- отображение окон в браузере администратора по запросу
- отправку действий пользователя на исполнение подсистеме управления
- отображение результата выполнения действий подсистемой управления в графическом виде
- интеграцию с подсистемой мониторинга и технического учёта для отображения их данных

| | | | | | | | | | |
|------|------|----------|-------|------|--------------|--------------|--------------|--------------|--------------|
| Изм. | Лист | № докум. | Подп. | Дата | Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата |
|------|------|----------|-------|------|--------------|--------------|--------------|--------------|--------------|

4. Входные и выходные данные

4.1. Подсистема управления

4.1.1. Модуль управления ПДУ и КРК

Входными данными модуля управления ПДУ и КРК являются данные, поступающие по протоколу AMQP со стороны интерфейса оператора (АРМ) а также ответы на запросы полученные от СПДУ

Выходными данными являются ответы на запросы со стороны интерфейса администратора (АРМ), отправляемые по протоколу AMQP, а также запросы к СПДУ.

4.1.2. Модуль управления трафиком, топологией и технологическими параметрами ККП

Входные данные модуля представляют собой набор параметров, определяющих построение коммуникационного канала, передаваемые по протоколу HTTP со стороны интерфейса оператора (АРМ).

Выходными данными модуля являются ответы в контексте полученных запросов, и отображаемых в интерфейсе оператора (АРМ).

4.2. Подсистема мониторинга

4.2.1. Модуль мониторинга ПДУ и КРК

Входные данные модуля представляют собой параметры команды на запрос состояния ПДУ и КРК, запросы от агента мониторинга и данные мониторинга ПДУ и КРК. Получив запрос от агента мониторинга, сервер отправляет ответ на этот запрос. Данные мониторинга ПДУ и КРК поступают на Zabbix сервер, запущенный в ВМ на ЦУМ. Zabbix сервер обрабатывает эти данные и заносит их в базу данных PostgreSQL.

Выходные данные модуля представляют собой результаты выполнения команд мониторинга ПДУ и КРК, ответы на запросы агента мониторинга, а

| | | | | |
|--------------|--------------|--------------|--------------|--------------|
| Име. № подл. | Подп. и дата | Взам. инв. № | Име. № дубл. | Подп. и дата |
|--------------|--------------|--------------|--------------|--------------|

| | | | | | |
|------|------|----------|-------|------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Лист |
| | | | | | 16 |

Выходными данными модуля экспорта данных во ВС являются:

- Файл конфигурации в текстовом формате, кодировка Unicode.
- Данные из Баз данных подсистемы мониторинга и подсистемы технического учета, передаваемые во ВС через брокер сообщений Kafka (служебный модуль коммутации данных ВС) и Apache ServiceMix, кодировка Unicode.
- Журнал логирования в текстовом формате, кодировка Unicode.

4.4.2. Модуль обработки запросов API в реальном времени

Входными данными модуля обработки запросов API в реальном времени являются структуры формата JSON, описывающие тело запроса и идентификатор очереди, в которую необходимо отправить ответ.

Выходными данными модуля обработки запросов API в реальном времени являются сообщения формата JSON, поступающие через очередь сообщений Rabbitmq. Формат выходных данных модуля обработки запросов API в реальном времени – JSON, кодировка текста Unicode.

4.5. Подсистема контроля доступа

Входные данные подсистемы контроля доступа содержат в себе идентификатор запроса для проверки сессии пользователя, либо логин и пароль для создания сессии. Формат входных данных подсистемы контроля доступа – запрос HTTPs, кодировка текста Unicode.

Выходными данными подсистемы контроля доступа выступают статус сессии пользователя и данные о группах пользователя в формате HTML, кодировка текста Unicode.

| | |
|--------------|--------------|
| Инв. № подл. | Подп. и дата |
| Взам. инв. № | Инв. № дубл. |
| Подп. и дата | |

| | | | | | |
|------|------|----------|-------|------|------|
| Изм. | Лист | № докум. | Подп. | Дата | Лист |
| | | | | | 20 |

4.6. ЛСУ и агенты ЛСУ

Входными и выходными данными являются данные в форматах соответствующих подсистем, протоколы передачи данных так же описана в соответствующих подсистемах

- Агент модуля управления ПДУ и КРК описан в п. 4.1.1
- Агент модуля мониторинга п 4.2.1 и 4.2.2
- Агент модуля технического учета описан в п 4.3.1 и 4.3.2
- Агент подсистемы контроля доступа описан в п 4.5

4.7. ПО АРМ Администратора

Входными данными ПО АРМ Администратора является тестовая строка запроса и поле данных запроса. По результатам обработки строки производится выбор страницы для генерации и отображения. Формат входных данных ПО АРМ Администратора – запрос HTTPs, кодировка текста Unicode.

Выходными данными ПО АРМ Администратора являются страницы формата HTML для отображения в браузере, кодировка текста Unicode.

| | | | | | | | | | | |
|--------------|--------------|--------------|--------------|--------------|--|--|--|--|--|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата | | | | | | Лист |
| | | | | | | | | | | 21 |
| Изм. | Лист | № докум. | Подп. | Дата | | | | | | |

Обозначения и сокращения

| | |
|---------|---|
| AMQP | Advanced Message Queuing Protocol |
| API | Application programming interface |
| CWDM | Coarse Wavelength Division Multiplexing |
| EVM | Extended Verification Module |
| IMA | Integrity Measurement Architecture |
| IMA/EVM | Integrity Measurement Architecture and Extended Verification Module |
| QBER | Quantum Bit Error Rate |
| QBER | Quantum Bit Error Rate |
| QKD | Quantum key distribution |
| SLA | Service Level Agreement |
| SNMP | Simple Network Management Protocol |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| YAML | Yet Another Markup Language |
| АРМ | Автоматизированное рабочее место |
| БД | База данных |
| ВМ | Виртуальная машина |
| КЗК | Квантово-защищенные ключи |
| ККП | Квантовая коммуникационная платформа цифровой экономики |
| КРК | Квантовое распределение ключей |
| ЛСУ | Локальный сервер управления |
| ПДУ | Подсистема организации доверенных опорных узлов квантовой связи |
| ПКРК | Подсистема квантового распределения ключей |
| ПО | Программное обеспечение |

Подл. и дата

Инв. № дубл.

Взам. инв. №

Подл. и дата

Инв. № подл.

| | | | | |
|------|------|----------|-------|------|
| Изм. | Лист | № докум. | Подп. | Дата |
|------|------|----------|-------|------|

Лист

22

| | |
|------|---|
| ПУМ | Подсистема управления и мониторинга квантовой сетью |
| СКЗИ | Система защиты информации |
| ЦУМ | Центр Управления и Мониторинга |
| | |

| | | | | | | | | | | | | | |
|--------------|--------------|--------------|--------------|--------------|------|------|------|------|------|------|------|------|------|
| Инв. № подл. | Подп. и дата | Взам. инв. № | Инв. № дубл. | Подп. и дата | Изм. | Изм. | Изм. | Лист | Лист | Лист | | | |
| | | | | | | | | | | | Лист | Лист | Лист |
| | | | | | | | | | | | | | |

