



АО "НТЦ ИТ РОСА"

**ПЛАТФОРМА
ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ЖИЗНЕННЫМ
ЦИКЛОМ ОПЕРАЦИОННЫХ СИСТЕМ
"РОСА ЦЕНТР УПРАВЛЕНИЯ"
Версия 2.4.0**

Описание применения

РСЮК.10121-09 31 01

Листов 16

Име. № подл.	Подпись и дата	Взам. инв. №	Име. № дубл.	Подпись и дата

2025

АННОТАЦИЯ

В настоящем документе содержится описание применения программного средства "Платформа централизованного управления жизненным циклом операционных систем "РОСА Центр Управления" РСЮК.10121-09 (далее – РОСА Центр Управления, Комплекс).

В документе представлена информация о назначении комплекса, областях и условиях его применения, а также о составе и функциях программных компонентов. Описаны условия применения комплекса, в том числе требования к программным и техническим средствам и устойчивости функционирования.

В разделе "Назначение программы" приведено описание назначения программы, возможности данной программы, а также ее основные характеристики и ограничения, накладываемые на область применения программы.

В разделе "Условия применения" определены условия, необходимые для выполнения программы (требования к необходимым для данной программы техническим средствам, и другим программам, а также требования организационного, технического и технологического характера).

В разделе "Описание задачи" обозначены задачи и методы ее решения.

В разделе "Входные и выходные данные" указаны общие характеристики входной и выходной информации.

При разработке документа использованы ссылки на следующие стандарты:

- ГОСТ Р 2.105-2019 "Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам";
- ГОСТ 2.601 "Единая система программной документации. Виды программных документов";
- ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов";
- ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам";
- ГОСТ 19.502-78 "Единая система программной документации. Описание применения".

Настоящий документ подготовлен в соответствии с технологической инструкцией "РОСА. Регламент формирования документации к программным продуктам" (шифр РСЮК.11001-02 90 01).

СОДЕРЖАНИЕ

Содержание.....	3
1 Назначение комплекса.....	4
1.1 Общие сведения.....	4
1.2 Возможности комплекса	4
1.3 Область применения.....	6
1.4 Состав комплекса	7
2 Условия применения.....	8
2.1 Требования к аппаратным средствам	8
2.1.1 Сервер РОСА Центр Управления	8
2.1.2 Сервер СИПА.....	8
2.2 Требования к сетевой инфраструктуре.....	9
2.3 Требования к программным средствам.....	10
2.4 Требования к персоналу	10
3 Описание задачи.....	11
3.1 Управление хостами	11
3.2 Управление конфигурациями	11
3.3 Мониторинг и оповещения	12
3.4 Отчеты и аудит	12
3.5 Управление комплексом	13
4 Входные и выходные данные	14
4.1 Входные данные	14
4.2 Выходные данные	14
Перечень сокращений	15

1 НАЗНАЧЕНИЕ КОМПЛЕКСА

1.1 Общие сведения

РОСА Центр Управления обеспечивает централизованное управление жизненным циклом гибридной ИТ-инфраструктуры корпоративного уровня, включающей инфраструктуру физической, виртуальной и частной облачной среды организации.

РОСА Центр Управления предоставляет пользователю следующие возможности для автоматизированного развертывания и конфигурирования управляемых хостов:

- осуществлять сетевое развертывание (установку ОС и настройку системной конфигурации) управляемых хостов (физических серверов и VM) в автоматическом режиме с применением сценариев развертывания Kickstart;
- осуществлять управление конфигурациями развернутых хостов;
- использовать графический веб-интерфейс для централизованного мониторинга и конфигурирования управляемых хостов.

1.2 Возможности комплекса

РОСА Центр Управления выполняет следующие функции:

- сбор сведений о первоначальной конфигурации аппаратной части хостов на момент установки клиентов;
- периодический опрос аппаратной части хостов с целью выявления изменений в составе и параметрах их аппаратной части;
- фиксация сведений об аппаратной части хостов в виде сохраняемых отчётов на дату опроса;
- хранение данных инвентаризации в течение не менее трех месяцев;
- настройка перечня инвентаризируемых аппаратных компонентов, а также их атрибутов;
- сбор перечня программного обеспечения;
- отображение сведений о программной части в виде отчётов с возможностью составления индивидуальных отчетов;
- сбор информации о файлах на локальных дисках хостов, подключенных к системе;
- оценка соответствия параметров хостов заданным шаблонам конфигурации;
- автоматическое присвоение группы для нераспределенных узлов;
- отображение результатов оценки в консоли администрирования в виде отчетов;

- управление содержимым, включая базовую ОС, службы промежуточного ПО и приложения конечных пользователей;
- управление различными типами содержимого на каждом этапе жизненного цикла ПО;
- управление подписками для поиска, доступа и загрузки содержимого из соответствующих репозитория;
- сбор информации об использовании программного обеспечения на основе информации о времени запуска и продолжительности работы исполняемых файлов приложений;
- хранение информации об использовании программного обеспечения;
- отображение собранной информации об использовании программного обеспечения в консоли администрирования в виде отчетов;
- доставка приложений или пакетов программного обеспечения до рабочих станций;
- запуск на рабочих станциях соответствующей программы установки для доставленного приложения или пакета программного обеспечения согласно заданному расписанию;
- отображение пользователям уведомлений об установке программного обеспечения и скрывание таких уведомлений при выполнении системных задач обслуживания;
- отображение и хранение сведений о процессе распространения программного обеспечения в виде отчетов с возможностью составления индивидуальных отчетов;
- установка операционной системы на хосты и серверы комплекса;
- выполнение сценариев развертывания операционной системы на новых и используемых ПК;
- миграция хостов на отечественную операционную систему;
- контроль процесса выполнения сценария в виде отчетов;
- установка обновлений как на все хосты, так и отдельно для заданной группы хостов;
- отображение пользователям уведомлений об установке обновлений программного обеспечения и своевременного предупреждения о необходимости перезагрузки хоста для завершения процесса установки;
- контроль процесса распространения обновлений в виде отчетов с возможностью составления индивидуальных отчетов;
- централизованный контроль цифровых ИТ-активов (лицензий);
- мониторинг и визуализация статусов сервисов компьютерной сети, серверов и сетевого оборудования ИТ-инфраструктуры;
- обеспечение работы подсистемы мониторинга;
- обеспечение работы подсистемы отображения;
- обеспечение работы подсистемы поиска и аналитики;

– интеграция с мобильными устройствами на ОС "РОСА Мобайл".

1.3 Область применения

РОСА Центр Управления может быть использован государственными и коммерческими средними предприятиями для централизованного управления жизненным циклом гибридной ИТ-инфраструктуры корпоративного уровня, включающей инфраструктуру физической, виртуальной и частной облачной среды.

Комплекс предназначен для использования системным администратором, пользователем и специалистом по техническому обслуживанию.

Квалификация системного администратора: высокий уровень знаний и наличие практического опыта выполнения работ по установке, настройке и администрированию программных средств, применяемых в комплексе, а также наличие профессиональных знаний и практического опыта в области системного администрирования.

Основными обязанностями системного администратора являются:

- установка, настройка и мониторинг работоспособности системного и базового программного обеспечения;
- инсталляция и настройка прикладного программного обеспечения;
- создание и изменение объектов службы каталогов;
- создание и изменение объектов политик;
- настройка локальной компьютерной сети и сетевого окружения;
- контроль доступа к сетевым ресурсам.

Квалификация специалиста по техническому обслуживанию: высокий уровень знаний и наличие практического опыта выполнения работ по установке, настройке и подключению компьютерного и серверного оборудования, применяемого в Системе, а также наличие профессиональных знаний и практического опыта в области технического обслуживания.

Основными обязанностями специалиста по техническому обслуживанию являются:

- а) модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих станций);
- б) конфигурирование и настройка программно-технических средств комплекса;
- в) диагностика типовых неисправностей.

Пользователи должны обладать знаниями и навыками работы в качестве пользователя персональных компьютеров в соответствии с Приложением к приказу Мининформсвязи России от 27.12.2005 г. № 147 "Об утверждении

квалификационных требований к федеральным государственным гражданским служащим и государственным гражданским служащим субъектов Российской Федерации в области использования информационных технологий".
Дополнительных требований к пользователям не предъявляется.

1.4 Состав комплекса

Комплекс включает в себя следующие основные структурные компоненты:

- подсеть;
- домен;
- настроенные и подготовленные к сетевой установке на управляемых хостах операционные системы РОСА "Кобальт", ROSA Enterprise Server, ROSA Linux, ALT Linux, Astra Linux, РЕД ОС;
- примеры групп хостов;
- настроенные ассоциации шаблонов развертывания;
- сервер Puppet;
- сервер Salt;
- Ansible;
- плагины управления вычислительными ресурсами систем виртуализации ROSA Virtualization, VMWare и Libvirt.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Требования к аппаратным средствам

2.1.1 Сервер РОСА Центр Управления

Требования к аппаратным средствам сервера, предназначенного для установки РОСА Центр Управления, приведены в таблице 1.

Таблица 1 – Требования к аппаратным средствам сервера РОСА Центр Управления

Параметр	Минимальное значение	Рекомендуемое значение
Количество ядер процессора	2	4
Объем оперативной памяти, Гбайт	8	20
Свободное дисковое пространство, Гбайт	40	80

Примечание – Для повышения производительности РОСА Центр Управления рекомендуется увеличить количество процессоров, а для ускорения работы подсистемы ввода-вывода (осуществление операций чтения-записи базы данных, ведение журналов и индексирование классов Puppet) рекомендуется использовать накопители SSD или иные носители высокой производительности.

Следует обратить внимание, что при увеличении количества управляемых хостов может потребоваться дополнительное дисковое пространство для хранения журналов.

2.1.2 Сервер СИПА

Требования к аппаратным средствам сервера, предназначенного для установки СИПА, приведены в таблице 2.

Таблица 2 – Требования к аппаратным средствам сервера СИПА

Параметр	Минимальное значение	Рекомендуемое значение
Количество ядер процессора	2	4
Объем оперативной памяти в Гбайт	8	20

Свободное дисковое пространство в Гбайт	20	40
---	----	----

2.2 Требования к сетевой инфраструктуре

Для функционирования комплекса следующие порты сервера РОСА Центр Управления должны быть открыты и доступны для входящих соединений, не должны использоваться другими службами или быть заблокированы межсетевым экраном:

- TCP/443 – HTTPS;
- TCP/4505, TCP/4506 – Salt;
- TCP/8140 – Puppet.

Для обеспечения внешней интеграции и обмена информацией серверу РОСА Центр Управления должны быть доступны конечные точки API используемой системы виртуализации (ROSA Virtualization, VMware).

Примечание – Сервер РОСА Центр Управления подключается к контролируемым хостам по протоколу SSH, используя по умолчанию порт TCP/22. Следует обратить внимание, что при использовании иного порта необходимо в процессе настройки РОСА Центр Управления добавить параметр `remote_execution_ssh_port`, в котором указать используемый номер порта для каждого такого хоста.

Для функционирования комплекса следующие порты сервера СИПА должны быть открыты и доступны для входящих соединений, не должны использоваться другими службами или быть заблокированы межсетевым экраном:

- TCP/80, TCP/443 – HTTP/HTTPS;
- TCP/389, TCP/636 – LDAP/LDAPS;
- TCP,UDP/88, TCP,UDP/464 – Kerberos;
- TCP,UDP/53 – DNS;
- UDP/123 – NTP.

Примечание – Дополнительно сервер СИПА может анализировать порт 8080 и – в некоторых конфигурациях – порты 8443 и 749. Указанные три порта используются для внутренних подключений и внешний доступ к ним не требуется. Рекомендуется не открывать порты 8080, 8443, 749 и заблокировать их с помощью межсетевого экрана для входящих соединений.

2.3 Требования к программным средствам

Доступ к веб-интерфейсу РОСА Центр Управления осуществляется с внешней рабочей станции через один из следующих рекомендуемых браузеров актуальной версии:

- Google Chrome;
- Microsoft Edge;
- Apple Safari;
- Mozilla Firefox, в том числе Mozilla Firefox ESR;
- Яндекс.Браузер.

2.4 Требования к персоналу

Системный администратор, осуществляющий процесс установки и первичной настройки, эксплуатацию и техническое обслуживание РОСА Центр Управления, должен обладать опытом развертывания и сопровождения серверных версий ОС Linux, совместимых с диалектом Red Hat® Enterprise Linux, таких как РОСА “Хром” Сервер, CentOS и тому подобных.

Квалификация системного администратора: высокий уровень знаний и наличие практического опыта выполнения работ по установке, настройке и администрированию программных средств, применяемых в комплексе, а также наличие профессиональных знаний и практического опыта в области системного администрирования.

Основными обязанностями системного администратора являются:

- а) установка, настройка и мониторинг работоспособности системного и базового программного обеспечения;
- б) инсталляция и настройка прикладного программного обеспечения;
- в) настройка локальной компьютерной сети и сетевого окружения;
- г) контроль доступа к сетевым ресурсам;
- д) техническое обслуживание комплекса, включающее обновление версий, резервное копирование и восстановление данных.

3 ОПИСАНИЕ ЗАДАЧИ

Комплекс РОСА Центр Управления предназначен для централизованного управления жизненным циклом гибридной ИТ-инфраструктуры корпоративного уровня

Графический веб-интерфейс комплекса используется для централизованного мониторинга и конфигурирования управляемых хостов. При этом доступ пользователей к элементам интерфейса РОСА Центр Управления и к функциональным возможностям операционного управления хостами реализован с применением ролевой модели.

В каждой рабочей области комплекса веб-интерфейса реализован механизм поиска, при этом объекты поиска варьируются в зависимости от контекста страницы с возможностью сложных запросов, созданных с использованием специальных операторов и символов.

3.1 Управление хостами

Функционал управления хостами предназначен для осуществления следующих операций:

- развертывание новых хостов под контролем РОСА Центр Управления выполняется в автоматическом режиме с применением стандартизированного сценария развертывания Kickstart;
- регистрация существующих хостов в РОСА Центр Управления;
- создание собственных групп хостов (в дополнение к группам, созданным в РОСА Центр Управления по умолчанию) для группировки управляемых хостов по различным признакам с целью единовременного применения конфигурационных настроек сразу к группе однотипных хостов;
- добавление хоста в группу и исключение из нее;
- получение информации о состоянии конкретного хоста и развернутой на нём конфигурации.

3.2 Управление конфигурациями

Управление конфигурациями хостов осуществляется с помощью модулей Ansible и/или Puppet для автоматизированного управления конфигурациями контролируемых хостов РОСА Центр Управления путем дистанционного запуска плейбуков на этих хостах.

Плейбук, запущенный на управляемом хосте, выполняет по очереди заданный набор всех ролей модуля, которые были выбраны пользователем для этого хоста. При этом каждая роль представляет собой отдельный исполняемый командный сценарий, осуществляющий определенную настройку конфигурации хоста.

В Комплексе реализован механизм миграции хостов на отечественную ОС с использованием классов Puppet.

3.3 Мониторинг и оповещения

РОСА Центр Управления осуществляет в автоматическом режиме постоянный сбор данных о значениях разнородных элементов информации (параметров, статусов, событий и тому подобных), связанных с функционированием комплекса. При этом каждый контролируемый элемент информации является отдельной метрикой мониторинга, а визуализация полученных данных осуществляется для пользователя на специально предназначенной панели мониторинга.

Оповещения (сообщения, предупреждения) о контролируемых событиях РОСА Центр Управления отображаются в интерфейсе комплекса, а также (при необходимости и соответствующих настройках) оповещения могут быть отправлены пользователю по электронной почте.

3.4 Отчеты и аудит

Комплекс позволяет формировать отчеты из предустановленных шаблонов в форматах CSV, JSON, YAML, HTML, а также (при необходимости и соответствующих настройках) отчет может быть отправлен пользователям по электронной почте.

Интерфейс РОСА Центр Управления предоставляет пользователю возможность для проведения аудита событий (изменений), произошедших в процессе функционирования комплекса за определенный период времени. При этом регистрация отслеживаемых изменений осуществляется в журнале аудита согласно предустановленным системным правилам аудита.

Автоматизированный сбор информации о программной и аппаратной конфигурациях хостов производится с использованием классов Puppet, при этом существует возможность дополнять собранную информацию записями на языке системы управления YAML.

3.5 Управление комплексом

Интеграция комплекса со службой каталогов LDAP сервера СИПА (или иной внешней службой каталогов LDAP) позволяет осуществлять аутентификацию пользователей по протоколу LDAP/LDAPS в РОСА Центр Управления. Кроме того, при наличии политики периодической смены паролей обеспечивается стойкость и регулярная смена паролей пользователей РОСА Центр Управления через внешнюю службу каталогов.

В РОСА Центр Управления реализована ролевая модель пользователей.

Интеграция комплекса с внешней системой виртуализации (ROSA Virtualization, VMware) позволяет в процессе развертывания новых хостов создавать ВМ напрямую через веб-интерфейс РОСА Центр Управления.

Для рассылки сообщений пользователям по электронной почте сервер РОСА Центр Управления интегрируется с внешним почтовым SMTP-сервером или настроен в качестве локального почтового агента МТА.

Периодическое создание резервной копии данных позволяет сохранять актуальную конфигурацию и различные типы данных РОСА Центр Управления и, в случае возникновения внештатной ситуации (в том числе при повреждении файлов ПО комплекса), осуществлять восстановление необходимых данных из резервной копии.

Процедуры создания резервной копии и восстановления данных осуществляются пользователем комплекса в терминальном окне хоста РОСА Центр Управления.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 Входные данные

Входными данными являются:

- перечень хостов, групп, конфигураций и параметров, управляемых комплексом;
- автоматически получаемые сведения о программно-аппаратной конфигурации и иные сведения о хостах;
- перечень автоматических процессов, запускаемых на хостах.

4.2 Выходные данные

Выходными данными являются:

- мониторинг доступности хостов, оповещения (сообщения, предупреждения) о контролируемых событиях;
- отчеты по предустановленным шаблонам о состоянии программно-аппаратных конфигураций и статистических данных комплекса;
- журнал аудита согласно предустановленным системным правилам аудита;
- уведомления в режиме реального времени о статусе выполнения автоматических процессов, об ошибках;
- отчет об успешности выполнения автоматических процессов на определенный момент времени, данные о произошедших ошибках.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
ВМ	Виртуальная машина
ИТ	Информационные технологии
ОС	Операционная система
ПО	Программное обеспечение
СИПА	Система идентификации, политик и аудита
ЦС	Центр сертификации
API	Application programming interface – программный интерфейс приложения
CA	Certification authority – центр сертификации (удостоверяющий центр)
DHCP	Dynamic host configuration protocol – протокол динамической настройки сетевой конфигурации хоста
DNS	Domain name system – система доменных имен
ESR	Extended support release – релиз с расширенной (долговременной) поддержкой
HTTP	Hypertext transfer protocol – протокол передачи гипертекста
HTTPS	Hypertext transfer protocol secure – защищенная версия протокола передачи гипертекста
IANA	Internet assigned numbers authority – организация по управлению адресами в сети Интернет
IETF	Internet engineering task force – инженерный совет сети Интернет
IP	Internet protocol – протокол межсетевого взаимодействия
IPA	Identity, policy and audit – система идентификации, политик и аудита (СИПА)
LDAP	Lightweight directory access protocol – протокол доступа к каталогам
LDAPS	Lightweight directory access protocol secure – защищенная версия протокола доступа к каталогам
MAC	Media access control – уникальный идентификатор сетевого оборудования
mDNS	Multicast DNS – многоадресный DNS
NTP	Network time protocol – протокол сетевого времени
SSD	Solid state drive – твердотельный накопитель
SSH	Secure shell – защищенная оболочка

Сокращение	Определение
SSL	Secure sockets layer – уровень защищенных сокетов
TCP	Transmission control protocol – протокол управления передачей данных
TFTP	Trivial file transfer protocol – протокол передачи файлов
UDP	User datagram protocol – протокол пользовательских датаграмм
URL	Uniform resource locator – сетевой адрес ресурса