УТВЕРЖДЕН

БЮЛИ.00131-01 13 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС «ПРОГРАММНО-ОПРЕДЕЛЯЕМАЯ ЛАБОРАТОРИЯ «ПОЛАТОР»

Описание программы

БЮЛИ.00131-01 13 01

Листов 52

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
А-3860	10.06.2021			

2021 Литера

АННОТАЦИЯ

Настоящий документ содержит общие сведения о назначении и условиях применения программного комплекса «Программно-определяемая лаборатория «ПОЛАТОР» БЮЛИ.00131-01 (далее по тексту – ПК или программа) и предназначен для обеспечения функционирования и эксплуатации программы.

Документ оформлен в соответствии с требованиями ГОСТ 19.402-78.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. ПК разработан на языке программирования C++ (кроссплатформенный код – Windows, Linux) в экосистеме «CI/NightBuild/AutoBuild/AutoTest/CodeStandart» на основе «GitLab».

1.2. ПК реализован на основе двухзвенной архитектуры распределенных систем и включает в себя следующие программные компоненты:

– программный компонент «ПОЛАТОР-Клиент» (далее – Клиент), предназначен для разработки СПО, реализующего следующие процессы:

а) взаимодействие с измерительной и управляющей аппаратурой;

б) сбор, обработка, отображение информации и результатов расчетов;

в) моделирование отдельных объектов и АС;

– программный компонент «ПОЛАТОР-Сервер» (далее – Сервер), предназначен для:

а) хранения данных СПО;

б) выдачи данных по запросам Клиента;

в) организации работы Клиентов в многопользовательском режиме.

1.3. Программа может использоваться в следующих организациях:

– предприятия по производству высокотехнологичной промышленной продукции РЭА и электронного приборостроения;

– учебные заведения и специализированные лаборатории, использующие элементы прототипирования в своей работе;

– поставщики ПО, ведущие разработку программно-аппаратной продукции и использующие программу в качестве инструмента прототипирования.

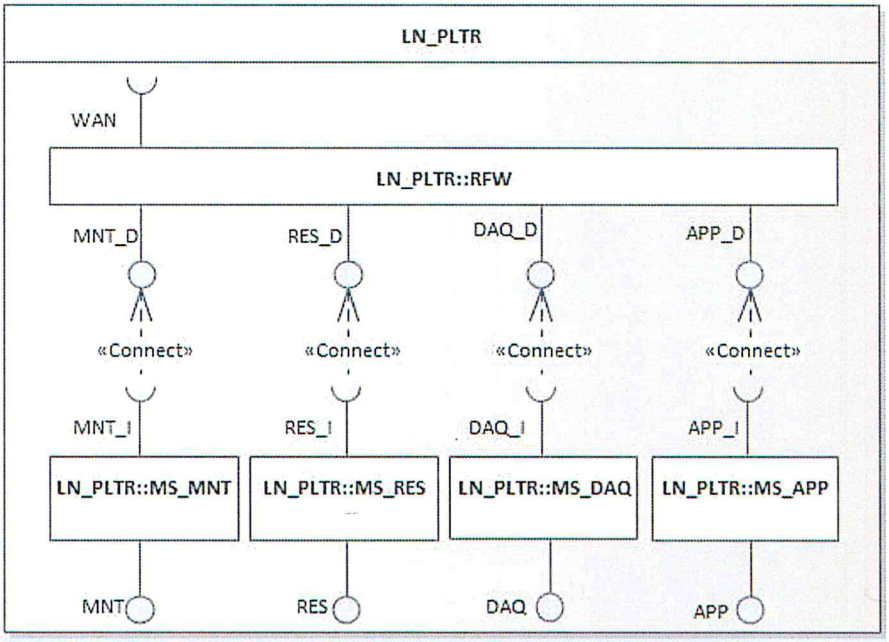
1.4. Программа поставляется на оптическом компакт-диске CD-R или DVD-R.

2. ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1. Принципы функционирования

2.1.1. Сетевые и коммуникационные средства

2.1.1.1. Функционирование Сервера предусматривается в сетевом окружении с архитектурой в соответствии со структурной схемой, приведенной на рис. 1.



LN_PLTR - Комплексный сегмент локальной вычислительной сети из состава программного комплекса «Программно-определяемая лаборатория «ПОЛАТОР».

LN_PLTR::RFW - Модуль маршрутизации и сетевого экранирования.

LN_PLTR::MS_MNT - Управляемый сетевой коммутатор (MS) сегмента.
Функциональная группа MNT (Maintenance).
Системное администрирование, обслуживание и ремонт аппаратных и программных средств.

LN_PLTR::MS_RES - Управляемый сетевой коммутатор (MS) сегмента.
Функциональная группа RES (Resources).
Системные сервисы и ресурсы, ресурсы файловой системы, системы управления базами данных, WEB-сервисы.

LN_PLTR::MS_DAQ - Управляемый сетевой коммутатор (MS) сегмента.
Функциональная группа DAQ (Distributed data acquistion).
Обеспечение ввода-вывода данных, поддержка специализированных коммуникационных протоколов со сторонними системами.

LN_PLTR::MS_APP - Управляемый сетевой коммутатор (MS) сегмента.
Функциональная группа APP (Application, functional).
Обеспечение комунникационной среды прикладных задач и коммуникация с автоматизированными рабочими местами(клиентскими приложениями).

Рис. 1 – Архитектура и сетевое окружение Сервера

2.1.1.2. Локальный сегмент вычислительной сети предусматривает функциональное разделение по группам (таблица 1).

Таблица 1 – Функциональные группы

Функциональная группа	Выполняемые функции	Характерные протоколы
MNT	системное администрирование, обслуживание и ремонт аппаратных и программных средств	IPsec, SNMP, RDP, IPMI
RES	системные сервисы и ресурсы, ресурсы файловой системы, системы управления базами данных, WEB-сервисы	iSCSI, SMB/CIFS, FCP, TCP
DAQ	обеспечение ввода/вывода данных, поддержка специализированных коммуникационных протоколов со сторонними системами	SCPI, VISA, PROFINET, OPC UA
APP	обеспечение коммуникационной среды прикладных задач и коммуникация с АРМ (клиентскими приложениями)	UDP, TCP

2.1.1.3. Функциональное разделение сетей обеспечивается с помощью следующих вариантов технических решений:

– применение выделенных сетевых коммутаторов для функциональных групп сегмента сети;

– использование технологий VLAN при совместном использовании единого аппаратного сетевого коммутатора.

2.1.1.4. ПК предусматривает интеграцию территориально распределенных компонент в единый комплекс путем интеграции распределенных сегментов ЛВС в соответствии со структурной схемой, изображенной на рис. 2.

Территориальное объединение сетей осуществляется на основе следующих технологий:

– выделенных частных коммуникационных линий связи;

– каналов публичных сетей (WAN) на основе технологий VPN.

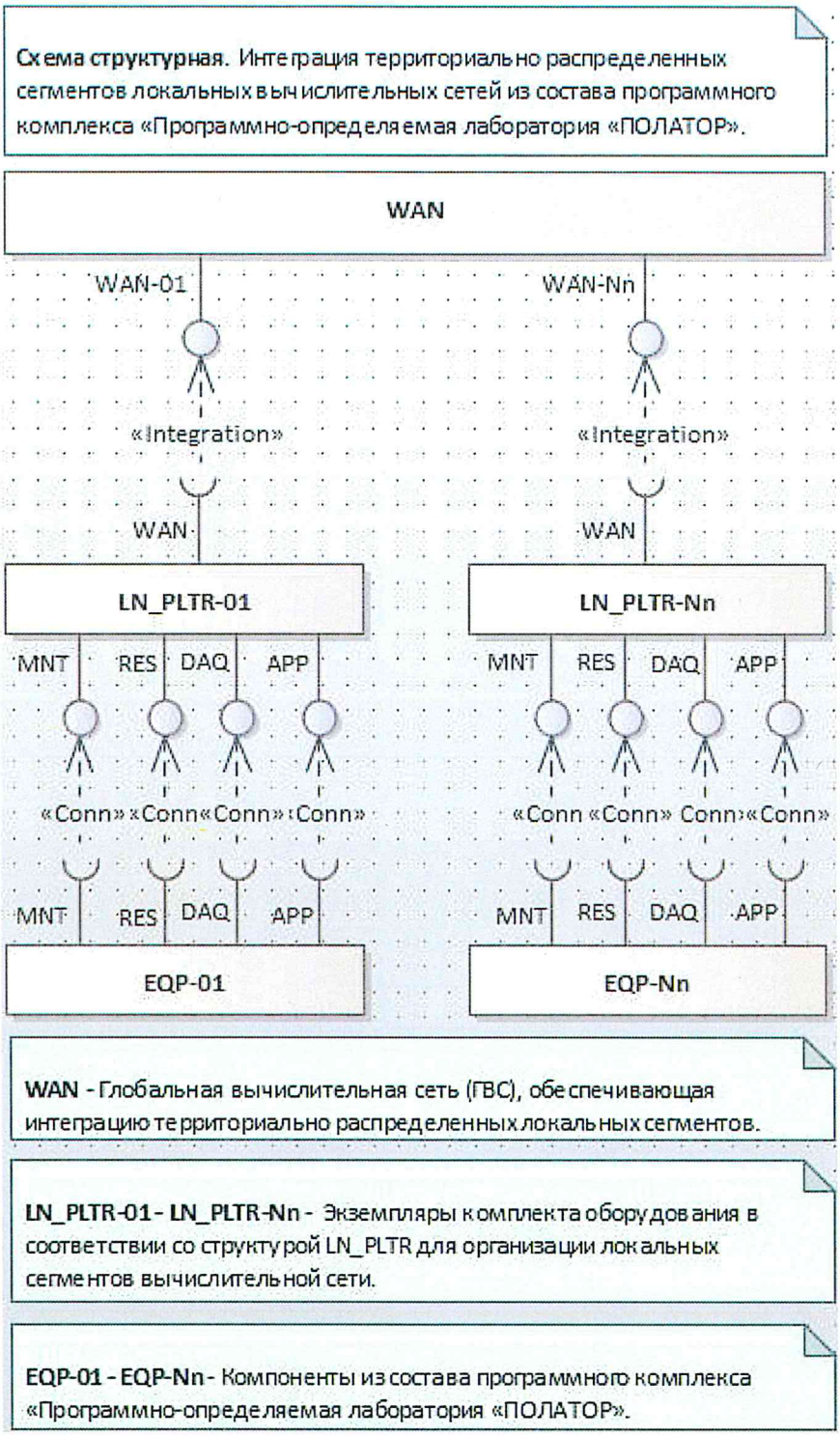


Рис. 2 – Интеграция территориально распределенных компонент

2.1.1.5. В качестве физического уровня сетей и коммуникационного оборудования предусмотрено использование следующих технологий:

– кабельные проводки категории не ниже CAT-5E;

– оптоволоконные кабельные линии;

– беспроводные каналы связи.

2.1.1.6. Требования информационной безопасности обеспечиваются за счет:

– предоставления необходимой степени физической защиты доступа к сетевому и коммуникационному оборудованию;

– обеспечения соответствующих регламентов на организационном уровне эксплуатации;

– применения технологий маршрутизации и сетевого экранирования;

– функционального разделения;

– интеграции сетевого оборудования в централизованную систему управления информационной безопасностью.

2.1.1.7. Обеспечение пропускной способности канала связи и балансировка нагрузки осуществляется путем:

– предоставления соответствующего количества физических каналов и линий связи;

– применения аппаратных средств портов соответствующей пропускной способности;

– параллельного использования нескольких портов в режиме балансировки нагрузки (teaming mode).

2.1.1.8. Обеспечение надежности и отказоустойчивости осуществляется путем:

– предоставления избыточности ресурса («холодное» или «горячее» резервирование) как на уровне портов, так и сетевых коммутаторов;

– применения аппаратных средств портов с соответствующими показателями надежности;

– параллельного использования нескольких портов в режиме балансировки нагрузки (teaming mode);

– обеспечения плановых превентивных регламентов обслуживания;

– обеспечения соответствующего уровня регламентов внеплановых ремонтных работ;

– обеспечения соответствующих регламентов на организационном уровне эксплуатации в части физического доступа к оборудованию;

– обеспечения соответствующей категории электропитания;

– обеспечения соответствующего уровня пожарной безопасности.

2.1.1.9. Обеспечение масштабируемости осуществляется путем изменения количества:

– физических каналов и линий связи;

– коммуникационных портов существующих сетевых коммутаторов;

– сетевых коммутаторов.

2.1.1.10. Обеспечение управляемости осуществляется путем:

– использования управляемых сетевых коммутаторов;

– интеграции сетевого оборудования в централизованную систему управления конфигурацией;

– интеграции сетевого оборудования в централизованную систему управления ИТ-инфраструктурой.

2.1.2. Аппаратные средства

2.1.2.1. ПК предусматривает функциональное разделение на компоненты, показанные на рис. 3.

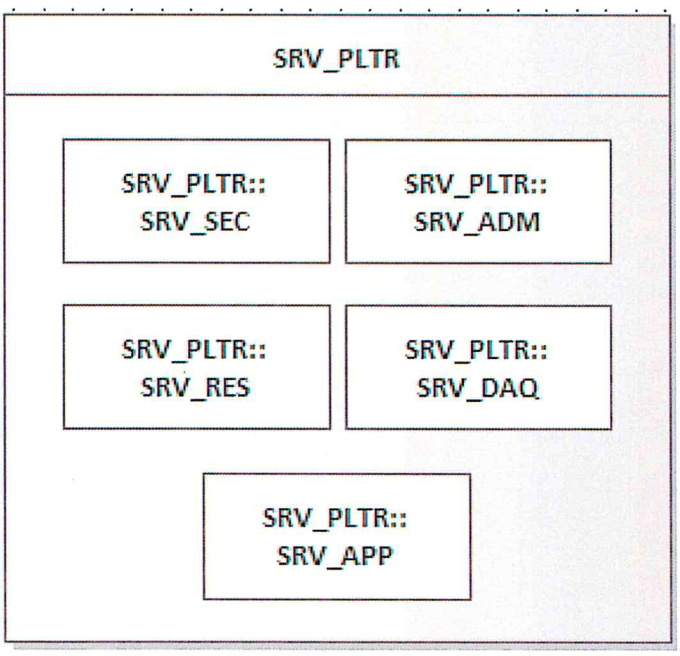


Рис. 3 – Функциональное разделение на компоненты

2.1.2.2. Краткая спецификация назначения функциональных компонент:

– SRV_SEC:

а) управление лицензиями;

б) обеспечение локальных сервисов информационной безопасности;

в) обеспечение интеграции в вышестоящую централизованную систему управления информационной безопасности;

– SRV_ADM:

а) обеспечение локальных сервисов системного администрирования, обслуживания и ремонта аппаратных и программных средств;

б) обеспечение интеграции в вышестоящую централизованную систему управления конфигурацией;

в) обеспечение интеграции в вышестоящую централизованную систему управления ИТ-инфраструктурой;

– SRV_RES:

а) обеспечение интеграции:

1) распределенных ресурсов файловых систем;

2) распределенных ресурсов СУБД;

3) распределенных ресурсов WEB-сервисов;

б) обеспечение централизованного доступа к локальным и интегрированным ресурсам:

1) файловой системы со стороны SRV_SEC, SRV_ADM, SRV_DAQ, SRV_APP;

2) систем управления базами данных со стороны SRV_SEC, SRV_ADM, SRV_DAQ, SRV_APP;

3) WEB-сервисов со стороны SRV_SEC, SRV_ADM, SRV_DAQ, SRV_APP;

– SRV_DAQ:

а) обеспечение ввода/вывода данных и представление их в форме тегов;

б) обеспечение коммуникации по специализированным протоколам и представление данных обмена в форме тегов;

в) предоставление доступа к тегам со стороны SRV_APP в различных режимах (циклические чтения/запись, чтение по обновлениям, запись

по запросу и т.п.);

– SRV_APP:

а) обеспечение работы с моделями в режиме дизайна;

б) обеспечение выполнения моделей в различных режимах (шаговый, циклический и т.п.);

в) обеспечение режима отладки моделей;

г) обеспечение отображения результатов выполнения модели;

д) обмен данными с АРМ, построенными на основе программного компонента «ПОЛАТОР-Клиент».

2.1.2.3. Функционирование компонент из состава Сервера предусмотрено в следующих вариантах:

– конфигурация HW_CFG01 (рис. 4). SRV_SEC, SRV_ADM, SRV_RES, SRV_DAQ, SRV_APP установлены и выполняются на одном физическом или виртуальном сервере SP00. Используется в случае применений с низкой нагрузкой.

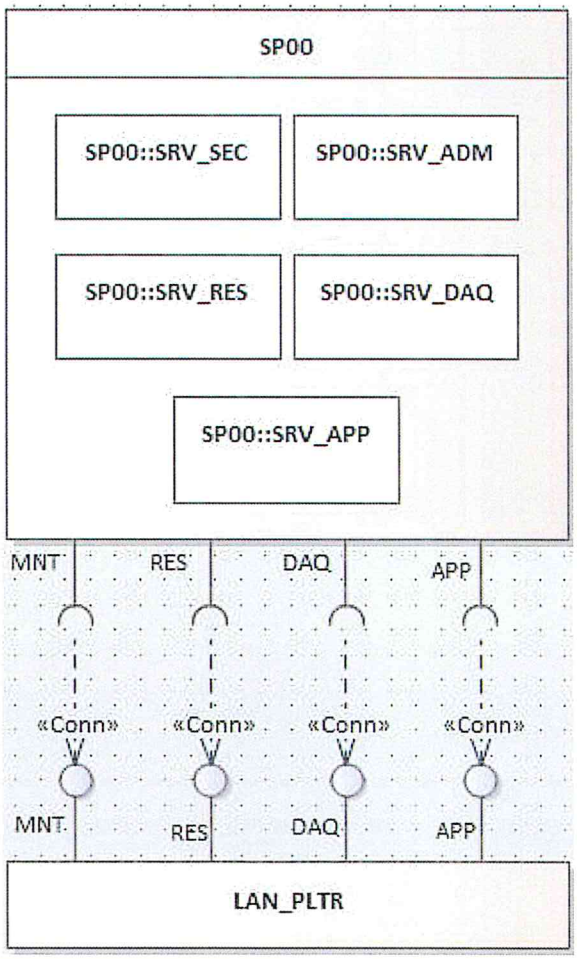


Рис. 4 – Конфигурация HW_CFG01

Требования к аппаратному обеспечению SP00:

а) процессор: не хуже Intel® Core™ i5 не ниже 9-го поколения. Рекомендуется использование аппаратных платформ на базе Intel® Xeon® не ниже 2-го поколения;

б) оперативная память: не менее 4 Гб DDR3. Рекомендуется использование DDR4 16 Гб;

в) объем жесткого диска: не менее RAID10 512 Гб. Рекомендуется использование локальной СХД объемом 2048 Гб;

г) ЛВС (LAN): не менее 1 x 1 Мбит/с. Сетевое соединение используется для интеграции с другими экземплярами ПК;

д) свободный USB (не ниже спецификации 2.x) – порт для подключения лицензионного ключа;

е) порт IPMI;

ж) операционная система:

1) Вариант 01: лицензионная ОС Microsoft Windows 10 Professional x64, СУБД PostgreSQL;

2) Вариант 02: ОС Debian GNU/Linux x64 10, СУБД PostgreSQL;

– конфигурация HW_CFG02 (рис. 5). Распределение компонентов происходит следующим образом:

а) SRV_SEC, SRV_ADM – установлены и выполняются на выделенном физическом или виртуальном сервере SP01;

б) SRV_RES, SRV_DAQ – установлены и выполняются на выделенном физическом или виртуальном сервере SP02;

в) SRV_APP – установлен и выполняется на выделенном физическом или виртуальном сервере SP03.

Данная конфигурация рекомендуется для использования в решениях средней сложности.

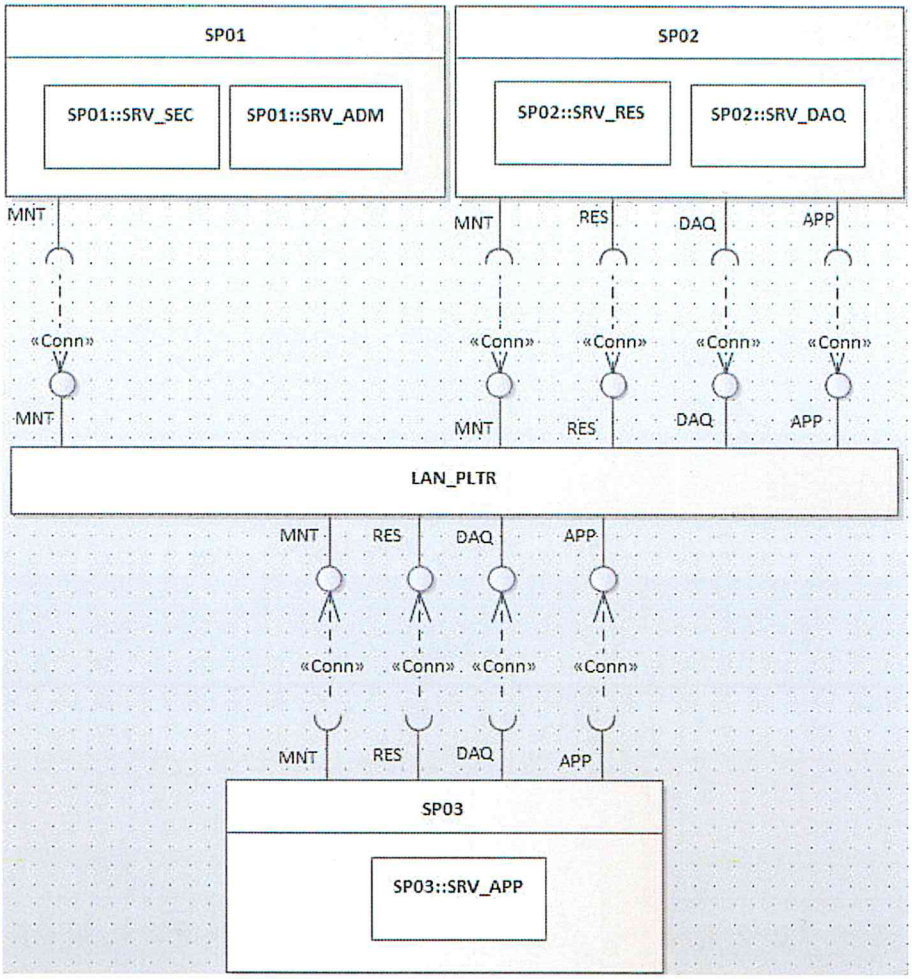


Рис. 5 – Конфигурация HW_CFG02

Требования к аппаратному обеспечению серверов для конфигурации HW_CFG02 рассмотрены в таблице 2.

Таблица 2 – Требования к аппаратному обеспечению серверов для конфигурации HW_CFG02

Аппаратное обеспечение	Сервер		
	SP01	SP02	SP03
Процессор	аппаратная платформа на базе Intel® Xeon® не ниже 2-го поколения		
Оперативная память	DDR4 8 Гб	DDR4 16 Гб	DDR4 8 Гб
Объем жесткого диска	RAID10 2048 Гб	RAID10 2048 Гб + RAID10 8192 Гб	RAID10 4096 Гб
ЛВС (LAN)	2 x 2 x 10 Мбит/с	2 x 2 x 1 Мбит/с	
Свободный USB	(не ниже спецификации 2.x)	—	

Аппаратное обеспечение	Сервер		
	SP01	SP02	SP03
	– порт для подключения лицензионного ключа, либо карта доверенной платформы со встроенной защищенной СХД		
Порт	IPMI		
Операционная система: Вариант 01 Вариант 02	 лицензионная ОС Microsoft Windows Server 2019, СУБД PostgreSQL ОС Debian GNU/Linux x64 10 Server, СУБД PostgreSQL		

– конфигурация HW_CFG03 (рис. 6). Все компоненты SRV_SEC, SRV_ADM, SRV_RES, SRV_DAQ, SRV_APP установлены и выполняются на выделенных физических или виртуальных серверах. Рекомендуется для использования в высоконагруженных применениях.

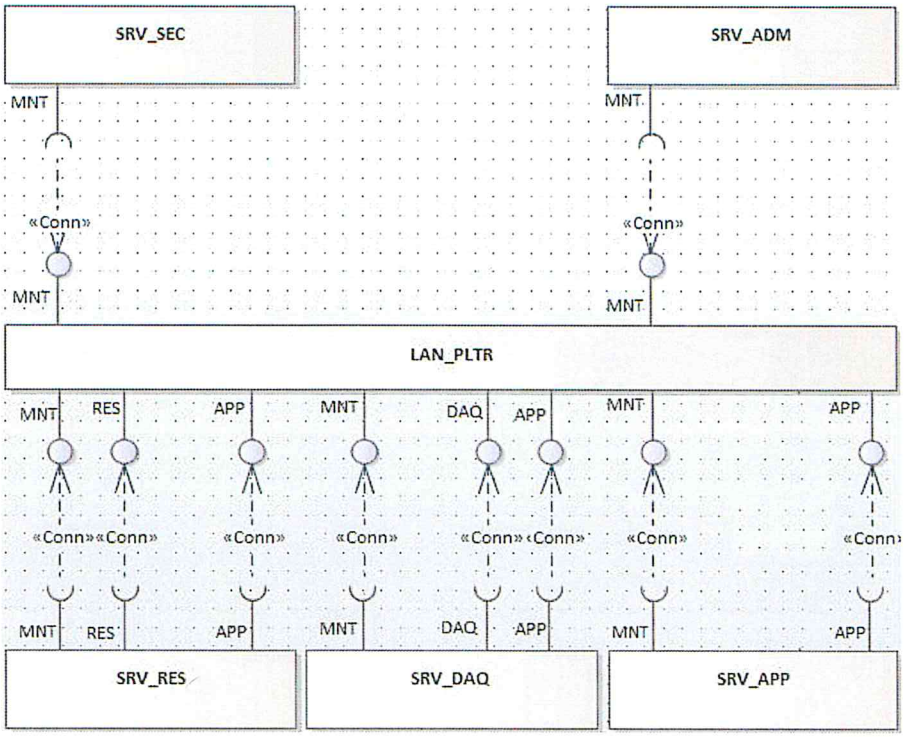


Рис. 6 – Конфигурация HW_CFG03

Требования к аппаратному обеспечению компонентов для конфигурации HW_CFG03 рассмотрены в таблице 3.

Таблица 3 – Требования к аппаратному обеспечению компонентов для конфигурации HW_CFG03

Аппаратное обеспечение	Компоненты				
	SRV_SEC	SRV_ADM	SRV_RES	SRV_DAQ	SRV_APP
Процессор	аппаратная платформа на базе Intel® Xeon® не ниже 2-го поколения				
Оперативная память	DDR4 4 Гб		DDR4 16 Гб	DDR4 8 Гб	DDR4 16 Гб
Объем жесткого диска	RAID10 2048 Гб		RAID10 2048 Гб + RAID10 8192 Гб	RAID10 2048 Гб + RAID10 4096 Гб	
ЛВС (LAN)	2 x 2 x 1 Мбит/с		2 x 2 x 10 Мбит/с	2 x 1 Мбит/с + 2 x 10 Мбит/с	2 x 2 x 10 Мбит/с
Свободный USB	(не ниже спецификации 2.x) – порт для подключения лицензионного ключа, либо карта доверенной платформы со встроенной защищенной СХД	—	—	—	—
Порт	IPMI				
Операционная система: Вариант 01 Вариант 02	лицензионная ОС Microsoft Windows Server 2019, СУБД PostgreSQL ОС Debian GNU/Linux x64 10 Server, СУБД PostgreSQL				

Функционирование SRV_SEC предполагается в приведенной на рис. 7 аппаратной конфигурации. WS_SEC является АРМ системы управления информационной безопасностью и обеспечивает ее интерфейс пользователя. В составе ПК предусматривается наличие не более 1-го WS_SEC. Наличие WS_SEC определяется лицензионным соглашением. WS_SEC является опциональным при интеграции Сервера в вышестоящие системы управления информационной безопасностью. Мониторинг и управление информационной безопасностью осуществляется только по сетям MNT.

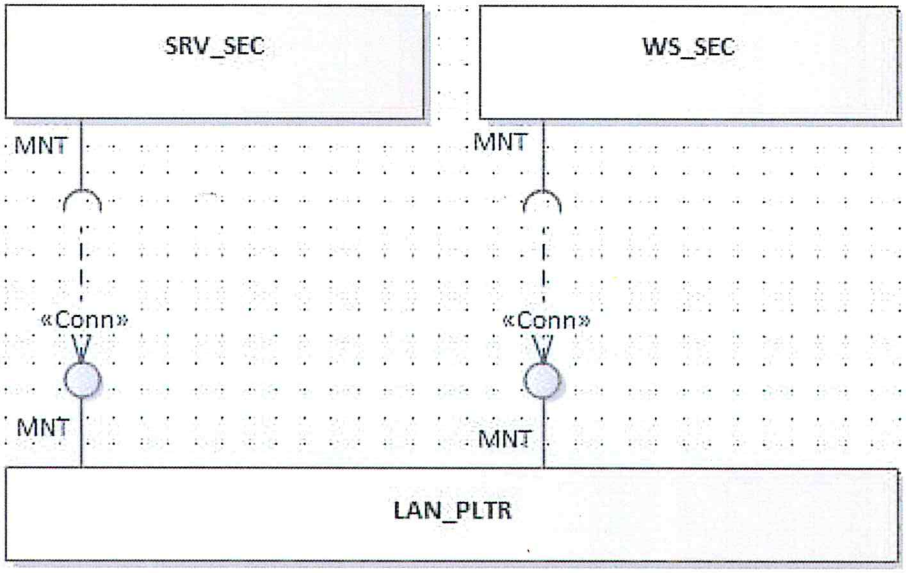


Рис. 7 – Аппаратная конфигурация функционирования SRV_SEC

Функционирование SRV_ADM предполагается в приведенной на рис. 8 аппаратной конфигурации. WS_ADM является АРМ системного администратора ПК. В составе ПК предусматривается наличие не более 1-го WS_ADM. Наличие WS_ADM определяется лицензионным соглашением. WS_ADM является опциональным при интеграции Сервера в вышестоящие системы управления конфигурацией и инфраструктурой ИТ. Системное администрирование осуществляется только по сетям MNT.

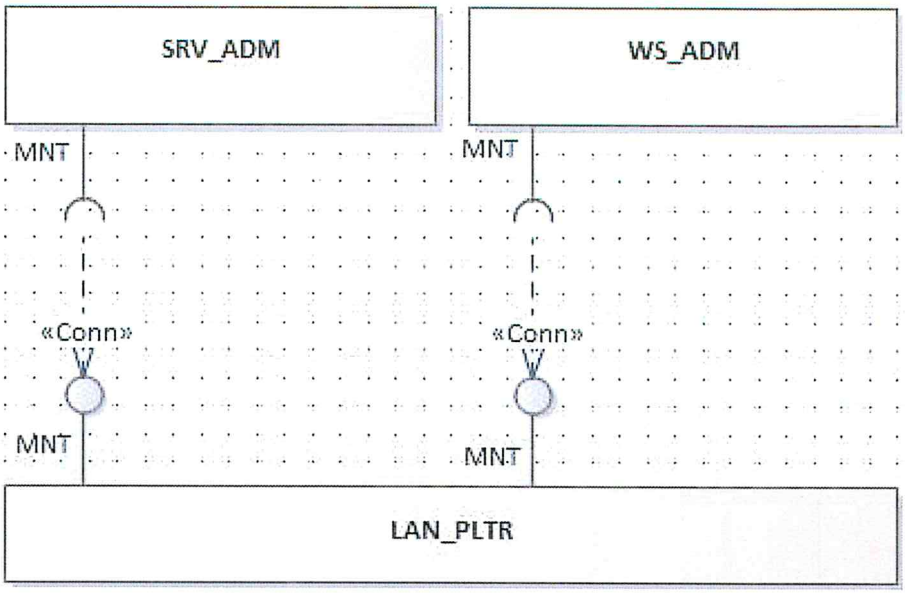


Рис. 8 – Аппаратная конффигурация функционирования SRV_ADM

Функционирование SRV_RES предполагается в приведенной на рис. 9 аппаратной конфигурации. Управление и пользовательский интерфейс Сервера предоставляется через WS_ADM. Интеграция внешних ресурсов осуществляется по сетям группы RES. Доступ со стороны SRV_APP осуществляется по сетям APP.

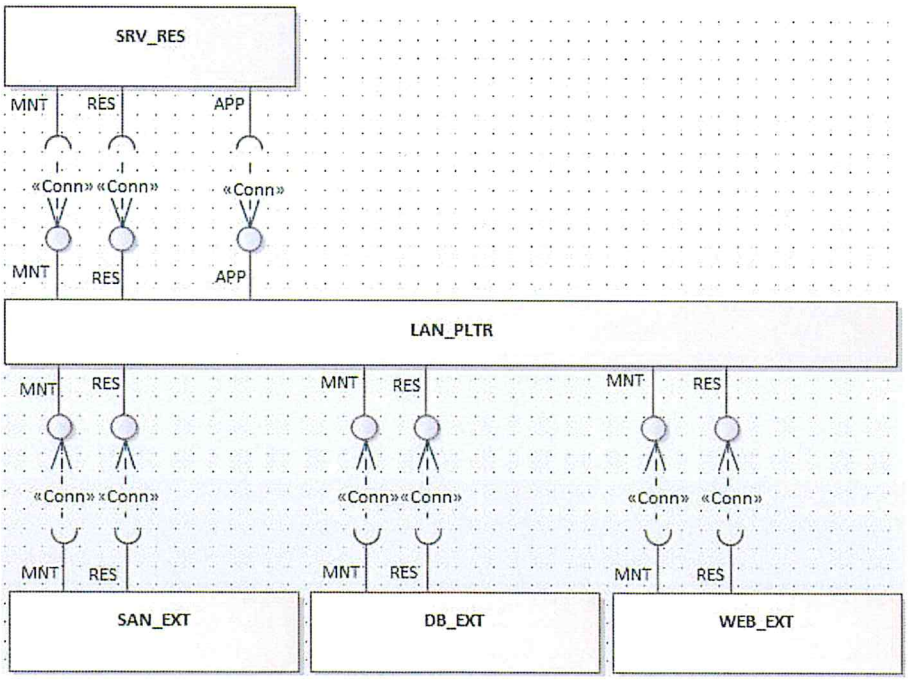


Рис. 9 – Аппаратная конфигурация функционирования SRV_RES

Функционирование SRV_DAQ предполагается в приведенной на рис. 10 аппаратной конфигурации. Управление и пользовательский интерфейс Сервера предоставляется через WS_ADM. Коммуникация с внешними системами осуществляется по сетям группы DAQ. Предусмотрен непосредственный ввод/вывод сигналов (Direct IO) посредством специализированных модулей расширения. Доступ со стороны SRV_APP осуществляется по сетям APP.

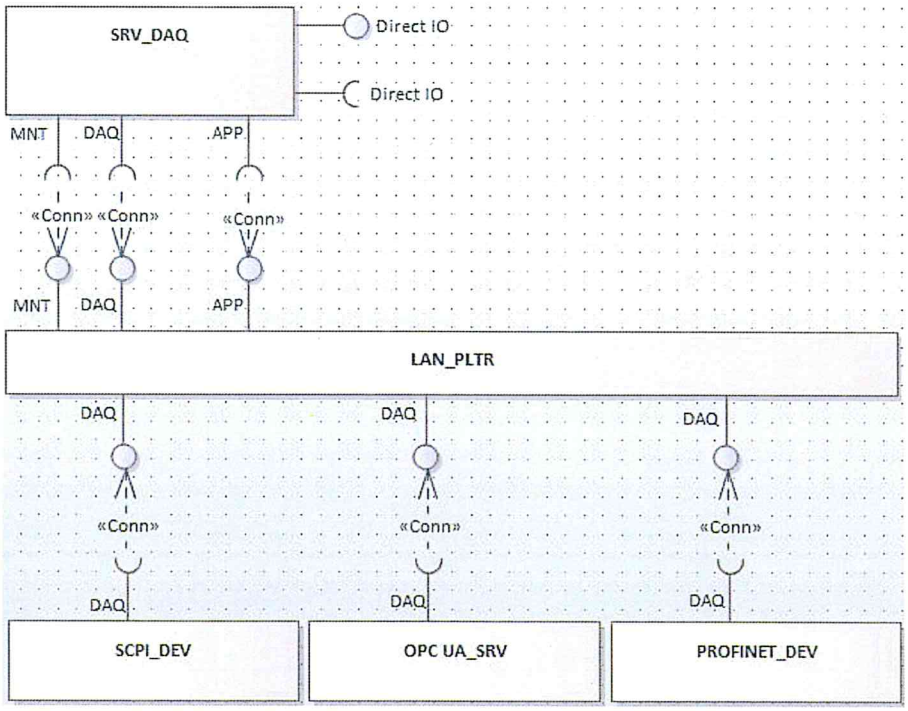


Рис. 10 – Аппаратная конфигурация функционирования SRV_DAQ

Функционирование SRV_APP предполагается в приведенной на рис. 11 аппаратной конфигурации. Пользовательский интерфейс Сервера предоставляется через WS_APP – АРМ пользователя ПК. В составе ПК предусматривается наличие 1-го и более WS_APP. Количество WS_APP определяется лицензионным соглашением.

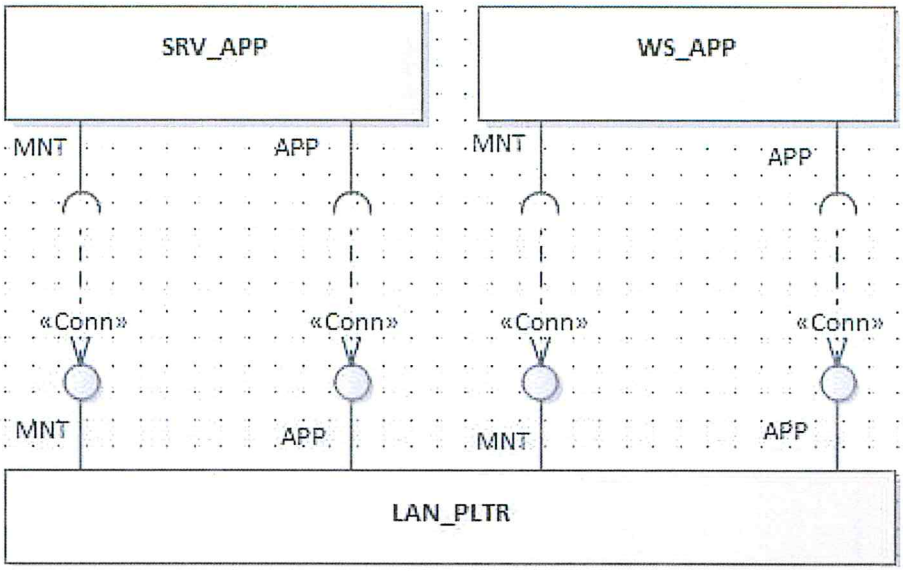


Рис. 11 – Аппаратная конфигурация функционирования SRV_APP

2.1.2.4. Требования информационной безопасности обеспечиваются за счет:

– необходимой степени физической защиты доступа к серверному оборудованию;

– соответствующих регламентов на организационном уровне эксплуатации;

– интеграции серверного оборудования в централизованную систему управления информационной безопасностью.

2.1.2.5. Обеспечение производительности и балансировка нагрузки осуществляется путем:

– горизонтальное масштабирование. Обеспечения соответствующего количества физических или виртуальных серверов;

– вертикальное масштабирование. Применения физических или виртуальных серверов соответствующей производительности;

– совместное использование горизонтальных и вертикальных методов масштабирования, а также балансировка нагрузки за счет встроенных конфигурируемых и динамических средств уровня используемых ОС.

2.1.2.6. Обеспечение надежности и отказоустойчивости осуществляется путем:

– обеспечения избыточности ресурса («холодное» или «горячее» резервирование) оборудования физических серверов;

– размещения серверов на платформах виртуализации с соответствующими показателями надежности и уровнем SLA;

– обеспечения плановых превентивных регламентов обслуживания;

– обеспечения соответствующего уровня регламентов внеплановых ремонтных работ;

– обеспечения соответствующих регламентов на организационном уровне эксплуатации в части физического доступа к оборудованию;

– обеспечения соответствующей категории электропитания;

– обеспечения соответствующего уровня пожарной безопасности.

2.1.2.7. Обеспечение управляемости осуществляется путем интеграции серверного оборудования в:

– централизованную систему управления информационной безопасности;

– централизованную систему управления конфигурацией;

– централизованную систему управления ИТ-инфраструктурой.

2.1.3. Программные средства

2.1.3.1. Архитектурно ПК построен в соответствии с архитектурным паттерном Multi-layer (Multi-tier), показанным на рис. 12.

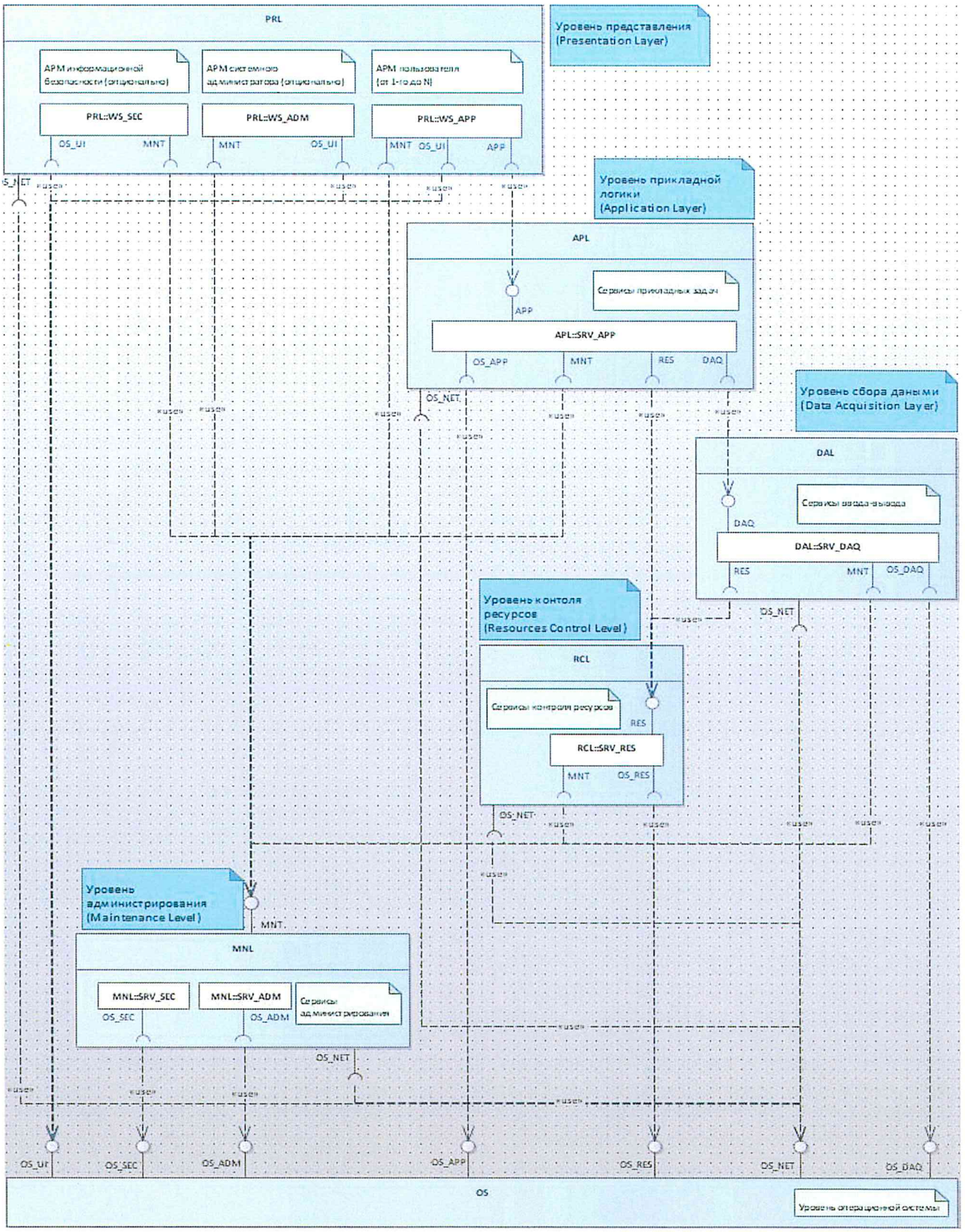


Рис. 12 – Архитектурный паттерн Multi-layer (Multi-tier)

2.2. Режимы функционирования и спецификация функций

2.2.1. Режим «Развертывание»

2.2.1.1. К работам по развертыванию Сервера допускается персонал, который прошел курс обучения и сдал сертификационный экзамен в соответствии с руководством системного программиста БЮЛИ.00131-01 32 01.

2.2.1.2. Работы по развертыванию Сервера осуществляются на аппаратно-программной платформе, показатели и характеристики которой соответствуют указанным в разделе 2.1.2 требованиям.

2.2.1.3. В режиме функционирования «Развертывание» предусмотрены следующие функции:

– чтение данных лицензионного соглашения Заказчика и реквизитов Пользователя с лицензионного ключа;

– формирование рекомендуемых названий вычислительного узла и имени Суперпользователя;

– первоначальный вход в систему под учетной записью Суперпользователя со специфицированным в документе «Лицензионное соглашение» паролем по схеме двухфакторной аутентификации;

– обеспечение формирования:

а) первоначального профиля пользователей в диалоговом режиме;

б) профиля конфигурации аппаратных средств в диалоговом режиме;

в) профиля сетевой конфигурации в диалоговом режиме;

г) профиля сетевой конфигурации программных средств в диалоговом режиме;

– развертывание Сервера в пакетном режиме в соответствии с заданными параметрами;

– информирование о результатах процесса выполнения развертывания. При успешном завершении процесса развертывания ПК готов к переходу в режим «Функционирование и поддержка».

2.2.1.4. Управление безопасностью осуществляется согласно алгоритму, рассмотренному на рис. 13.

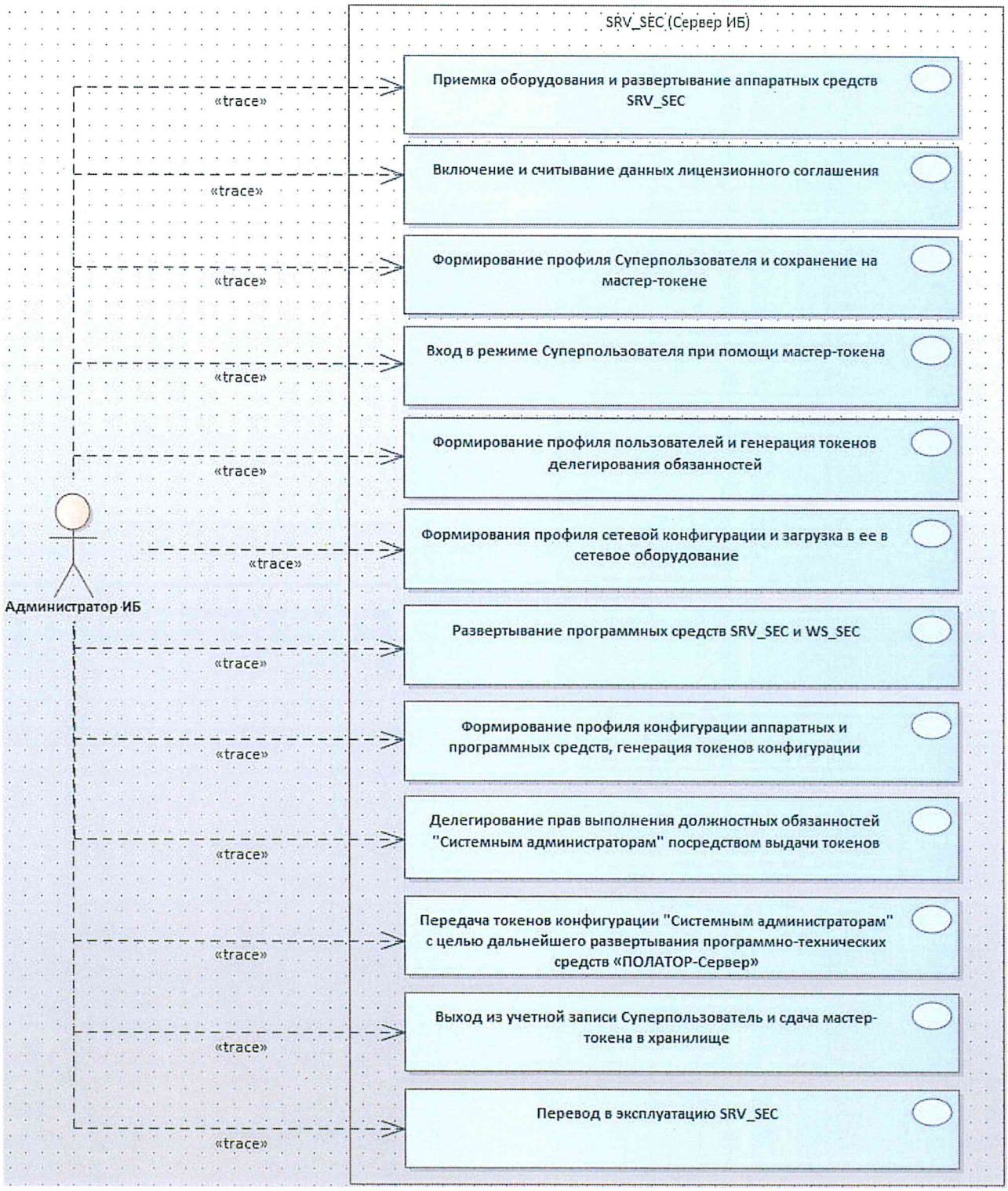


Рис. 13 – Управление безопасностью

2.2.1.5. Общее администрирование осуществляется согласно алгоритму, рассмотренному на рис. 14.

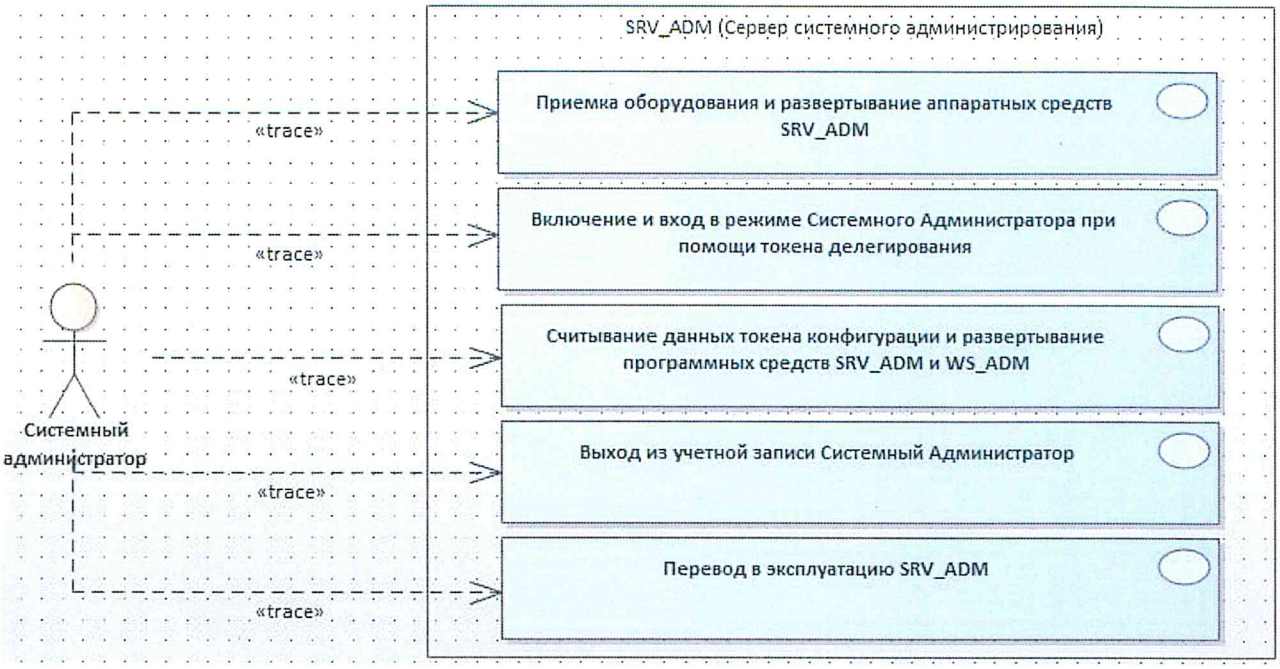


Рис. 14 – Общее администрирование

2.2.1.6. Администрирование и управлени ресурсами осуществляется согласно алгоритму, рассмотренному на рис. 15.

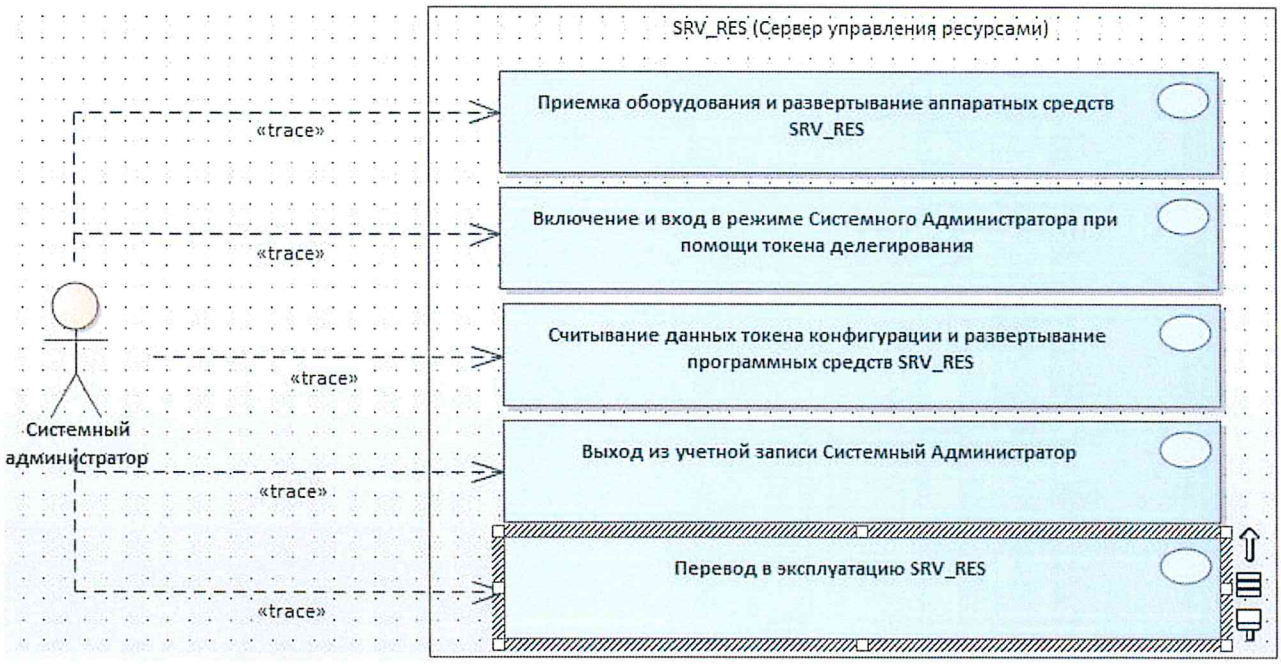


Рис. 15 – Администрирование и управление ресурсами

2.2.1.7. Администрирование сбора данных осуществляется согласно алгоритму, рассмотренному на рис. 16.

Рис. 16 – Администрирование сбора данных

2.2.1.8. Администрирование прикладнымх задач осуществляется согласно алгоритму, рассмотренному на рис. 17.

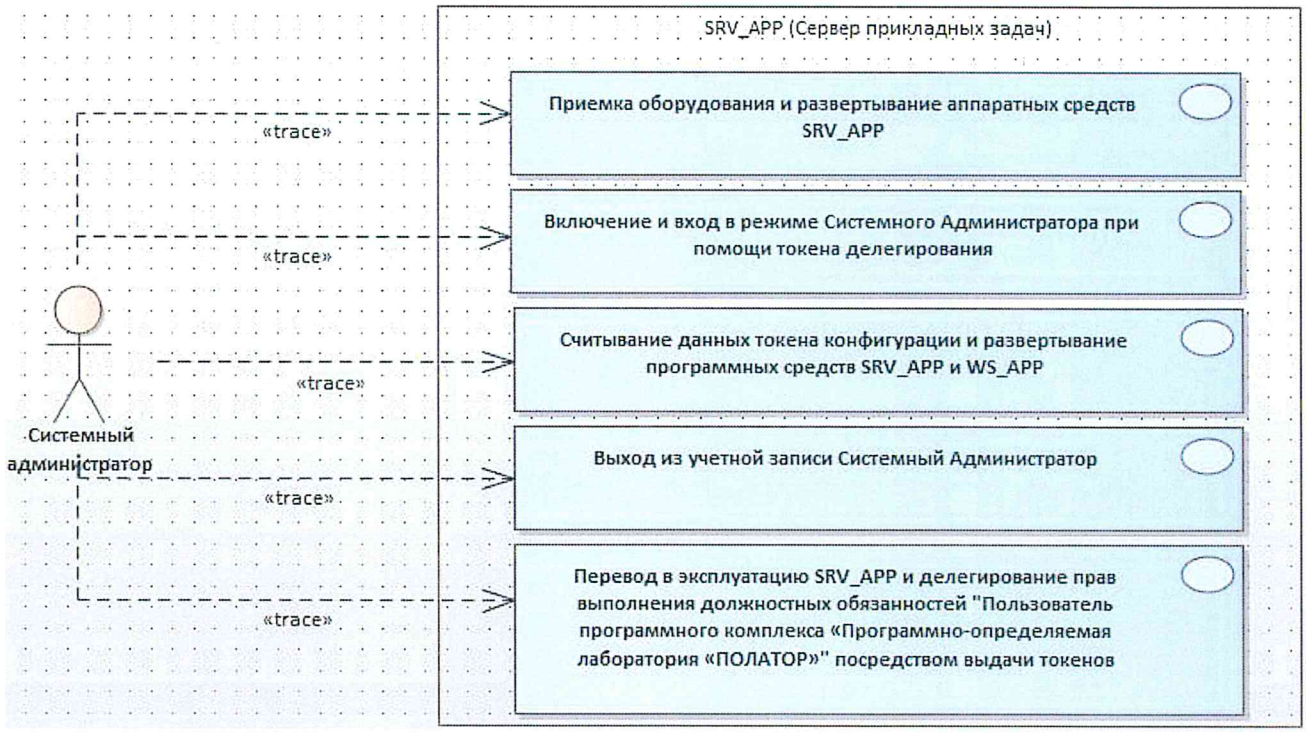


Рис. 17 – Администрирование прикладнымх задач

2.2.2. Режим «Функционирование». Запуск и функционирование в проектном режиме

2.2.2.1. К работам по запуску и обеспечению функционирования в штатном режиме Сервера допускается персонал, который прошел курс обучения и сдал сертификационный экзамен в соответствии с руководством системного программиста БЮЛИ.00131-01 32 01.

2.2.3. Режим «Функционирование». Плановые регламенты и останов в проектном режиме

2.2.3.1. К работам по проведению плановых регламентных работ и останову в штатном режиме Сервера допускается персонал, который прошел курс обучения и сдал сертификационный экзамен в соответствии с руководством системного программиста БЮЛИ.00131-01 32 01.

2.2.3.2. Режим «Функционирование» предназначен для выполнения следующих операций:

– запуск Сервера при процессе старта ОС с обеспечением последовательности запуска компонент в соответствии с зависимостями;

– обеспечение выполнения пользовательских настроек:

а) SRV_RES. Спецификация ресурсов пользователя для организации проектов;

б) SRV_APP. Спецификация пользователем состава и параметров пользовательских проектов;

в) SRV_DAQ. Спецификация пользователем состава и параметров ввода/вывода, обмена данными в рамках проектов;

г) SRV_RES. Спецификация ресурсов пользователя для организации библиотек;

д) SRV_APP. Спецификация пользователем состава и параметров пользовательских библиотек;

– создание пользовательских проектов;

– открытие существующих пользовательских проектов и их загрузка;

– создание пользовательских библиотек;

– подключение существующих пользовательских библиотек;

– редактирование графической модели на языке GPL;

– управление вставкой, редактированием и удалением элементов графической модели на языке GPL;

– управление отображением и редактированием параметров элементов графической модели на языке GPL;

– редактирование кода на языке SPL;

– создание пользовательского интерфейса элементов, созданных как в нотации GPL, так и SPL;

– обеспечение управления:

а) состоянием проекта;

б) состоянием библиотеки;

в) журналом событий;

– запуск прикладных моделей и программ в режиме:

а) «Выполнение» (Циклический режим выполнения). Количество запущенных экземпляров масштабируется производительностью SRV_APP;

б) «Отладка» (Шаговый режим выполнения). Количество запущенных экземпляров масштабируется производительностью SRV_APP;

– обеспечение нормального останова Сервера при:

а) процессе останова ОС;

б) останове ОС при реакции на сигнал от подсистемы мониторинга электропитания;

в) централизованном управлении состоянием аппаратных и программных средств;

– обеспечение нормального останова Сервера из рабочего аппаратно-программного окружения системного программиста в соответствии с руководством системного программиста БЮЛИ.00131-01 32 01.

2.2.3.3. Операции с проектами в плановом режиме рассмотрены на рис. 18.

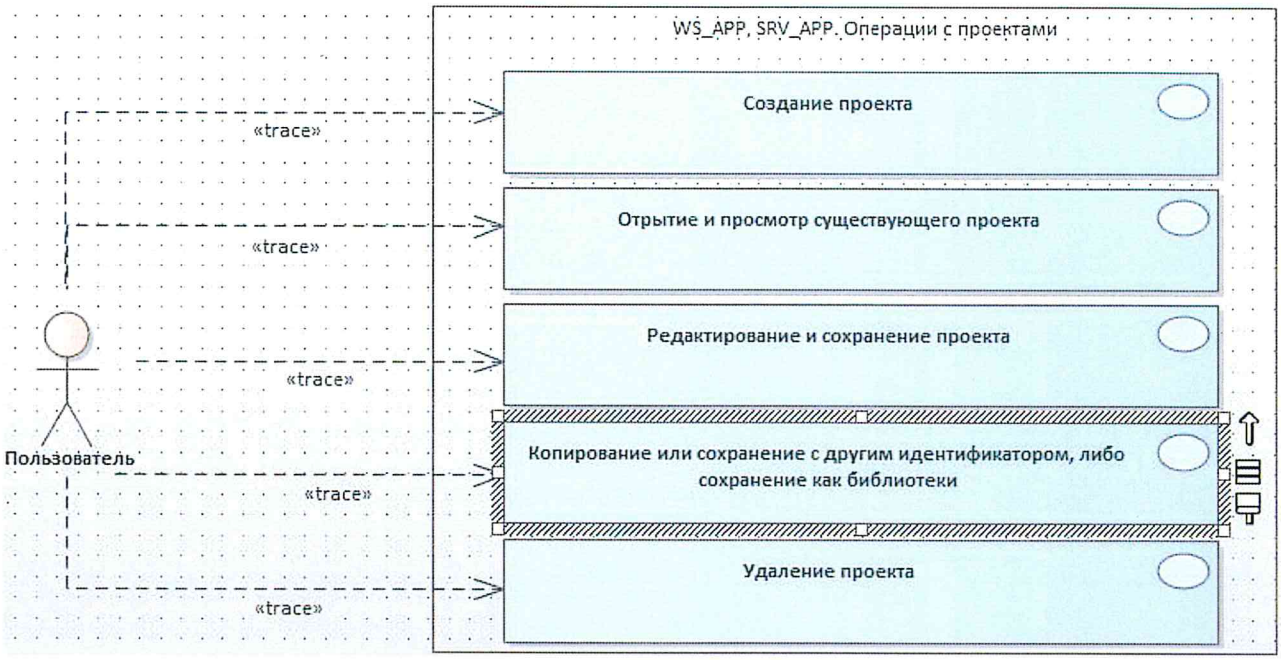


Рис. 18 – Плановый режим: операции с проектами

2.2.3.4. Операции с библиотеками в плановом режиме рассмотрены на рис. 19.

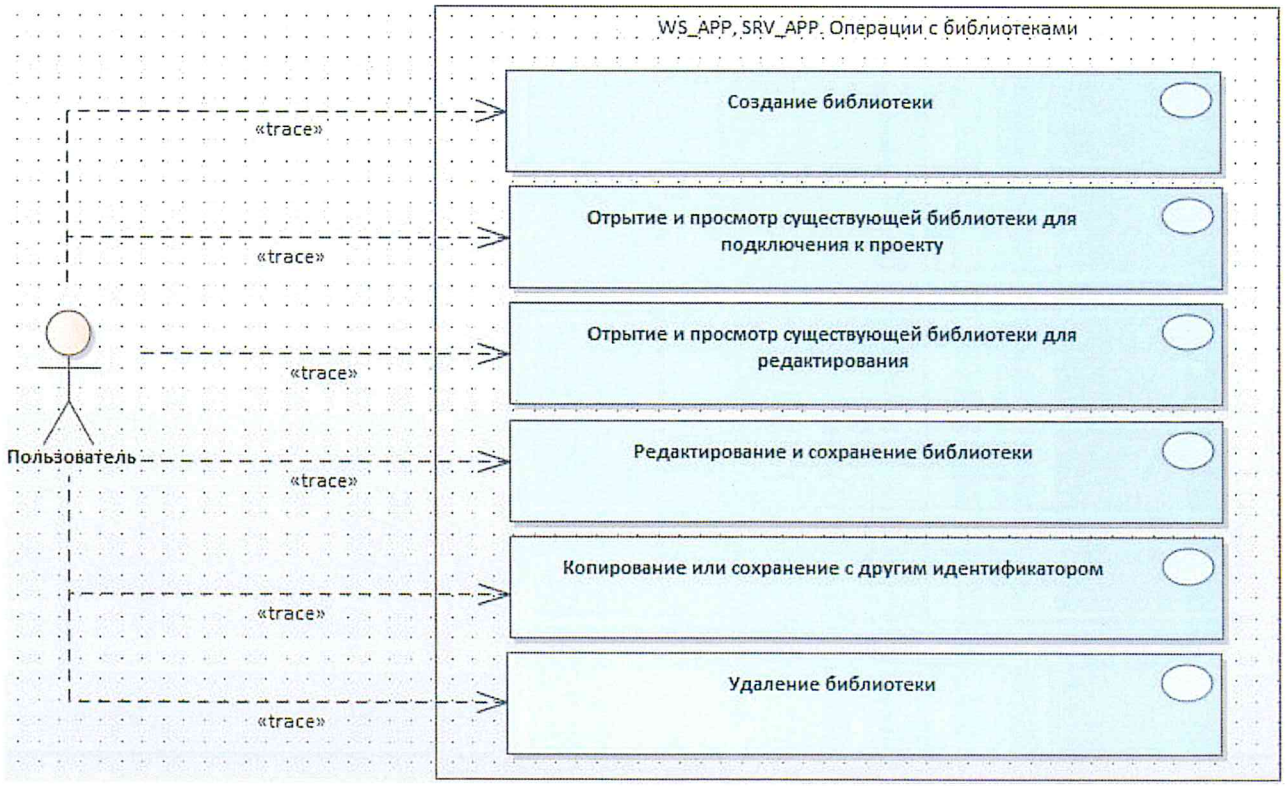


Рис. 19 – Плановый режим: Операции с библиотеками

2.2.3.5. Операции с элементами моделей в плановом режиме рассмотрены на рис. 20.

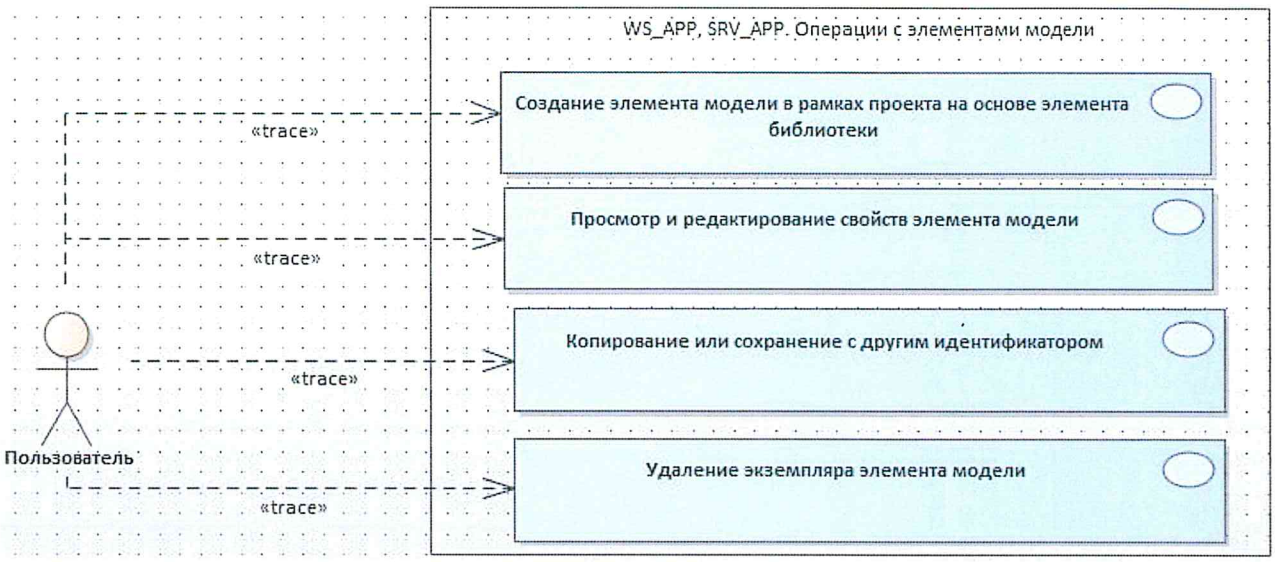


Рис. 20 – Плановый режим: операции с элементами моделей

2.2.3.6. Операции с элементами SPL (программирование) в плановом режиме рассмотрены на рис. 21.

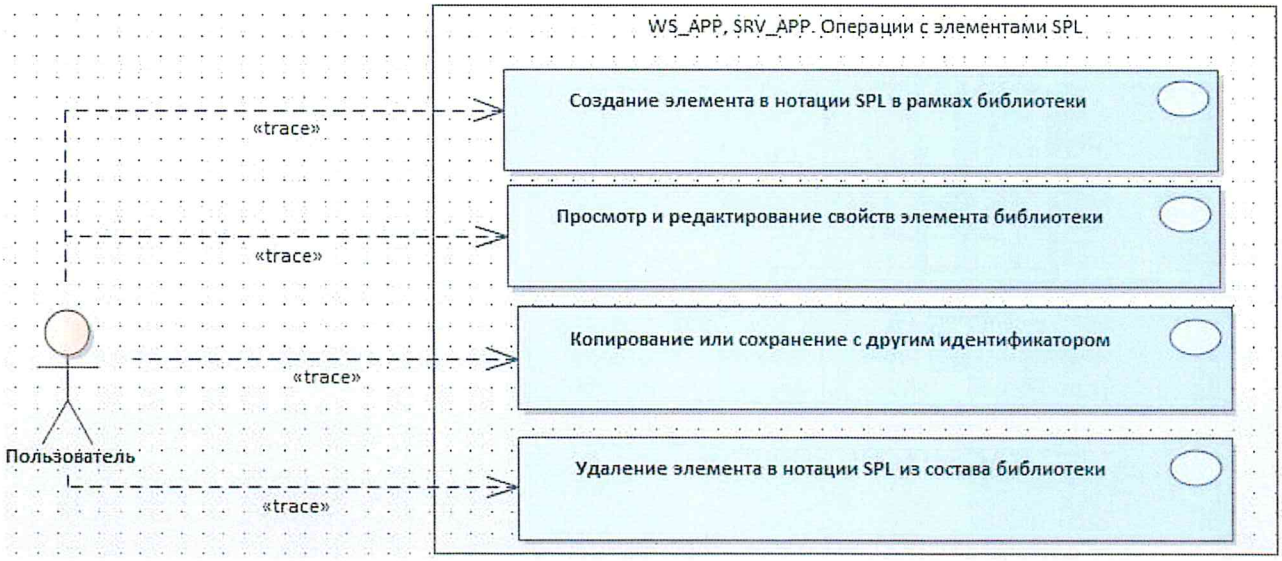


Рис. 21 – Плановый режим: операции с элементами SPL (программирование)

2.2.3.7. Операции с элементами UI (программирование) в плановом режиме рассмотрены на рис. 22.

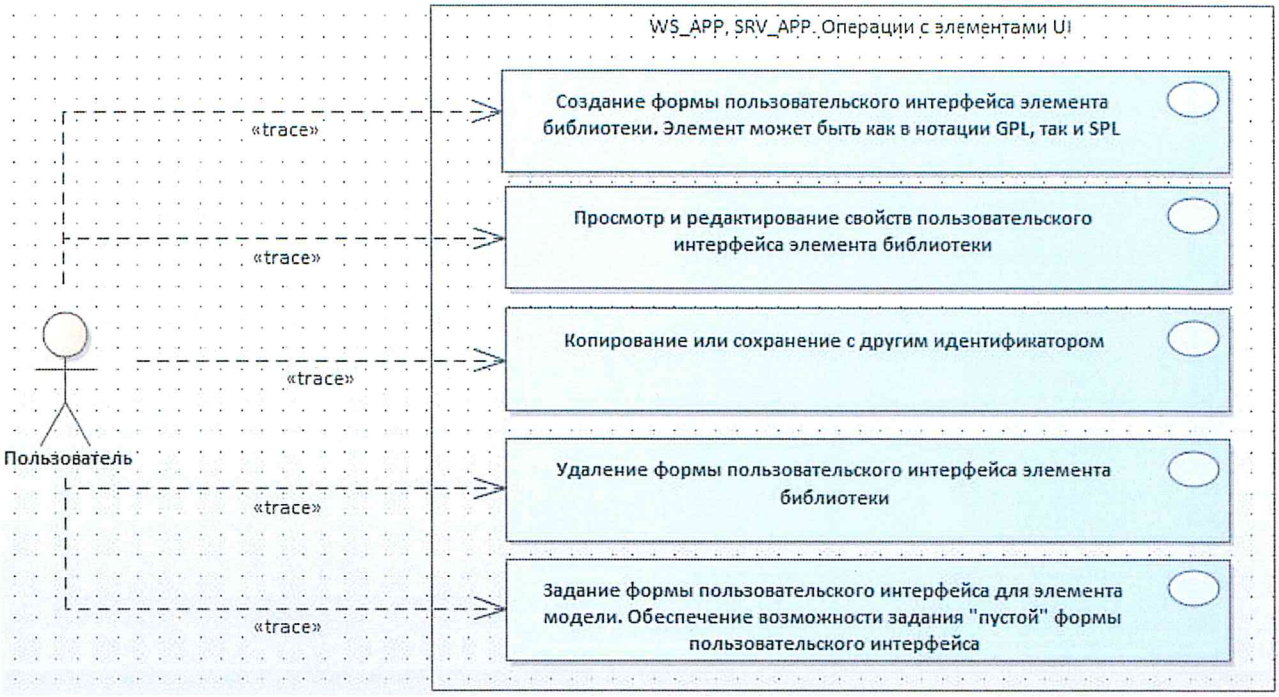


Рис. 22 – Плановый режим: операции с элементами UI (программирование)

2.2.4. Режим «Функционирование». Внеплановые ремонтные и аварийные режимы работы

2.2.4.1. К проведению внеплановых ремонтных работ, а также выполнению действий при аварийных режимах работы Сервера допускается персонал, который прошел курс обучения и сдал сертификационный экзамен в соответствии с руководством системного программиста БЮЛИ.00131-01 32 01.

2.2.4.2. Обеспечение доступности ресурсов осуществляется согласно схеме, показанной на рис. 23.

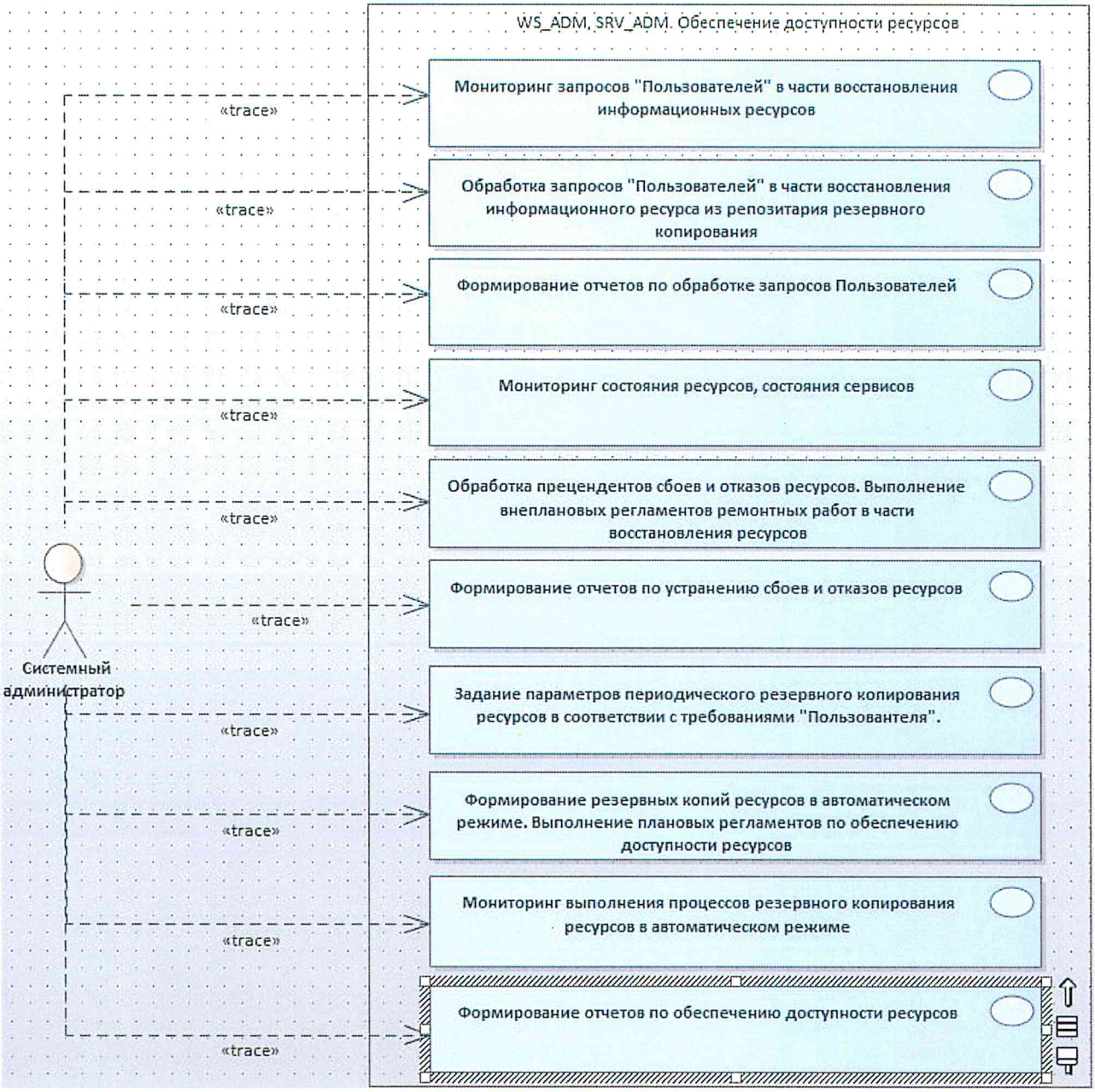


Рис. 23 – Обеспечение досупности ресурсов

2.2.4.3. Обеспечение надежности функционирования осуществляется согласно схеме, показанной на рис. 24.

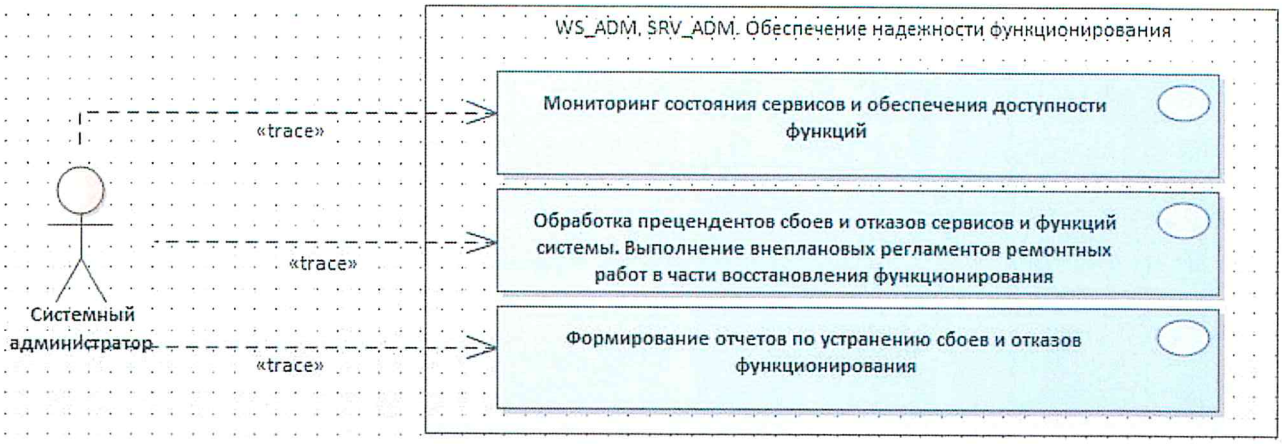


Рис. 24 – Обеспечение надежности функционирования

2.2.4.4. Обеспечение информационной безопасности осуществляется согласно схеме, показанной на рис. 25.

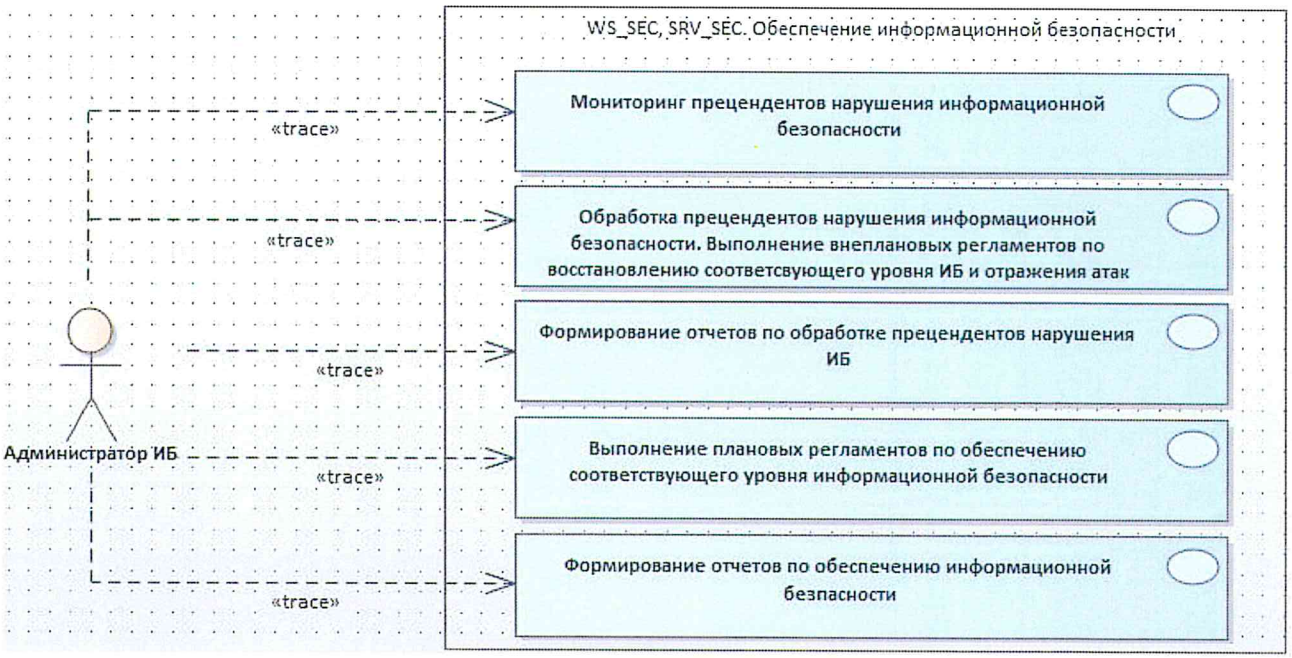


Рис. 25 – Обеспечение информационной безопасности

2.2.5. Режим «Прекращение применения»

2.2.5.1. Перед проведением работ по прекращению применения Сервера рекомендуется ознакомиться с соответствующими требованиями руководства системного программиста БЮЛИ.00131-01 32 01.

2.2.5.2. Завершение эксплуатации осуществляется согласно рис. 26.

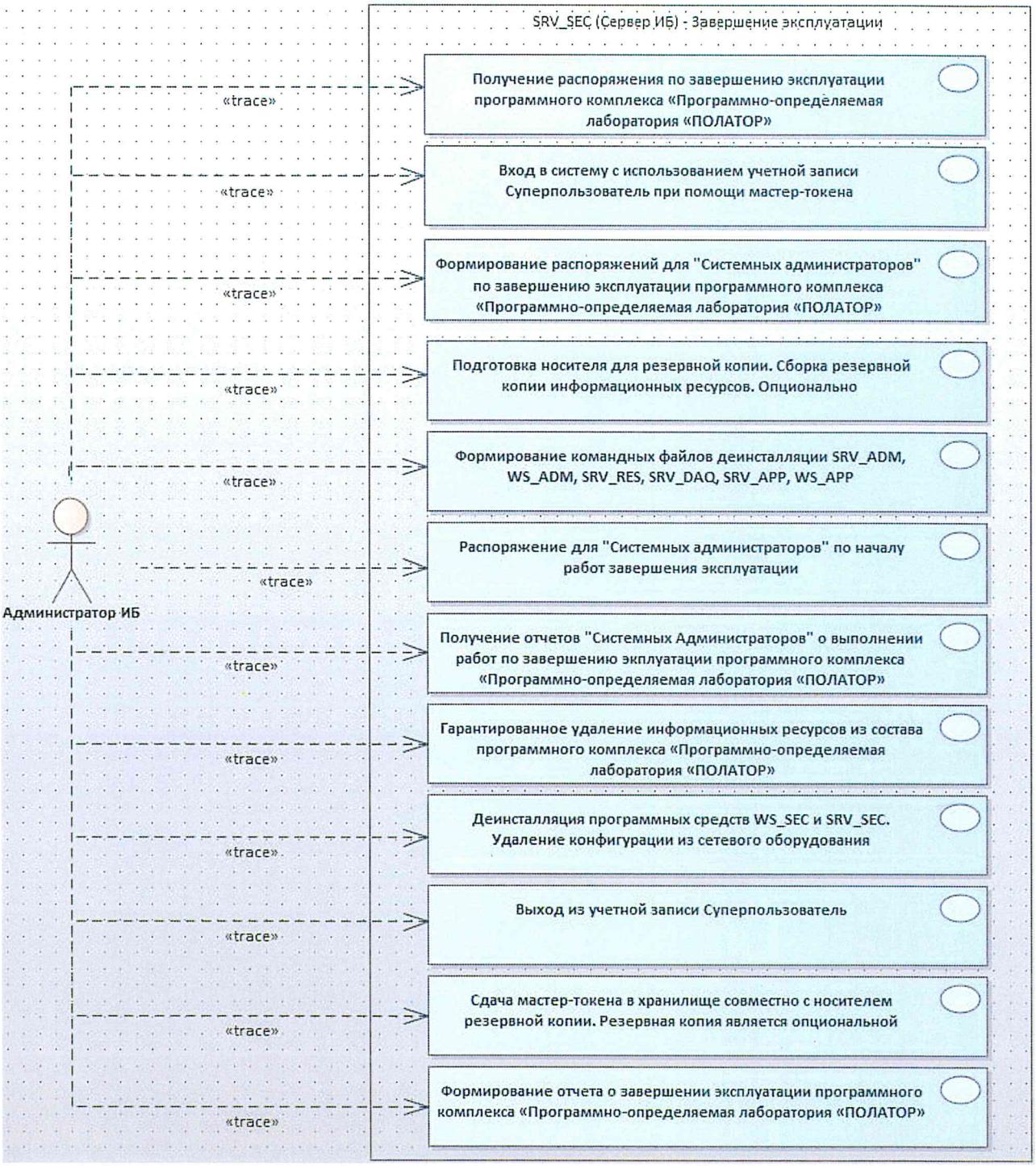


Рис. 26 – Завершение эксплуатации

2.3. Межсистемные интерфейсы

2.3.1. Сведения о межсистемных интерфейсах

2.3.1.1. Дополнительно к функциям управления конфигурацией и мониторингом состояния со стороны специализированных компонент из состава ПК,

Сервер предусматривает интерфейсы интеграции в соответствующие системы уровня предприятия с целью обеспечения централизованного группового управления и мониторинга.

2.3.1.2. Для обеспечения и управления безопасностью аппаратных и программных компонент из состава Сервера предусмотрен интерфейс интеграции в системы управления информационной безопасностью (Security Capsule, RuSIEM, Microsoft SCCM):

– анализ и управление рисками безопасности;

– сбор, обработка и анализ событий безопасности;

– обнаружение атак и нарушений критериев и политик безопасности;

– централизованное управление аутентификацией и контролем доступа;

– антивирусная защита и защита от вредоносного кода;

– межсетевое экранирование;

– формирование отчетных документов безопасности.

2.3.1.3. Для управления конфигурацией аппаратных и программных компонент из состава Сервера предусмотрен интерфейс интеграции в системы управления конфигурацией ИТ-инфраструктур (Microsoft SCCM, Ansible, Chef):

– централизованное управление конфигурацией системных ресурсов сервера. Возможность интеграции с распределенными ресурсами СХД (iSCSI, Samba, Ceph, HDFS) с целью обеспечения требований производительности и надежности;

– централизованное управление конфигурацией системных ресурсов сервера. Возможность интеграции с распределенными ресурсами систем БД с целью обеспечения требований производительности и надежности;

– централизованное управление обновлениями программных компонент ОС;

– централизованное управление обновлениями компонент базового ПО;

– централизованное управление обновлениями программных компонент из состава ПК.

2.3.1.4. Для мониторинга состояния аппаратных и программных компонент из состава Сервера предусмотрен интерфейс интеграции в системы управления ИТ-инфраструктурой (Microsoft SCCM, Zabbix, Nagios):

– централизованное управление состоянием аппаратных компонент на базе SNMP;

– мониторинг состояния аппаратных компонент на базе SNMP и SNMP-ловушек;

– централизованное управление состоянием программных компонент на базе SNMP;

– мониторинг состояния программных компонент на базе SNMP и SNMP-ловушек;

– централизованный мониторинг журналов системных событий;

– SLA-мониторинг, формирование отчётов и тенденций;

– комплексная реакция на события с возможностью расширения за счет выполнения внешних скриптов.

3. ОПИСАНИЕ ЛОГИЧЕСКОЙ СТРУКТУРЫ

3.1. Структура программы

3.1.1. С целью обеспечения модульности архитектуры программы предусмотрено разделение программных компонент из состава ПК на выделенные процессы на основе функциональных признаков.

3.1.2. Выделенные процессы могут выполняться как на одном вычислительном узле, так и на отдельных или выделенных вычислительных узлах.

3.1.3. В качестве вычислительных узлов используются как физические вычислители, так и виртуальные вычислительные узлы, функционирующие на платформах виртуализации.

3.1.4. С целью обеспечения требований надежности и необходимого уровня производительности физические вычислительные узлы могут быть реализованы в форме кластерных высокопроизводительных отказоустойчивых комплексов.

3.1.5. Приведенная далее функциональная структура (рис. 27) представляет схему функционального деления, которая не накладывает требований на структурное деление. Допускается структурное исполнение указанных компонент в виде решений, начиная от совмещенных в одном процессе до архитектурных решений, предполагающих выделенные кластеры для каждого из функциональных компонент.

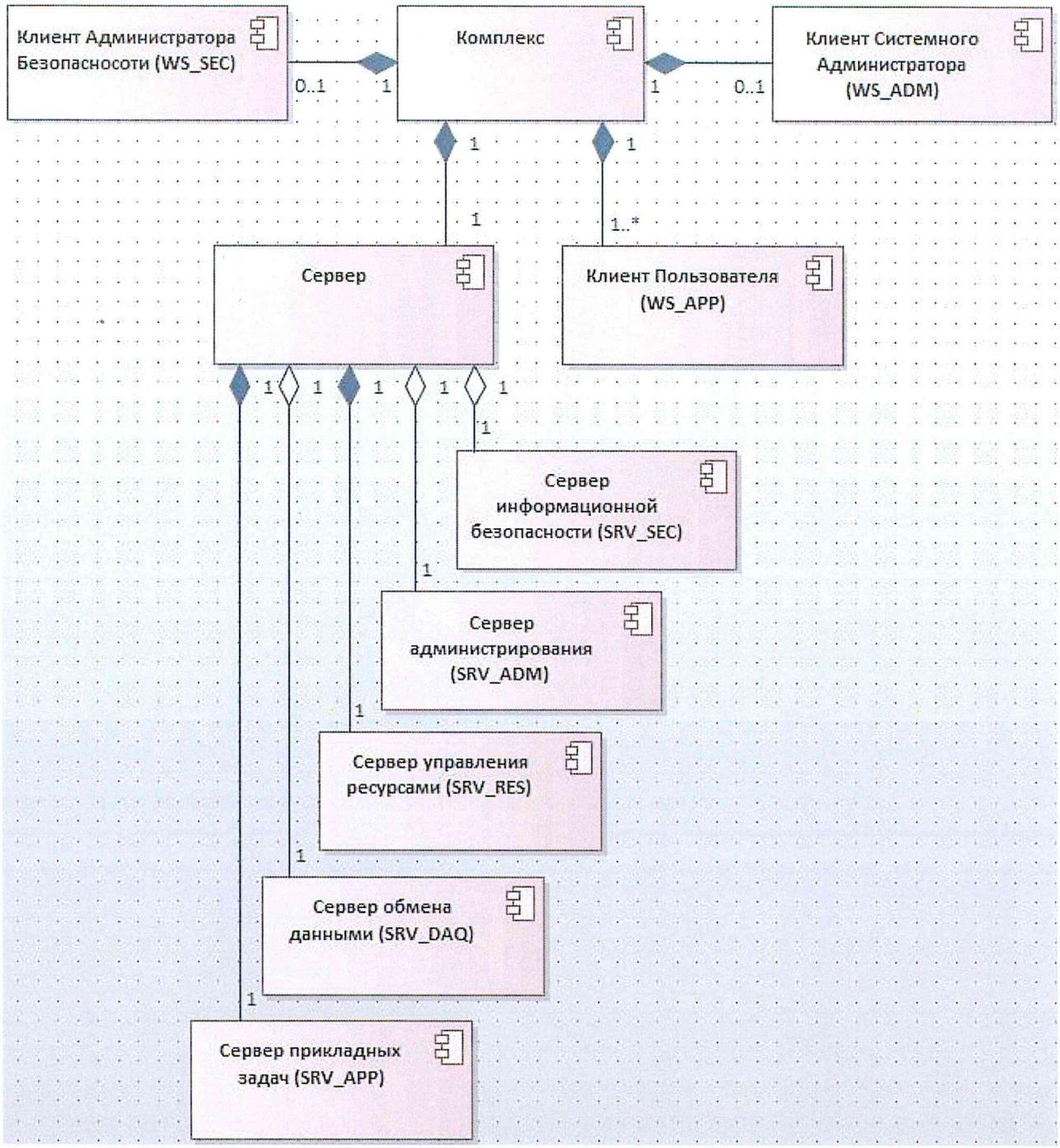


Рис. 27 – Функциональная структура

3.2. Составные части программы

3.2.1. Подсистема информационной безопасности

3.2.1.1. Подсистема информационной безопасности (SRV_SEC) выполняет следующие функции:

– управление лицензиями;

– обеспечение локальных сервисов информационной безопасности;

– обеспечение интеграции в вышестоящую централизованную систему управления информационной безопасности.

3.2.2. Подсистема системного администрирования

3.2.2.1. Подсистема системного администрирования (SRV_ADM) выполняет следующие функции:

– обеспечение локальных сервисов системного администрирования, обслуживания и ремонта аппаратных и программных средств;

– обеспечение интеграции в вышестоящую централизованную систему управления конфигурацией;

– обеспечение интеграции в вышестоящую централизованную систему управления ИТ-инфраструктурой.

3.2.3. Подсистема управления ресурсами

3.2.3.1. Подсистема управления ресурсами (SRV_RES) выполняет следующие функции:

– обеспечение интеграции распределенных ресурсов:

а) файловых систем;

б) систем управления баз данных;

в) WEB-сервисов;

– обеспечение централизованного доступа к локальным и интегрированным ресурсам:

а) файловой системы со стороны SRV_SEC, SRV_ADM, SRV_DAQ, SRV_APP;

б) систем управления БД со стороны SRV_SEC, SRV_ADM, SRV_DAQ, SRV_APP;

в) WEB-сервисов со стороны SRV_SEC, SRV_ADM, SRV_DAQ, SRV_APP.

3.2.4. Подсистема обмена данными

3.2.4.1. Подсистема обмена данными (SRV_DAQ) выполняет следующие функции:

– обеспечение ввода/вывода данных и представление их в форме тегов;

– обеспечение коммуникации по специализированным протоколам и представление данных обмена в форме тегов;

– предоставление доступа к тегам со стороны SRV_APP в различных режимах (циклические чтения/запись, чтение по обновлениям, запись по запросу и т.п.).

3.2.5. Подсистема прикладных задач

3.2.5.1. Подсистема прикладных задач (SRV_APP) выполняет следующие функции:

– обеспечение работы с моделями в режиме дизайна;

– выполнения моделей в различных режимах (шаговый, циклический и т.п.);

– обеспечение режима отладки моделей;

– отображение результатов выполнения модели;

– обмен данными с АРМ Клиента.

3.3. Связи между составными частями

3.3.1. Обмен данными между программными модулями из состава Сервера, а также между Сервером и Клиентом осуществляется посредством архитектурного решения на основе разделяемой базы данных[1)] (рис. 28).

[1)] Применена архитектура класса «ON-HOST».

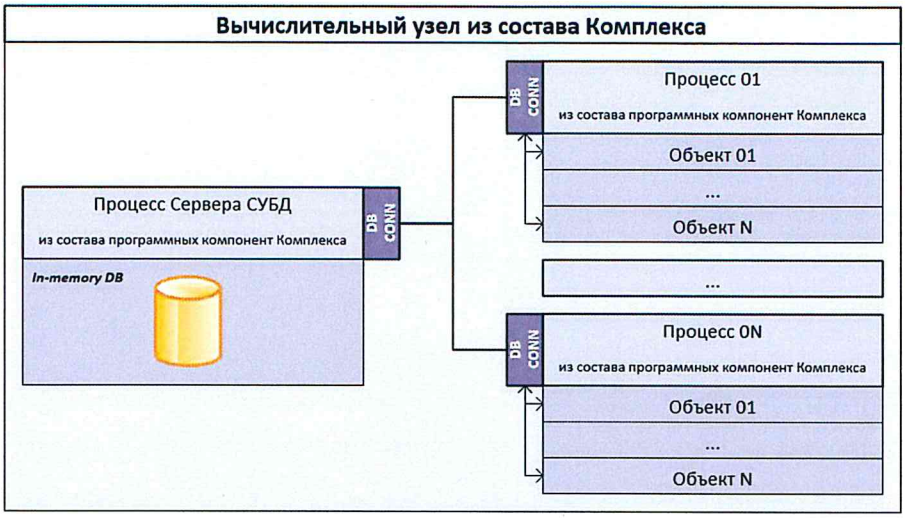


Рис. 28 – Обмен данными через БД

3.3.2. Для обмена данными организуются следующее структурное разделение на группу доменов:

– домен метаданных системы. Спецификация структуры, конфигурации и параметров программных компонент из состава ПК;

– домен информационных ресурсов прикладных проектов. Содержит в структурированной форме данные прикладных проектов и библиотек;

– домен данных в режиме реального времени. Содержит в структурированной форме необходимый набор параметров и результатов выполнения SPL-программ и GPL-моделей;

– домен данных обмена сообщениями в режиме реального времени;

– домен архивных данных.

3.3.3. Структура доменов БД показана на рис. 29.

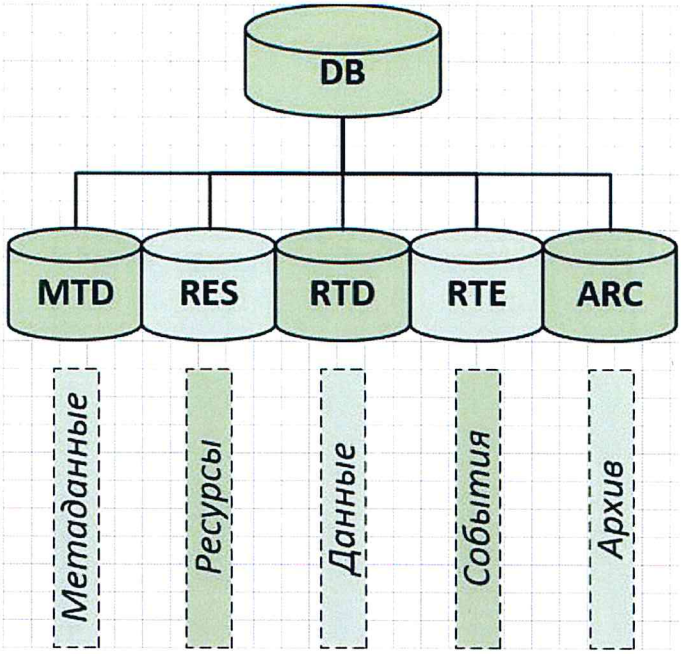


Рис. 29 – Структура доменов БД

3.3.4. Деление производится на основе комплекса признаков с целью оптимизации структуры под требования специфической функциональности.

Данное архитектурное решение обеспечивает:

– применение современных подходов на базе технологий ORM, которые позволяют гибко и надежно реализовать двунаправленное преобразование объектно-ориентированного подхода для представления сущностей предметной области в памяти прикладных процессов к реляционной модели представления в СУБД;

– применение современных методологий, компонент и инструментов с высокими значениями технических показателей, а также высокая доступность пула ресурса разработчиков;

– параллельное многопользовательское функционирование программных компонент из состава ПК обеспечивается посредством встроенных программных механизмов ACID – транзакционный многопользовательский доступ с гарантией изоляции, при котором транзакции одного пользователя не влияют на транзакции другого пользователя;

– высокую пропускную способность. Интеграция программных компонент из состава ПК посредством прямых подключений к БД обеспечивает обработку больших

объемов данных с гарантированным временем доступа. При необходимости, масштабируемость решения обеспечивается путем организации выделенного сервера СУБД с применением к нему соответствующих методов вертикального и горизонтального масштабирования;

– требуемый уровень показателей надежности реализуется:

а) на уровне программно-технических решений – посредством применения аппаратных и программных средств с соответствующими значениями показателей;

б) на организационном уровне – путем применения на стадии эксплуатации проектных плановых и внеплановых регламентов ТОиР;

в) на уровне архитектурного решения в части СУБД как единичной точки отказа в качестве СУБД применена система соответствующего класса;

– требуемый уровень показателей информационной безопасности реализуется посредством развитых методов централизованного применения основанных на корпоративных и юридических нормах политик информационной безопасности со сбалансированной гранулярностью на уровнях базы данных, таблиц и объектов данных. Предусмотрена возможность применения шифрования данных;

– требуемый уровень показателей обслуживаемости и контролепригодности реализуется посредством:

а) наличия соответствующего инструментария в составе СУБД,

б) наличия API для интеграции в смежные и вышестоящие уровни системного администрирования;

в) высокой степени документированности;

г) наличия развитой инфраструктуры поддержки программного продукта СУБД.

3.4. Связи с другими программами

3.4.1. Сервер предусматривает опциональный программно-технический

модуль, который реализует интерфейс открытых систем на базе семейства протоколов OPC:

– OPC UA;

– OPC DA;

– OPC AE;

– OPC HDA.

Указанный программный модуль обеспечивает интерфейс со сторонними программными системами и функционально входит в состав подсистемы обмена данными (SRV_DAQ).

3.4.2. Дополнительно к функциям управления конфигурацией и мониторингом состояния со стороны специализированных компонент из состава ПК, Сервер предусматривает интерфейсы интеграции в соответствующие системы уровня предприятия с целью обеспечения централизованного группового управления и мониторинга.

3.4.3. Для обеспечения и управления безопасностью аппаратных и программных компонент из состава Сервера предусмотрен интерфейс интеграции в системы управления информационной безопасностью (Security Capsule, RuSIEM, Microsoft SCCM):

– анализ и управление рисками безопасности;

– сбор, обработка и анализ событий безопасности;

– обнаружение атак и нарушений критериев и политик безопасности;

– централизованное управление аутентификацией и контролем доступа;

– антивирусная защита и защита от вредоносного кода;

– межсетевое экранирование;

– формирование отчетных документов безопасности.

3.4.4. Для управления конфигурацией аппаратных и программных компонент из состава Сервера предусмотрен интерфейс интеграции в системы управления конфигурацией ИТ-инфраструктур (Microsoft SCCM, Ansible, Chef):

– централизованное управление конфигурацией системных ресурсов сервера. Возможность интеграции с распределенными ресурсами СХД (iSCSI, Samba, Ceph, HDFS) с целью обеспечения требований производительности и надежности;

– централизованное управление конфигурацией системных ресурсов сервера. Возможность интеграции с распределенными ресурсами систем БД с целью обеспечения требований производительности и надежности;

– централизованное управление обновлениями программных компонент ОС;

– централизованное управление обновлениями компонент базового ПО;

– централизованное управление обновлениями программных компонент из состава ПК.

3.4.5. Для мониторинга состояния аппаратных и программных компонент из состава Сервера предусмотрен интерфейс интеграции в системы управления ИТ-инфраструктурой (Microsoft SCCM, Zabbix, Nagios):

– централизованное управление состоянием аппаратных компонент на базе SNMP;

– мониторинг состояния аппаратных компонент на базе SNMP и SNMP-ловушек;

– централизованное управление состоянием программных компонент на базе SNMP;

– мониторинг состояния программных компонент на базе SNMP и SNMP-ловушек;

– централизованный мониторинг журналов системных событий;

– SLA-мониторинг, формирование отчётов и тенденций;

– комплексная реакция на события с возможностью расширения за счёт выполнения внешних скриптов.

4. ИСПОЛЬЗУЕМЫЕ ТЕХНИЧЕСКИЕ СРЕДСТВА

4.1. ПК разработан для использования на ПЭВМ со следующими техническими характеристиками:

– процессор – не хуже IntelCore i5;

– объем установленной памяти DDR – не менее 4 Гб;

– объем жесткого диска – не менее 512 Гб;

– видеоконтроллер – интегрированный;

– количество разъемов LAN (RJ-45) – не менее 1;

– количество портов USB – не менее 3;

– клавиатура;

– манипулятор типа «мышь».

4.2. ПК разработан для использования на ПЭВМ, на которой должно быть установлено следующее лицензионное программное обеспечение и необходимые библиотеки:

– операционная система – кроссплатформенное решение, с возможностью работы на ОС Microsoft Windows и GNU/Linux;

– драйверы устройств – Windows на базе WDK/DDK, GNU/Linux Kernel 2.6+;

– количество графических блоков в библиотеке «виртуальных двойников» – не ограничено (ограничено размером HDD).

5. ВЫЗОВ И ЗАГРУЗКА

5.1. Описание установочного комплекта

5.1.1. Установочные комплекты, необходимые для установки Сервера, находятся на съемном носителе, входящем в состав ПК:

– SERVER_INSTALL.EXE – стартовый установочный комплект Сервера;

– INSTALL_SRV_SEC.EXE – установочный комплект сервера информационной безопасности;

– INSTALL_WS_SEC.EXE – установочный комплект АРМ администратора информационной безопасности;

– INSTALL_SRV_ADM.EXE – установочный комплект сервера системного администрирования;

– INSTALL_WS_ADM.EXE – установочный комплект АРМ системного администратора;

– INSTALL_SRV_RES.EXE – установочный комплект сервера управления ресурсами;

– INSTALL_SRV_DAQ.EXE – установочный комплект сервера обмена данными;

– INSTALL_SRV_APP.EXE – установочный комплект сервера прикладных задач;

– INSTALL_WS_APP.EXE – установочный комплект АРМ пользователя;

– POSTGRESQL.EXE – установочный комплект СУБД PostgreSQL.

Примечание – В комплект поставки входит лицензионное соглашение, которое поставляется на отдельном специализированном носителе с интерфейсом USB.

5.2. Подготовка к установке ПК

5.2.1. Перед установкой программы на ПЭВМ необходимо выполнить следующие действия:

– проверить соответствует ли ПЭВМ техническим требования, описанным в разделе 4;

– произвести развертывание и аттестацию функционирования аппаратных средств;

– проверить наличие:

а) учетной записи пользователя с привилегированными правами в ОС, на которую производится установка конфигурации;

б) полного установочного комплекта в соответствии с 5.1.1;

в) съемного носителя с лицензионным соглашением.

5.3. Установка ПК

5.3.1. Процесс установки ПО Сервера включает в себя следующие этапы:

– установить прилагаемый лицензионный ключ в свободный USB-порт компьютера;

– установить съемный носитель ПК в устройство считывания DVD-дисков;

– в программе «Проводник» операционной системы Windows открыть съемный носитель. «Проводник» выведет файлы, находящиеся на съемном носителе;

– запустить программу SERVER_INSTALL.EXE;

– дождаться открытия окна программы установки Сервера;

– в открывшемся окне внимательно ознакомиться с лицензионным соглашением на использование программы, после чего подтвердить свое согласие на использование программы путем установки отметки в поле «Я согласен с условиями лицензионного соглашения». Выполнить одно из следующих действий:

а) нажать кнопку «Далее» в случае согласия с условиями лицензии, сценарий установки перейдет к следующему шагу;

б) нажать кнопку «Отмена» в случае несогласия с условиями лицензии, программа установки будет закрыта, установка будет прервана;

– программа установки предложит выбор установочного пути Сервера. При необходимости изменения пути необходимо нажать кнопку «Обзор» и выбрать каталог установки. Для подтверждения выбранного пути нажать кнопку «Далее»;

– программа установки предложит указать для учетной записи, обладающей исключительным набором прав, имя и пароль[1)], а также запросит его подтверждение. Указать имя и пароль учетной записи, произвести подтверждение пароля, затем нажать кнопку «Далее»;

– программа установки запросит подтверждение создания учетной записи в диалоговом окне. Произвести подтверждение, нажав кнопку «Да», или вернуться к указанию имени и пароля учетной записи, нажав кнопку «Нет»;

– программа установки начнет копирование данных, сопровождаемое выводом информации в журнал установки;

– по завершению копирования программа уведомит об успешной установке Сервера. Нажать кнопку «Завершить».

[1)] Требования к имени и паролю:

– при вводе имени допускается использование латинских букв и цифр;
– регистр букв в имени не учитывается;
– имя должно содержать не менее 3 символов;
– при вводе пароля допускается использование букв, цифр и служебных символов;
– регистр букв в пароле учитывается;
– пароль должен содержать не менее 8 символов, в том числе:
а) буквы в верхнем и нижнем регистрах;
б) как минимум одну цифру;
в) как минимум один служебный символ.

Перечень принятых сокращений

ACID	–	Atomicity, Consistency, Isolation, Durability (атомарность, консистентность, изолированность, стойкость)
API	–	Application Programming Interface (программный интерфейс приложения)
APP	–	Application (приложение)
DAQ	–	Distributed data acquisition (система сбора данных)
GPL	–	Graphical Programming language (графический язык программирования)
LAN	–	Local Area Network (локальная вычислительная сеть)
MNT	–	Maintenance (техническое обслуживание)
ORM	–	Object-Relational Mapping (объектно-реляционное отображение)
RES	–	Resources (ресурсы)
SLA	–	Service Level Agreement (соглашение об уровне обслуживания)
SNMP	–	Simple Network Management Protocol (простой протокол сетевого управления)
SPL	–	Structured Programming Language (текстовый язык программирования)
UI	–	User Interface (пользовательский интерфейс)
VLAN	–	Virtual Local Area Network (виртуальная локальная сеть)
VPN	–	Virtual Private Network (виртуальная частная сеть)
WAN	–	Wide Area Network (глобальная компьютерная сеть)
АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
БД	–	база данных
ИТ	–	информационные технологии
ЛВС	–	локальная вычислительная сеть
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
ПЭВМ	–	персональная электронно-вычислительная машина
РЭА	–	радиоэлектронная аппаратура
СПО	–	специализированное программное обеспечение

СУБД – система управления базами данных

СХД – система хранения данных

ТОиР – техническое обслуживание и ремонт

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					