



RuBackup

**Система резервного копирования
и восстановления данных**

ОСНОВНЫЕ СВЕДЕНИЯ

ВЕРСИЯ 2.7.0.0.0, 14.10.2025

Содержание

Поддерживаемые продукты	4
Преимущества	5
1. Функции	6
1.1. Надежность и производительность	6
1.2. Автоматизация	6
1.3. Управляемость	6
1.4. Безопасность	7
2. Ключевые понятия	8
3. Архитектура и инфраструктура	11
3.1. Элементы инфраструктуры СРК	12
Клиент резервного копирования	12
Основной сервер	13
Резервный сервер	13
Медиасервер	14
Служебная база данных	14
3.2. Минимальная конфигурация	15
3.3. Управление хранением	15
4. Зависимости пакетов RuBackup	17
5. Способы установки	18
5.1. Локальная установка	18
5.2. Распределённая установка	18
5.3. Сравнение способов установки	19
5.4. Как выбрать?	19
6. Способы управления	21
6.1. Локальное управление	21
6.2. Централизованное управление	21
7. Многопользовательская модель	22
7.1. Суперпользователь	22
7.2. Супервайзер	24
7.3. Сопровождающий	24
7.4. Администратор	24
7.5. Аудитор	24
8. Хранилища секретов	25
8.1. Подготовка к использованию	26
8.2. Добавление хранилища секретов	27

8.3. Добавление метода получения секрета	28
8.4. Настройка доступа пользователей к хранилищу секретов	28
9. Удаленное логирование	30
9.1. Преимущества использования Syslog	30
9.2. Syslog в CPK RuBackup	30
9.3. Интеграция с SIEM-системами в CPK RuBackup	31
9.4. Установка и настройка	31
9.4.1. Установка и настройка сервера syslog-ng	31
Установка	31
Настройка	32
9.4.2. Установка и настройка сервера rsyslog	34
Установка	34
Настройка	34
9.5. Настройка удаленного логирования в интерфейсе	35
9.5.1. Настройка логирования в RBM	36
9.5.2. Настройка логирования в Tuscana	37
9.6. Настройка <code>rb_syslog_reporter</code>	38
9.6.1. Настройка конфигурационного файла <code>rb_siem.conf</code>	38
9.6.2. Настройка планировщика событий Linux	38
Приложение А: События информационной безопасности	39
Приложение Б: Конфигурационный файл <code>rb_siem.conf</code>	40

Система резервного копирования RuBackup — клиент-серверное приложение, которое:

- автоматически выполняет резервное копирование СУБД, виртуальных машин, почтовых систем, файловых систем, подсистемы Linux и службы каталогов;
- восстанавливает данные из резервных копий по запросу.

Полностью российская разработка с возможностью гибкой адаптации под требования заказчика.

Для быстрого создания системы обеспечения сохранности данных используйте программный комплекс [RuBackup OneClick](#). Продукт ориентирован на малый, средний бизнес и территориально распределенные организации.

Поддерживаемые продукты

СУБД	Системы виртуализации (безагентный способ)	Почтовые системы
Tantor Special Edition (с использованием модуля PostgreSQL) Arenadata Greenplum Microsoft SQL Server MySQL Oracle Database PostgreSQL + в кластере Patroni Postgres Pro SAP HANA YandexDB РЕД База Данных	ПК СВ «Брест» VMmanager Альт Виртуализация (с использованием модуля Proxmox VE) АЭРОДИСК vAir P-Виртуализация РУСТЭК Basis DynamiX Enterprise KVM Microsoft Hyper-V OpenStack oVirt/zVirt/REDVirt Proxmox VE ROSA Space VM Tionix VMware vSphere	RuPost CommuniGate Pro Mailion VK Workmail Microsoft Exchange
Файловые системы	Подсистема Linux	
Linux (Ext4, Ext3, Ext2, XFS, ZFS, BTRFS) Windows (NTFS)	LVM Linux	
Службы каталогов	Хранилища	
ALD Pro FreelPA MS AD	Файловые хранилища Блочные устройства Облачные хранилища Ленточные библиотеки Клиентские хранилища	

Преимущества

- Лучшая производительность среди российских решений
- Сертификат соответствия ФСТЭК России №4879
- Единственное решение с многопоточностью — на всех этапах позволяет выполнять самые жесткие требования к срокам RPO и RTO
- Широкие возможности интеграции — полнофункциональный REST API, толстый клиент и Web, CLI, документация для интеграторов и клиентов
- Надежность и масштабируемость — встроенные алгоритмы кластеризации и балансировки нагрузки между узлами СРК, резервирование собственных компонентов СРК
- Глубокая интеграция с Postgres — поддержка инкрементальных и дифференциальных копий (PTRACK, DELTA, PAGE), использование механизмов работы с томами (LVM и аппаратные снапшоты)

Быстрый старт

Начните работу в корпоративной среде

Глава 1. Функции

1.1. Надежность и производительность

- Полное, инкрементальное и дифференциальное [резервное копирование](#)
- [Хранение](#) резервных копий в СХД, ленточных библиотеках, облаке S3
- Автоматическая [верификация](#) резервных копий (размер файлов, md5sum, электронная подпись)
- [Сжатие](#) резервных копий на клиенте СРК или на сервере
- [Срочное резервное копирование](#) по инициативе клиента СРК или администратора
- Параллелизм — количество одновременных сессий ограничено только аппаратными характеристиками сервера. Параллельные сессии доступны как для СРК в целом, так и для отдельного клиента

1.2. Автоматизация

- Аналитика — построение плана резервного копирования с прогнозированием требуемых ресурсов
- Экономия дискового пространства — автоматическое перемещение резервных копий на другие носители и удаление устаревших копий
- Балансировка нагрузки — распределение копий по разным хранилищам в зависимости от выбранной политики
- Глобальное расписание — автоматическое создание резервных копий клиентских устройств
- Локальное расписание — клиенты могут управлять резервным копированием самостоятельно
- Стратегии резервного копирования — автоматические групповые операции с клиентами СРК

1.3. Управляемость

- Полноценное управление СРК из [командной строки](#) (CLI)
- Графические приложения для [клиента](#) и для [администратора](#) СРК
- [Веб-приложение](#) для администратора СРК, адаптированное под мобильные устройства
- Взаимодействие с СРК через [REST API](#)

1.4. Безопасность

- [Многопользовательская модель](#) администрирования
- Локальный лист запретов (с regex) для каждого клиента, ограничивающий доступную для копирования информацию
- Защитное преобразование резервных копий по [алгоритмам](#) ГОСТ 34-12-2015 (Kuznyechik), Anubis, ARIA, CAST6, Camellia, Kalyna, MARS, AES, Serpent, Simon, SM4, Speck, Treefish, Twofish
- Интеграция с [хранилищем секретов](#)
- [Рассылка уведомлений](#) пользователям о событиях в СРК
- [Протоколирование](#) всех действий администратора и пользователей в базе данных и системном журнале

Глава 2. Ключевые понятия

Серверная группировка RuBackup состоит из основного сервера, необязательного резервного сервера и медиасерверов. В простейшем случае медиасервером является основной сервер резервного копирования (а также резервный сервер, при наличии).

Клиент системы резервного копирования — это отдельный сервер, компьютер или виртуальная машина, на которой установлено клиентское ПО RuBackup для выполнения резервного копирования. Для удобства клиенты могут быть объединены в **группы клиентов**.

На программном уровне сервером RuBackup называется также фоновый процесс (сервис) на сервере СРК, а клиентом RuBackup — фоновое клиентское ПО.

Хранение данных резервных копий (архивов) реализовано в виде хранилищ (storage). Каждое **хранилище** входит в определенный **пул**. Пул — это логическое объединение однотипных устройств хранения резервных копий. Каждый **пул** принадлежит определенному **медиасерверу**. Таким образом, организация хранения данных резервных копий имеет следующую структуру:

Медиасервер → Пул → Хранилище

Метаданные резервных копий хранятся в **репозитории**. Непосредственно **резервные копии** располагаются в **хранилищах** резервных копий, которые ассоциированы с **пулами** хранения резервных копий. Хранилища бывают пяти типов:

1. файловая система;
2. ленточная библиотека;
3. облако;
4. блочные устройства;
5. определяемые клиентом.

Все действия СРК реализованы в виде **задач**, которые объединены в **очереди задач**, в зависимости от типа.

Периодические задания резервного копирования и восстановления данных реализованы в виде **правил глобального расписания**, которые входят в **глобальное расписание** резервного копирования ([Рисунок 1](#)).

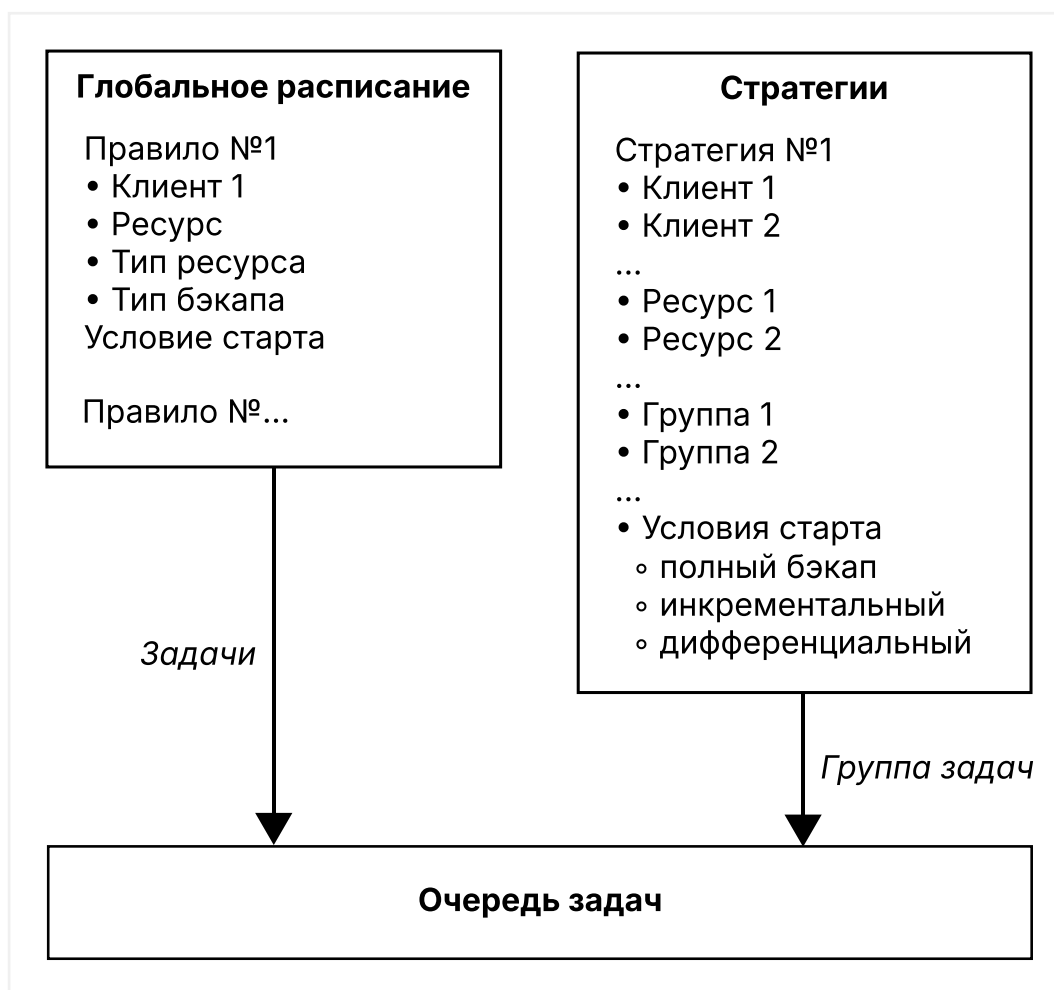


Рисунок 1. Глобальное расписание, стратегии и очередь задач

Одновременные действия над группами ресурсов реализованы в виде **стратегий**, которые создают **задачи** резервного копирования в соответствии с **расписаниями** для всех ресурсов и клиентов, которые их касаются.

Система уведомлений RuBackup использует **пользователей** и **группы пользователей** RuBackup для уведомления о событиях системы резервного копирования.

Автономный режим работы клиента — использование клиента СРК RuBackup без сервера резервного копирования. При этом сохраняется возможность использования некоторых клиентских функциональных модулей для создания резервных копий. Чтобы узнать, поддерживается ли использование модуля в автономном режиме, запустите исполняемый файл модуля с опцией `--autonomous` и проверьте код возврата.

Пример 1. Команда проверки поддержки автономного режима для модуля `rb_module_filesystem`

```
sudo /opt/rubackup/modules/rb_module_filesystem --autonomous
```

Пример 2. Команда проверки кода возврата

```
echo $?
```

Код возврата `0` говорит о том, что модуль поддерживает автономный режим. Другие коды возврата говорят о том, что автономный режим не поддерживается.

Неинтерактивный режим работы — режим для сценариев массового развертывания, например при использовании Ansible.



Резервный сервер и медиасервер не функционируют с тестовой лицензией!

Глава 3. Архитектура и инфраструктура

Архитектура системы резервного копирования (СРК) — программные компоненты СРК и их связи между собой.

Инфраструктура СРК — физические или виртуальные машины (узлы), на каждом из которых может быть установлен один или более программных компонентов СРК, и связи между ними.

Элементы инфраструктуры СРК:

- обязательные:
 - [основной сервер](#);
 - [служебная база данных](#).
- опциональные:
 - [клиент резервного копирования](#) (клиент РК);
 - [резервный сервер](#);
 - [медиасервер](#).

На одном узле может быть установлено более одного программного компонента СРК (один узел может выполнять функции нескольких элементов инфраструктуры СРК). Если в инфраструктуре СРК более одного узла, между этими узлами должна быть обеспечена связь по протоколу TCP.

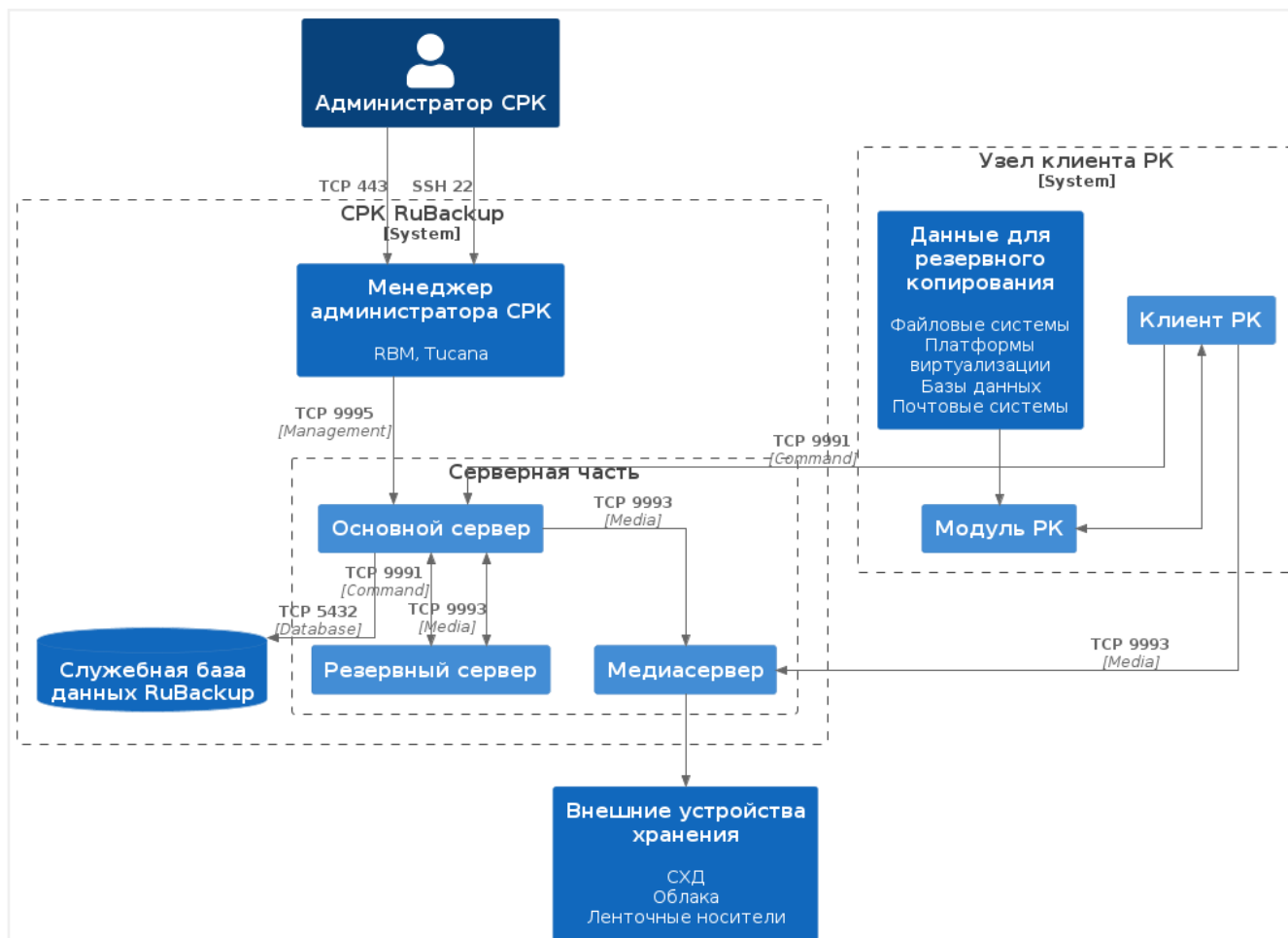


Рисунок 2. Условная схема инфраструктуры CPK RuBackup

3.1. Элементы инфраструктуры CPK

Клиент резервного копирования

Клиент PK — узел, на котором

- доступен ресурс, для которого выполняется резервное копирование;
- установлен пакет `rubackup-client`;
- обеспечен сетевой доступ к серверу;
- обеспечен сетевой доступ к медиасерверу (при наличии).

У клиента PK есть *модули*. Модуль клиента PK — подключаемый программный компонент, который отвечает за резервное копирование и восстановление ресурса определенного типа (например, блочных устройств или базы данных) и упаковку резервных копий.

Модули, устанавливаемые по умолчанию вместе с программным компонентом `rubackup-client`, позволяют резервировать [Резервное копирование и восстановление файловых систем Linux](#) и [Резервное копирование и восстановление логических томов Linux](#).

Клиент РК отвечает за взаимодействие с сервером *RuBackup* с одной стороны, и с модулями резервного копирования и восстановления — с другой.

API модулей резервного копирования является открытым и может быть использован для разработки модулей третьими лицами.

Клиенты РК могут быть объединены в группы.

Взаимодействие в системе резервного копирования обеспечивает основной сервер резервного копирования либо резервный сервер, если он функционирует в режиме замещения основного сервера.

Основной сервер

Основной сервер — узел, на котором

- установлены пакеты `rubackup-server` и `rubackup-client`;
- обеспечен сетевой доступ к клиенту РК;
- обеспечен сетевой доступ к медиасерверу (при наличии).

Основной сервер — главный управляющий сервер, обеспечивающий взаимодействие элементов СРК. Основной сервер хранит информацию о том, что и куда сохранено, а также как восстановить информацию.

Основной и резервный серверы включают в себя функции медиасервера.

Основной сервер выполняет функцию медиасервера при установке способом «Всё в одном», в процессе которой все программные компоненты СРК *RuBackup* устанавливаются на одном узле.

Резервный сервер

При обслуживании высококритичных сервисов система резервного копирования может быть дополнена резервным сервером.

Резервный сервер — узел, на котором

- установлены пакеты `rubackup-server` и `rubackup-client`;
- обеспечен сетевой доступ к клиенту РК;
- обеспечен сетевой доступ к медиасерверу (при наличии).


Резервный сервер выполняет функции основного сервера, если основной сервер становится недоступен. В случае отказа основного сервера клиенты РК автоматически подключаются к резервному серверу. После восстановления функционирования основного сервера клиенты РК вернуться к работе с основным сервером.

Решение об использовании резервного сервера принимается *клиентом РК* немедленно.

ленно, если основной сервер не отвечает на запрос *при выполнении операции*.

Если клиент РК не выполняет операций, требующих ответа сервера, он не получит информации об отказе основного сервера.

При недоступности основного сервера подключите [Менеджер администратора RuBackup \(RBM\)](#) или [Tucana](#) к резервному серверу.

В графических интерфейсах управления недоступный сервер будет отмечен знаком в разделе  **Серверы RuBackup**.

Медиасервер

Медиасервер — узел, обеспечивающий хранение резервных копий в доступных ему хранилищах, на котором

- установлены пакеты `rubackup-server` и `rubackup-client`;
- обеспечен сетевой доступ к клиенту РК.

Медиасервер:

- получает резервные копии от клиентов РК;
- хранит резервные копии;
- передает клиентам РК резервные копии по запросу.

Основной и резервный серверы включают в себя функции медиасервера.

При увеличении количества клиентов РК, а также при увеличении количества ресурсов, на которых предполагается хранить резервные копии, могут возникнуть задачи распределения нагрузки. В этом случае в серверную группировку могут быть добавлены медиасерверы, с помощью которых можно перераспределить задачи резервного копирования на несколько серверов резервного копирования или построить иерархическую систему хранения резервных копий.

Служебная база данных

В служебной базе данных хранится информация о:

- глобальных настройках резервного копирования;
- клиентах РК;
- глобальном расписании;
- стратегиях;
- репозитории резервных копий и пр.

Служебная БД хранится в СУБД PostgreSQL или Tantor с именем по умолчанию

rubackup.

Служебная база данных может находиться как на одном узле с сервером, так и на отдельном узле (машине).

Для изменения большинства параметров конфигурации СРК не требуется останавливать СРК и редактировать файлы настроек. Изменения производятся с помощью штатных [средств администрирования RuBackup](#).

3.2. Минимальная конфигурация

В минимальной конфигурации СРК *RuBackup* состоит из:

- одного сервера;
- одного клиента РК, установленного на том же узле, на котором работает сервер резервного копирования.

В минимальной конфигурации единственный сервер резервного копирования взаимодействует с клиентом РК, координирует задания СРК и хранит резервные копии на доступных ему (как медиасерверу) ресурсах: файловых системах, картриджах ленточных библиотек и облачных сервисах.

Развертывание СРК *RuBackup* в этой конфигурации описано в разделе [Быстрый старт](#).



Для использования *RuBackup* в продуктивных окружениях среднего и промышленного масштаба, а также для проведения нагрузочных испытаний, рекомендуем разворачивать *RuBackup*, включая служебную базу данных *RuBackup*, на отдельных машинах с рекомендуемой конфигурацией ([Системные требования](#)). Это позволит достичь максимальных показателей производительности и выполнить резервное копирование, восстановление и удаленную репликацию данных в кратчайшие сроки.

3.3. Управление хранением

Система резервного копирования может быть настроена таким образом, что резервные копии будут перемещаться на другие устройства хранения (например с дискового устройства хранения на картридж ленточной библиотеки) по достижении определенного срока хранения.

Общий объем резервных копий, хранящихся в системе резервного копирования, может быть ограничен для клиента РК, для правила резервного копирования, а также для стратегии резервного копирования.

Устаревшие резервные копии могут быть удалены из СРК автоматически. Сообщение о том, что устаревшие копии следует удалить, может быть отправлено

администраторам СРК.

Глава 4. Зависимости пакетов RuBackup

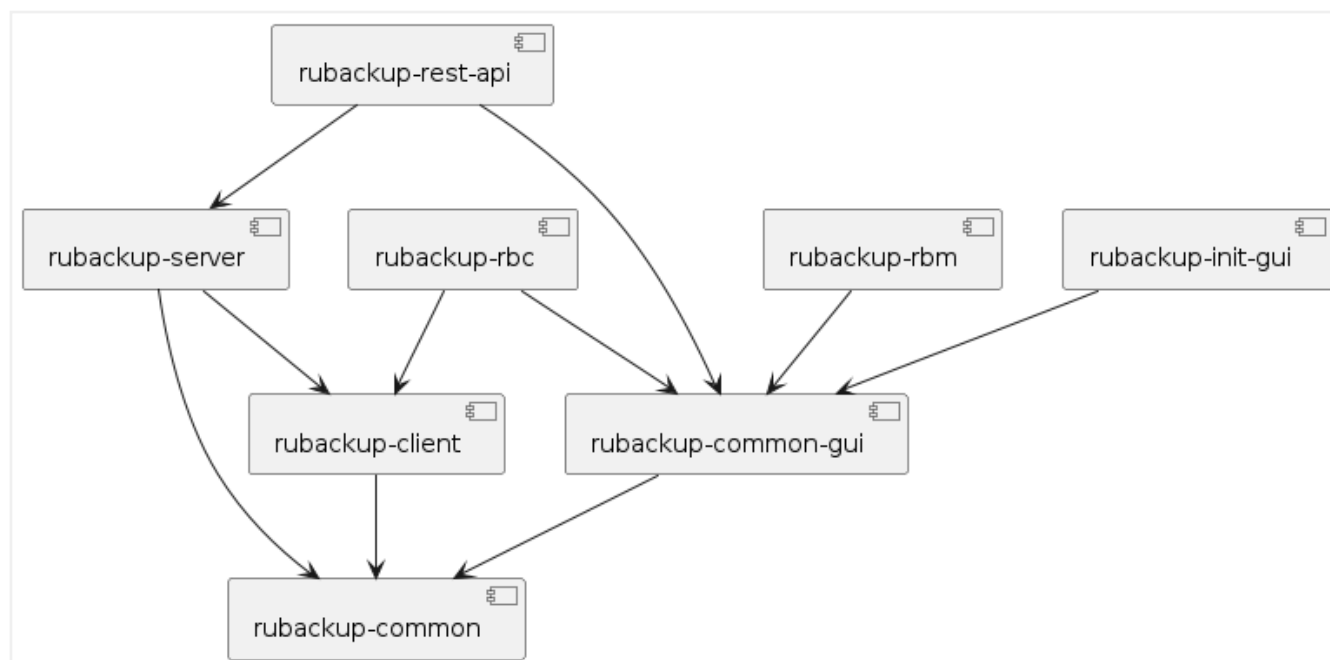


Рисунок 3. Зависимости пакетов RuBackup

Глава 5. Способы установки

Способы установки СРК:

- локальная;
- распределённая.

5.1. Локальная установка

Локальная установка означает, что все компоненты СРК развёртываются на одном узле (сервере, компьютере или виртуальной машине).

Сервер, база данных, клиент РК и модули работают в рамках одного узла.

Преимущества

- Простота развёртывания. Не требует настройки сети и настройки компонентов на каждом узле.
- Автономность.
- Подходит для тестирования или небольших систем.

Недостатки

- Масштабируемость. Резервируемые источники данных в пределах одного узла. При высокой нагрузке ресурсы одного медиасервера могут быть недостаточны.
- Отказоустойчивость. Выход из строя основного сервера приводит к полной недоступности СРК.

5.2. Распределённая установка

Распределённая установка — развёртывание компонентов СРК на нескольких узлах, связанных между собой через сеть.

Каждый узел выполняет свою функцию. Примеры:

- служебная база данных;
- основной сервер;
- резервный сервер;
- медиасервер;
- клиент РК 1;
- клиент РК 2;

- АРМ администратора.

Преимущества

- Масштабируемость. Можно добавлять новые узлы для обработки растущей нагрузки (горизонтальное масштабирование).
- Отказоустойчивость. Если основной сервер выйдет из строя, то его функции продолжит выполнять резервный сервер.
- Гибкость. Можно резервировать разные данные.
- Оптимизация ресурсов. Каждый сервер специализируется на своей задаче (например, хранение данных).

Недостатки

- Сложность настройки. Необходимы настройка каждого компонента на узлах, сетевые настройки, синхронизация данных;
- Усложнённое управление. Необходимо мониторить все узлы, обеспечивая безопасность, балансировать нагрузку.

5.3. Сравнение способов установки

Таблица 1. Сравнение способов установки СРК RuBackup

Критерий	Локальная установка	Распределённая установка
Масштабируемость	Ограничена ресурсами одного сервера	Масштабируется добавлением узлов
Отказоустойчивость	Низкая (единая точка отказа)	Высокая (дублирование)
Производительность	Зависит от одного клиента РК	Распределение нагрузки между узлами
Сложность	Простота развёртывания	Требует настройки сети и координации

5.4. Как выбрать?

Когда лучше выбрать распределённую установку?

- Высокие нагрузки (разнообразие резервируемых ресурсов).
- Критическая отказоустойчивость.
- Гибкость архитектуры.

Когда лучше выбрать локальную установку?

- Тестирование, разработка.
- Небольшие проекты с низкой нагрузкой.
- Быстрое развёртывание без сложной архитектуры.

Глава 6. Способы управления

Возможные способы управления:

- локальное;
- централизованное.

6.1. Локальное управление

Локальное управление резервным копированием и восстановлением данных выполняется на клиенте ПК одним из инструментов, установленным на этом же узле:

- [Менеджер администратора RuBackup \(RBM\)](#);
- [Менеджер клиента RuBackup \(RBC\)](#);
- [Утилиты командной строки](#).

6.2. Централизованное управление

Централизованное управление резервным копированием и восстановлением данных клиента ПК выполняется на любом удалённом узле, имеющем сетевой доступ к узлам компонентов СРК:

- [Tucana](#);
- [Утилиты командной строки](#);
- [Менеджер администратора RuBackup \(RBM\)](#).



Рекомендуем включить функцию централизованного восстановления на клиенте ПК. Это позволит управлять восстановлением данных на клиенте удаленно через приложение [Менеджер администратора RuBackup \(RBM\)](#).

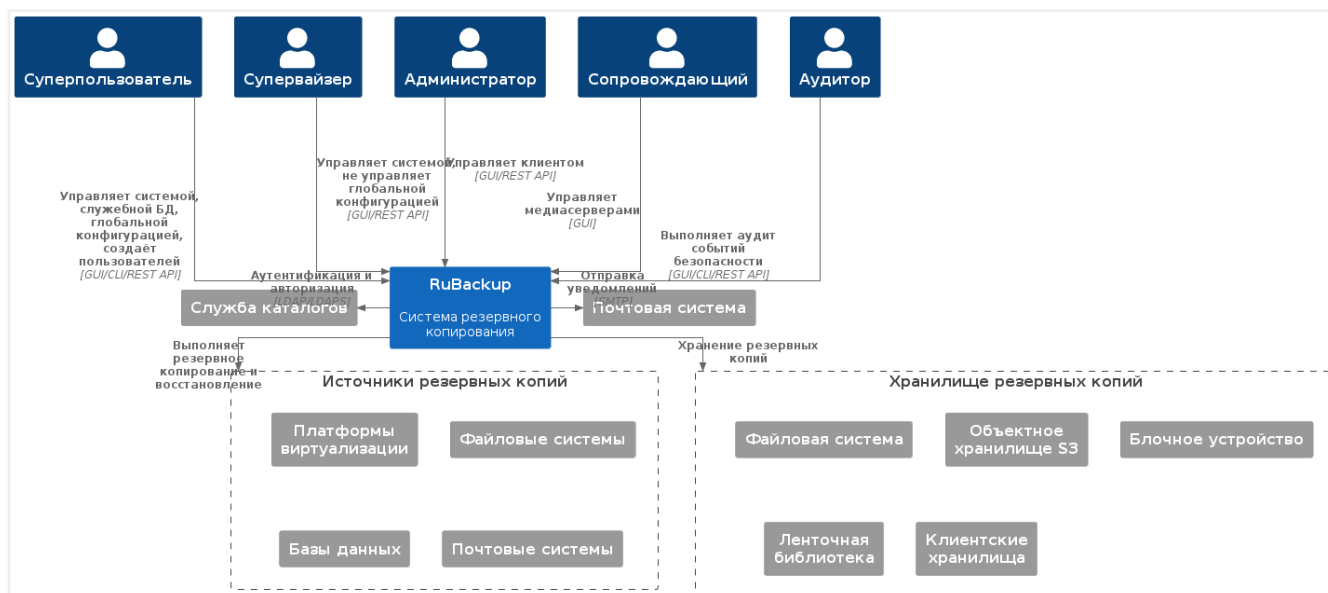
1. Откройте конфигурационный файл клиента ПК `/opt/rubackup/etc/config.file` (Linux) или `C:\RuBackup-win-client\etc\config.file.txt` (Windows).
2. Установите значение `yes` параметра `centralized-recovery`. Сохраните изменения.
3. Перезапустите клиент ПК.

Глава 7. Многопользовательская модель

В СРК RuBackup реализован многопользовательский режим работы, т. е. назначение типа пользователя и предоставление ему набора полномочий для выполнения определенных рабочих задач в соответствии с его ролью.

В СРК RuBackup предусмотрены следующие типы пользователей:

1. суперпользователь (владелец базы данных RuBackup);
2. супервайзер;
3. сопровождающий;
4. администратор;
5. аудитор.



7.1. Суперпользователь

Суперпользователь является привилегированным администратором, которому позволены любые действия в СРК. Суперпользователь создаётся при конфигурации основного сервера. Имя суперпользователя и пароль задаются также при настройке. Чтобы поменять пароль суперпользователя в конфигурационном файле сервера, используйте команду:

```
rb_init --passwd
```

```
root@rbs:~# rb_init --passwd
RuBackup initialization utility
Copyright 2018-2022: LLC "RUBACKUP"
```

```

Исключительные права принадлежат 000 "РУБЭКАП"
Author is Andrey Kuznetsov
Version: 2.0 Build: 48024de
password found in /opt/rubackup/etc/config.file

Please enter old password:
Enter new password:
Repeat password:
  Copy old config file to: /opt/rubackup/etc/config.file.old.2024-Jan-18H16-
05-32
Password was changed successfully
root@rbs:~#

```

Для смены пароля в служебной базе данных `rubackup`:

1. Подключитесь к базе данных, используя пользователя `rubackup` или `postgres`, с помощью команды:

```
sudo -u rubackup psql
```

или

```
sudo -u postgres psql
```

2. Выполните команду:

```
sql ALTER USER rubackup PASSWORD '<new-password>';
```

Суперпользователь создается одновременно с базой данных `rubackup` и является владельцем этой базы данных. В списке пользователей СРК пользователя Суперпользователь увидеть нельзя. Нельзя создать нового пользователя с тем же именем.

Суперпользователь может:

- добавлять новых пользователей в систему. Выбранная группа создаваемого пользователя влияет только на задачи уведомления. Чтобы пользователь мог получить административные привилегии в СРК, его нужно добавить в супервайзеры, сопровождающие или администраторы;
- менять пароль для других пользователей с помощью RBM.

7.2. Супервайзер

Супервайзер может выполнять действия, доступные Суперпользователю, за исключением:

- любых действий с пользователями кроме назначения ролей Сопровождающего и Администратора;
- изменения глобальной конфигурации СРК.

7.3. Сопровождающий

Сопровождающий отвечает за медиасервер и может управлять устройствами хранения на этом медиасервере.

7.4. Администратор

Администратор отвечает за группу клиентов и может выполнять их настройки и действия, связанные с клиентами, входящими в группу.

Администратор в дереве объектов видит только «своих» клиентов, и имеет доступ к правилам глобального расписания, резервным копиям и задачам только «своих» клиентов.

7.5. Аудитор

Аудитор — роль, предназначенная для сотрудников информационной безопасности. Аудитору доступен просмотр всех настроек и информации в СРК (кроме настроек глобальной конфигурации) без возможности редактирования. Аудитору также доступны для просмотра все журналы, включая «Журнал событий ИБ».

Порядок назначения типов пользователя, их поиска и удаления можно найти в [Пользователи](#).

Глава 8. Хранилища секретов

Аутентификационная информация (секрет) для подключения к резервируемым ресурсам чаще всего хранится в файлах настроек модулей. Если файлы настроек недостаточно защищены или система, в которой они располагаются, скомпрометирована, третьи лица могут получить доступ к резервируемым ресурсам.

Безопаснее использовать стороннее решение по управлению секретами (хранилище секретов).

Если модуль настроен на использование хранилища секретов, то сервер RuBackup по запросу клиента (модуля) обращается к хранилищу секретов, получает данные и передает их клиенту.

Секрет на сервере RuBackup «привязан» к клиенту.

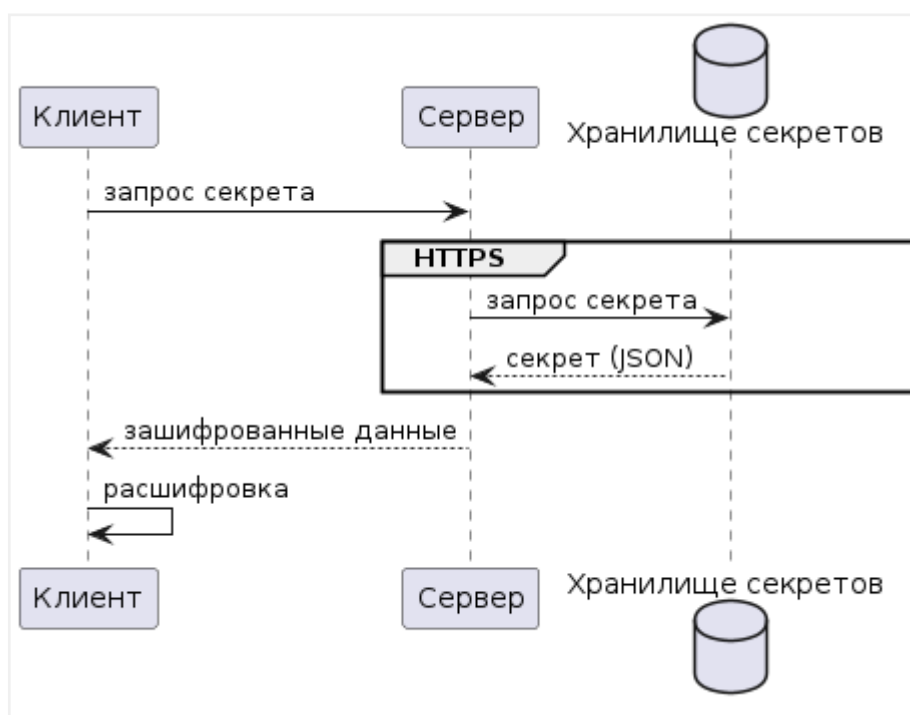


Рисунок 4. Взаимодействие клиента, сервера и хранилища секретов

Хранилищем секретов управляет заказчик — выпускает сертификаты, токены доступа и другие артефакты. Рекомендуем подключение к хранилищу секретов по HTTPS.

RuBackup совместим с хранилищами секретов:

- HashiCorp Vault,
- Deckhouse Stronghold.



Управление доступом к аутентификационной информации в хранилище секретов возможно с помощью консольной утилиты `rb_secret_storage`.

Информацию о поддержке модулем хранилища секретов см. в документации модуля.

8.1. Подготовка к использованию

Убедитесь, что модуль поддерживает использование хранилища секретов.

Получите от администратора хранилища секретов:

- подтверждение, что секрет в хранилище секретов создан;
 - токен для доступа к хранилищу секретов;
 - метод (эндпоинт) доступа к секрету.
1. Проверьте, что сервер хранилища секретов доступен: IP-адрес внесен в `/etc/hosts` или в локальный DNS организации.
 2. Проверьте номер и доступность порта, по которому выполняется защищенное HTTPS-подключение к хранилищу секретов.
 3. Получите цепочку HTTPS-сертификатов хранилища секретов в формате PEM.

```
openssl s_client \  
-connect host \ ① ②  
-showcerts \ ③  
-servername hostname \ ④  
> ~/secretstorage.pem ⑤
```

- ① Флаг `-connect` показывает диагностическую информацию об SSL-подключении к серверу.
- ② `host` — имя и опционально порт сервера хранилища секретов.
- ③ Флаг `-showcerts`, добавленный к `-connect`, показывает всю цепочку сертификатов сервера в формате PEM.
- ④ Включение SNI.
- ⑤ Экспорт полученной цепочки сертификатов в файл.

Сохраните файл `~/secretstorage.pem`, он потребуется при добавлении хранилища секретов.

4. Проверьте подключение к хранилищу секретов.

Проверить подключение к хранилищу секретов можно с помощью `curl`, передав HTTPS-сертификат, токен доступа в заголовке `X-Vault-Token` или `Authorization: Bearer`.

Эндпоинты KV v1 (неверсионизируемые) и KV v2 (версионизируемые) могут отли-

ваться. Как правило, если эндпоинту KV v2 не передан номер версии секрета, возвращается самый новый (latest).

Пример 3. Запрос неversionируемого секрета (KV v1)

```
curl
  --cacert ~/secretstorage.pem \ ❶
  --header 'X-Vault-Token: TOKEN' \ ❷
  'https://example.ru/v1/kv/postgres' ❸
```

- ❶ HTTPS-сертификат подключения.
- ❷ Токен доступа `TOKEN` в заголовке `X-Vault-Token`.
- ❸ Запрос к эндпоинту KV v1.

Пример 4. Запрос versionируемого секрета (KV v2)



```
curl
  --cacert ~/secretstorage.pem \ ❶
  --header 'Authorization: Bearer TOKEN' \ ❷
  'https://example.ru/v1/kv_rubackup/data/postgres' ❸
```


- ❶ HTTPS-сертификат подключения.
- ❷ Токен доступа `TOKEN` в заголовке `Authorization`.
- ❸ Запрос к эндпоинту KV v2. Обратите внимание на `/data/`.

5. В конфигурационном файле модуля установите флаг, включающий использование хранилища секретов.
6. В конфигурационном файле модуля удалите аутентификационные данные подключения к резервируемому ресурсу.

8.2. Добавление хранилища секретов

Добавление сервера хранилища секретов доступно только Суперпользователю СРК.




1. Перейдите  **Безопасность** → **Хранилище секретов** → **Список хранилищ секретов**. Нажмите  **Добавить**.
2. Укажите **Имя хранилища секретов** — оно будет показано в других диалоговых окнах.
3. Выберите **Тип хранилища секретов**.

4. (опционально) При использовании защищенного HTTPS-соединения с хранилищем секретов добавьте сертификат стандарта X.509 в текстовом формате.
5. (опционально) Добавьте описание хранилища секретов.
6. Нажмите  **Применить**.

Добавленное хранилище будет показано в списке хранилищ секретов и будет доступно при добавлении метода доступа к секрету.

8.3. Добавление метода получения секрета

Добавление метода получения секрета доступно только Суперпользователю СРК.

1. Перейдите  **Безопасность** → **Хранилище секретов** → **Список методов получения секрета**. Нажмите  **Добавить**.
2. Задайте **Имя метода получения секрета**.
3. Выберите из выпадающего списка **Имя хранилища секретов** доступное хранилище секретов, к которому будет выполняться подключение.
4. Введите **Токен** (идентификатор для получения секрета).
5. Укажите **Метод получения секрета** (адрес, порт и эндпоинт), предварительно полученный у администратора хранилища секретов.
6. (опционально) Введите описание метода получения секрета.
7. Нажмите  **Применить**.

Добавленный метод будет доступен в **Списке методов получения секрета**.

8.4. Настройка доступа пользователей к хранилищу секретов




Суперпользователь может назначить Супервайзеру или Администратору доступ к выбранному секрету посредством ассоциации пользователя с методом получения секрета.

Таблица 2. Права доступа пользователей RuBackup к секретам хранилища

Операция	Роль				
	Супер-пользователь 	Администратор	Аудитор	Сопровождающий	Супервайзер
Редактирование данных хранилища секретов	✓	✗	✗	✗	✗
Добавление данных хранилища секретов	✓	✗	✗	✗	✗
Удаление данных хранилища секретов	✓	✗	✗	✗	✗

Добавление методов получения секретов	✓	✗	✗	✗	✗
Просмотр методов получения секретов	✓	👤	✗	✗	👤
Редактирование методов получения секретов	✓	✗	✗	✗	✗
Удаление методов получения секретов	✓	✗	✗	✗	✗
Управление доступом к методам получения секретов	✓	✗	✗	✗	✗

👤 — доступ на выбранный метод назначает Суперпользователь

1. Перейдите  **Безопасность** → **Хранилище секретов** → **Доступ пользователей к методам**. Нажмите  **Добавить**.
2. Выберите из выпадающего списка **Имя хранилища секретов** хранилище секретов.
3. Выберите из выпадающего списка **Имя метода получения секрета** метод, с которым будет ассоциирован пользователь.
4. Выберите из списка пользователей (с ролью *Супервайзер* и *Администратор*), которым будет назначен доступ к методу получения секрета в выбранном хранилище секретов.
5. Нажмите  **Применить**.

Добавленный пользователь и ассоциированный с ним метод будет показан в окне **Доступ пользователей к методам**.

Глава 9. Удаленное логирование

Syslog (System Logging Protocol) — это стандартный протокол для передачи и централизованного сбора сообщений о событиях в компьютерных системах и сетях. Протокол был разработан для унификации процесса логирования в различных устройствах и операционных системах.

Основные компоненты для удаленного логирования включают:

- Syslog-сервер — центральный узел для сбора и хранения логов.
- Syslog-клиенты — устройства, отправляющие сообщения о событиях.
- Форматирование сообщений — стандартизированный формат записи логов.

9.1. Преимущества использования Syslog

Внедрение централизованного логирования через syslog предоставляет ряд существенных преимуществ:

- Централизация данных — все логи собираются в одном месте, что упрощает их анализ и мониторинг.
- Масштабируемость — система легко расширяется для работы с большим количеством устройств.
- Безопасность — возможность шифрования трафика и аутентификации источников.
- Фильтрация и сортировка — гибкие возможности для обработки логов.
- Автоматизация — интеграция с системами мониторинга и оповещения.
- Долгосрочное хранение — централизованное архивирование исторических данных.

9.2. Syslog в CPK RuBackup

RuBackup поддерживает работу с любыми серверами Syslog, поддерживающими протокол TCP и UDP.

Рекомендуется использовать следующие сервера Syslog:

- [Раздел 9.4.1.](#)
- [Раздел 9.4.2.](#)

Для настройки удаленного логирования в SIEM используйте [Раздел 9.3.](#)

9.3. Интеграция с SIEM-системами в CPK RuBackup

SIEM (Security Information and Event Management) представляет собой комплексное решение для обеспечения информационной безопасности, объединяющее управление информацией о безопасности (SIM) и управление событиями безопасности (SEM). Это централизованная система, предназначенная для сбора, анализа и обработки событий безопасности в реальном времени.

Интеграция с SIEM-системами реализована с помощью удаленного логирования Syslog.

Syslog-сервер выступает в роли промежуточного звена между CPK RuBackup и платформой безопасности MaxPatrol SIEM.

CPK RuBackup предоставляет возможность использования SIEM-системы MaxPatrol SIEM.

Для использования SIEM в CPK RuBackup выполните следующие шаги:

1. Установите и настройте один из рекомендуемых syslog-серверов:
 - [Раздел 9.4.1.](#)
 - [Раздел 9.4.2.](#)
2. Выполните настройку параметров удаленного логирования в одном из интерфейсов:
 - [Раздел 9.5.2.](#)
 - [Раздел 9.5.1.](#)
3. Выполните [Раздел 9.6.](#)

9.4. Установка и настройка

9.4.1. Установка и настройка сервера syslog-ng

Установка

1. Некоторые дистрибутивы Linux уже содержат пакет `syslog-ng`. Проверьте наличие пакета:

```
syslog-ng --version
```

2. Если сервер не установлен, установите его из репозитория:

```
apt update
```



```
apt install syslog-ng
```

3. Запустите сервер:

```
systemctl start syslog-ng.service
```

4. Проверьте статус сервера:

```
systemctl status syslog-ng.service
```

5. Добавьте сервер в автозапуск:

```
systemctl enable syslog-ng.service
```

Настройка

Для приема сообщений от RuBackup сервер `rsyslog` должен быть настроен на прослушивание сетевых сокетов по протоколам TCP и(или) UDP.

Для этого:

1. Откройте файл `/etc/syslog-ng/syslog-ng.conf`:

```
nano /etc/syslog-ng/syslog-ng.conf
```

2. Раскомментируйте и отредактируйте строку:

```
source s_net { tcp(ip(127.0.0.1) port(1000)); };
```

где:

- `tcp` — указывает, что сервер будет слушать TCP-порт;
- `ip(127.0.0.1)` — указывает, что сервер будет слушать локальный адрес (хост) ^[1];
- `port(1000)` — указывает, что сервер будет слушать порт 1000 ^[1].

3. При необходимости использования TLS добавьте еще один источник для прослушивания:

```
source s_tls {
```

```

network(
    ip(0.0.0.0) ❶
    port(6514) ❷
    transport("tls")
    tls(
        key-file("/etc/syslog-ng/cert.d/server.key")
        cert-file("/etc/syslog-ng/cert.d/server.crt")
        peer-verify(required-untrusted)
        peer-verify(optional-untrusted)
        trusted-dn("CN=rubakup")
    )
);
};

```

❶ Выполните настройку в соответствии с настройкой основного сервера RuBackup.

❷ Стандартная настройка TLS. Изменение порта недопустимо.

4. (опционально) Для вывода логов RuBackup в отдельный файл добавьте строку в конфигурационный файл:

```
destination d_rubakup { file("/var/log/rubakup.log"); };
```

5. Укажите путь к файлу сбора логов:

```
log { source(s_net); destination(d_rubakup); };
```

6. Если используется TLS, добавьте:

```
log { source(s_tls); destination(d_rubakup); };
```

7. Сохраните конфигурационный файл и проверьте синтаксическую корректность:

```
syslog-ng --syntax-only
```

Команда не должна вернуть никаких ошибок.

8. Перезапустите `syslog-ng`:

```
systemctl restart syslog-ng.service
```

Проверьте, что сервер слушает указанный сокет:

```
ss -tulpan | grep syslog
```

Пример успешной настройки syslog-ng (состояние портов)

```
tcp    LISTEN  0    255      0.0.0.0:8181  0.0.0.0:*    users:(("syslog-ng",pid=4255,fd=12))
```

9.4.2. Установка и настройка сервера rsyslog

Установка

1. Некоторые дистрибутивы Linux уже содержат пакет rsyslog. Проверьте наличие пакета:

```
rsyslogd -v
```

2. Если сервер не установлен, установите его из репозитория:

```
apt update
apt install rsyslog
```

3. Запустите сервер:

```
systemctl start rsyslog
```

4. Проверьте статус сервера:

```
systemctl status rsyslog
```

5. Добавьте сервер в автозапуск:

```
systemctl enable rsyslog
```

Настройка

Для обеспечения приема сообщений от RuBackup сервер rsyslog должен быть настроен на прослушивание сетевых сокетов по протоколам TCP и(или) UDP.

Для этого:

1. Откройте файл `/etc/rsyslog.conf`:

```
nano /etc/rsyslog.conf
```

2. Добавьте строки, в зависимости от того, какой протокол будет использоваться: TCP и(или) UDP:

```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="515")
```

3. Перезапустите `rsyslog`:

```
systemctl restart rsyslog.service
```

Проверьте, что сервер слушает указанные сокеты:

```
ss -tulpan | grep rsyslog
```



Пример успешной настройки `rsyslog` (состояние портов)

```
udp    UNCONN 0    0      0.0.0.0:515    0.0.0.0:*
users:(("rsyslogd",pid=1436,fd=5))
udp    UNCONN 0    0      [::]:515      [::]:*
users:(("rsyslogd",pid=1436,fd=6))
tcp    LISTEN 0    25     0.0.0.0:514    0.0.0.0:*
users:(("rsyslogd",pid=1436,fd=7))
tcp    LISTEN 0    25     [::]:514      [::]:*
users:(("rsyslogd",pid=1436,fd=8))
```

9.5. Настройка удаленного логирования в интерфейсе

9.5.1. Настройка логирования в RBM


Для настройки взаимодействия с SIEM системами в Менеджере администратора RuBackup:



1. Перейдите в раздел  **Безопасность** → **Журналы** → **Настройка внешних журналов** → **Серверы сбора логов**.
2. Нажмите  **Добавить** для добавления нового сервера сбора логов.
3. Заполните параметры сервера сбора логов:

▼ Параметры сервера сбора логов

Параметр	Описание
Имя хоста *	Имя хоста Syslog-сервера
Порт *	Порт Syslog-сервера
Тип соединения	TCP или UDP протокол

При необходимости можно добавить описание сервера сбора логов.


Нажмите  **Применить** для сохранения настроек.

4. Перейдите в раздел  **Безопасность** → **Журналы** → **Настройка внешних журналов** → **Цели логирования**.
5. Нажмите  **Добавить** для создания нового правила сбора [Приложение 9.A](#).
6. Заполните параметры цели логирования:

▼ Параметры цели логирования

Параметр	Описание
Сервер логирования *	Данные Syslog сервера вида: <имя_хоста>:<порт> <тип_соединения>
Протокол логирования *	На данный момент поддерживается только протокол SysLog
Формат логирования *	На данный момент поддерживается только формат CEF
Использовать TLS	Будет ли использоваться TLS протокол
Путь к сертификату TLS ^[2]	Полный путь к файлу с сертификатом
Включить логирование	Активирует логирование для этой цели

При необходимости можно добавить описание цели логирования.

Нажмите  **Применить** для сохранения настроек.

7. Включите необходимую цель логирования для формата CEF переключателем



9.5.2. Настройка логирования в Tuscana

Для настройки взаимодействия с SIEM системами в Tuscana необходимо выполнить следующие шаги:

1. Перейдите в раздел **Безопасность** → **Журналы** → **Серверы сбора логов**.
2. Нажмите **+ Добавить** для добавления нового сервера сбора логов.
3. Заполните параметры сервера сбора логов:

▼ Параметры сервера сбора логов

Параметр	Описание
Имя хоста *	Имя хоста Syslog-сервера
Порт *	Порт Syslog-сервера
Тип соединения	TCP или UDP протокол

При необходимости можно добавить описание сервера сбора логов.

Нажмите **В Применить** для сохранения настроек.

4. Перейдите в раздел **Безопасность** → **Журналы** → **Точки логирования**.
5. Нажмите **+ Добавить** для добавления правила сбора [Приложение 9.A](#).
6. Заполните параметры цели логирования:

▼ Параметры цели логирования

Параметр	Описание
Сервер логирования *	Данные Syslog сервера вида: <имя_хоста>:<порт> <тип_соединения>
Протокол *	На данный момент поддерживается только протокол SysLog
Формат *	На данный момент поддерживается только формат CEF
Использовать TLS	Будет ли использоваться TLS протокол
Путь к сертификату TLS ^[3]	Полный путь к файлу с сертификатом
Точка логирования	Активирует логирование для этой цели

При необходимости можно добавить описание цели логирования.

Нажмите **В Применить** для сохранения настроек.

7. Включите необходимую цель логирования для формата CEF переключателем **О**.

9.6. Настройка `rb_syslog_reporter`

Утилита представляет собой исполняемый файл `rb_syslog_reporter`, входит в состав пакета `rubackup-server_<версия-пакета>_amd64_signed.deb`. Утилита предназначена для сбора и анализа данных из syslog-файлов и отправки их в syslog-сервер.

Предоставьте права на выполнение:

```
chmod 111 /opt/rubackup/bin/rb_syslog_reporter
```

9.6.1. Настройка конфигурационного файла `rb_siem.conf`

1. Создайте конфигурационный файл с помощью утилиты `rb_syslog_reporter`:

```
/opt/rubackup/bin/rb_syslog_reporter -gen > /opt/rubackup/etc/rb_siem.conf
```

2. Откройте [Приложение 9.Б](#) и отредактируйте его в соответствии с вашими требованиями.
3. Ограничьте доступ к файлу `rb_siem.conf`:

```
chown root:root rb_siem.conf  
chmod 600 rb_siem.conf
```

9.6.2. Настройка планировщика событий Linux

Запуск утилиты осуществляется через планировщик `cron` согласно заданному расписанию. В планировщике необходимо указать интервалы запуска.

Для этого:

1. Откройте планировщик:


```
crontab -e
```

2. Добавьте строчку:

```
* * * * * RB_SIEM_CONFIG=/abs/path/to/rb_siem.conf  
/opt/rubackup/bin/rb_syslog_reporter >> /tmp/sync.log 2>>  
/tmp/sync_error.log
```

где:

- `/abs/path/to/rb_siem.conf` — абсолютный путь до конфигурационного файла;
- `/opt/rubackup/bin/rb_syslog_reporter` — абсолютный путь к исполняемому файлу `rb_syslog_reporter`;
- `/tmp/sync.log`, `/tmp/sync_error.log` — абсолютные пути до файлов с логами.

 Рекомендуется запускать ее каждую минуту.

3. Сохраните изменения.

Приложение А: События информационной безопасности

Таблица 3. Пользовательские сценарии, приводящие к формированию событий в журнале ИБ

Элемент системы	Сценарий
Стратегии	Добавление стратегии
	Редактирование стратегии
	Удаление стратегии
	Включение/выключение стратегии
Правила стратегии	Добавление правила стратегии
	Удаление правила стратегии
Репозиторий	Добавление резервной копии
	Удаление резервной копии
	Перемещение резервной копии
	Копирование резервной копии
	Редактирование срока хранения резервной копии
Клиенты РК	Добавление клиента вручную
	Удаление клиента
Медиасерверы	Добавление медиасервера вручную
	Удаление медиасервера
Пулы	Добавление пула
	Редактирование пула
	Удаление пула
Группы пулов	Добавление группы пулов
	Удаление группы пулов

Элемент системы	Сценарий
Подмена пулов	Добавление правила подмены пулов
	Удаление правила подмены пулов
Очередь задач	Появление новой задачи в очереди задач
	Перезапуск задачи в очереди задач
	Изменение статуса задачи в очереди задач
	Удаление задачи из очереди задач

Приложение Б: Конфигурационный файл `rb_siem.conf`

Таблица 4. Параметры `rb_siem.conf`

Параметр	Описание
<code>RB_HOST</code>	IP-адрес сервера RuBackup
<code>RB_USER</code>	Логин пользователя RuBackup
<code>RB_PASSWORD</code>	Пароль пользователя RuBackup
<code>DB_HOST</code>	IP-адрес служебной базы данных RuBackup
<code>DB_PORT</code>	Порт, на котором запущена служебная базы данных RuBackup
<code>DB_NAME</code>	Имя системной служебной базы данных
<code>RB_ROOT_CA_CERT</code>	Путь до корневого сертификата сервера RuBackup
<code>RB_CLIENT_CERT</code>	Путь до клиентского сертификата сервера RuBackup
<code>RB_CLIENT_CERT_KEY</code>	Путь до ключа клиентского сертификата сервера RuBackup

[1] Выполните настройку в соответствии с настройкой основного сервера RuBackup.

[2] Обязательное поле, если используется TLS.

[3] Обязательное поле, если используется TLS.