# Программное обеспечение «Базис.Virtual Protect». Руководство по эксплуатации

RU.НРФЛ.00001-01.97.01

Москва

16/08/2023

# Содержание

# Аннотация

Настоящий документ предназначен для технического администратора ПО и содержит инструкции по выполнению работ, необходимых для эксплуатации ПО.

Руководство содержит инструкции по выполнению задач, связанных с:

- сопровождением и обслуживанием ПО;
- диагностикой, локализацией и устранением предусмотренных неисправностей.

# Перечень эксплуатационных документов

Дополнительно к настоящему документу технические администраторы должны использовать следующие документы:

- RU.НРФЛ.00009-01.96.01«ПО «Базис.Virtual Protect». Руководство по установке;
- RU.НРФЛ.00009-01.95.01«ПО «Базис.Virtual Protect». Руководство администратора.

# Идентификационные данные документа

| **Идентификационные данные ПО** | **Программа для ЭВМ «Базис.Virtual Protect»** |
|---|---|
| Название документа | «ПО «Базис.Virtual Protect». Руководство по эксплуатации» |
| Обозначение документа | RU.НРФЛ.00009-01.97.01 |
| Автор документа | ООО «БАЗИС» |

# Требования к составу и квалификации обслуживающего персонала

Системный инженер – должностное лицо, служебная деятельность которого обеспечивает качественную и безопасную эксплуатацию оборудования ЦОД или виртуального ЦОД – облачной платформы – после внедрения (ввода в эксплуатацию).

Администратор ОП – должностное лицо, служебная деятельность которого связана с эксплуатацией программных продуктов и стороннего ПО, используемого при создании среды функционирования:

- Kubernetes - проект с открытым исходным кодом, предназначенным для управления кластером контейнеров Linux как единой системой. Kubernetes управляет и запускает контейнеры Docker на большом количестве хостов, а так же обеспечивает совместное размещение и репликацию большого количества контейнеров.
- Docker - проект с открытым исходным кодом для автоматизации развертывания приложений в виде переносимых автономных контейнеров, выполняемых в облаке или локальной среде.
- MinIO - высокопроизводительное хранилище объектов MinIO. MinIO - высокопроизводительное решение для хранения объектов, которое предоставляет API, совместимый с S3, и поддерживает все основные функции S3. В свою очередь, настройки кластеров и учетные данные пользователей хранятся в документоориентированной базе mongo. Данные о резервных копиях, запланированных резервных копиях и хранилищах хранятся в целевых кластерах. Конечным, обобщающим все данные, является объектное хранилище совместимое с API S3, что позволяет осуществлять миграцию на новые кластера.
- Объектное S3-совместимое хранилище - облачный сервис, позволяющий хранить файлы любого типа и объема, используемый для хранения неструктурированных данных. В объектном хранилище файлы представлены в виде объектов. Обычно каждый объект состоит из трех основных компонентов: содержимого объекта, метаданных объекта и его идентификатора. Уникальный идентификатор позволяет быстро находить файл в хранилище и управлять им. Метаданные позволяют управлять объектами нужного типа (выгрузка, политики хранения, удаления для определенных объектов и т. д.). Объекты хранятся в специальных контейнерах — корзинах (buckets) с уникальным ID. В S3 объекты хранятся в плоском адресном пространстве, как в файловом хранилище. Доступ к объектам возможен через API или HTTP/HTTPS.

Системный инженер должен иметь навыки проектирования или настройки аппаратных и программных конфигураций компьютерных сетей, обслуживания локальных вычислительных сетей. Кроме того, он может быть ответственен за организацию защиты информации и производить установку антивирусов и другого программного обеспечения, обновление ПО. Полезным будет также навык анализа затрат на системное обслуживание, составление отчетов и поиск способов оптимизации расходов.

Оперативный персонал (системный инженер), осуществляющий манипуляции с оборудованием на площадке, должен иметь допуск к эксплуатации электроустановок до 1000В. Категория допуска должна быть согласована со службами эксплуатации ЦОД.

Обычными задачами системного администратора, в зависимости от инфраструктуры, являются контроль работы компьютерных программ и устранение ошибок в их работе, разовая диагностика/ремонт ПК и другой офисной техники.

Системный администратор должен уметь использовать множество утилит и инструментов администрирования системой с целью:

- контроля работоспособности системы (проверки основного функционала);
- проверки работоспособности отдельных системных служб;
- конфигурирования виртуальных сервисов системы;
- резервного копирования и восстановления виртуальных машин.

Для выполнения задач по сопровождению ПО «Базис.Virtual Protect», необходимо иметь опыт работы, связанный с системным администрированием серверного оборудования, а также понимать основные принципы резервного копирования и восстановления данных.

Деятельность системного инженера регулируется и контролируется отделом информационной безопасности, а также внутренними регламентами предприятия, нацеленными на обеспечение безопасности данных и соблюдение конфиденциальности.

# Описание и работа ПО

## Назначение ПО

ПО «Базис.Virtual Protect» (далее Базис.Virtual Protect, ПО, система) предназначено для управления резервным копированием кластеров kubernetes, а также восстановлением из резервных копий.

Резервному копированию и восстановлению из резервных копий доступны:

- системные компоненты Kubernetes (конфигурация самого кластера);
- рабочие нагрузки (оркестрируемые контейнеры);
- персистентные данные рабочих нагрузок.

Для хранения резервных копий используется любое S3-совместимое хранилище, что снижает риск потери данных за счет использования независимого совместимого с API S3 хранилища данных.

## Структура ПО

ПО «Базис.Virtual Protect» включает следующие программные компоненты:

- backend (написан на Golang);
- decort-go-sdk - компонент, представляющий библиотеку, написанную на языке GO, позволяющую взаимодействовать с API облачной платформы DECORT. Библиотека содержит в себе структуры и методы, необходимые для отправки запросов. Decort SDK имеет встроенный http-клиент и поддерживает разные способы авторизации на платформе. Библиотека так же содержит в себе модели ответов от платформы;
- frontend - компонент, представляющий собой фреймворк с открытым исходным кодом для создания пользовательских интерфейсов, интегрирующийся в проекты с использованием других JavaScript-библиотек.

На рисунке 1 отображена схема взаимодействия ПО «Базис.Virtual Protect» с внешними приложениями:

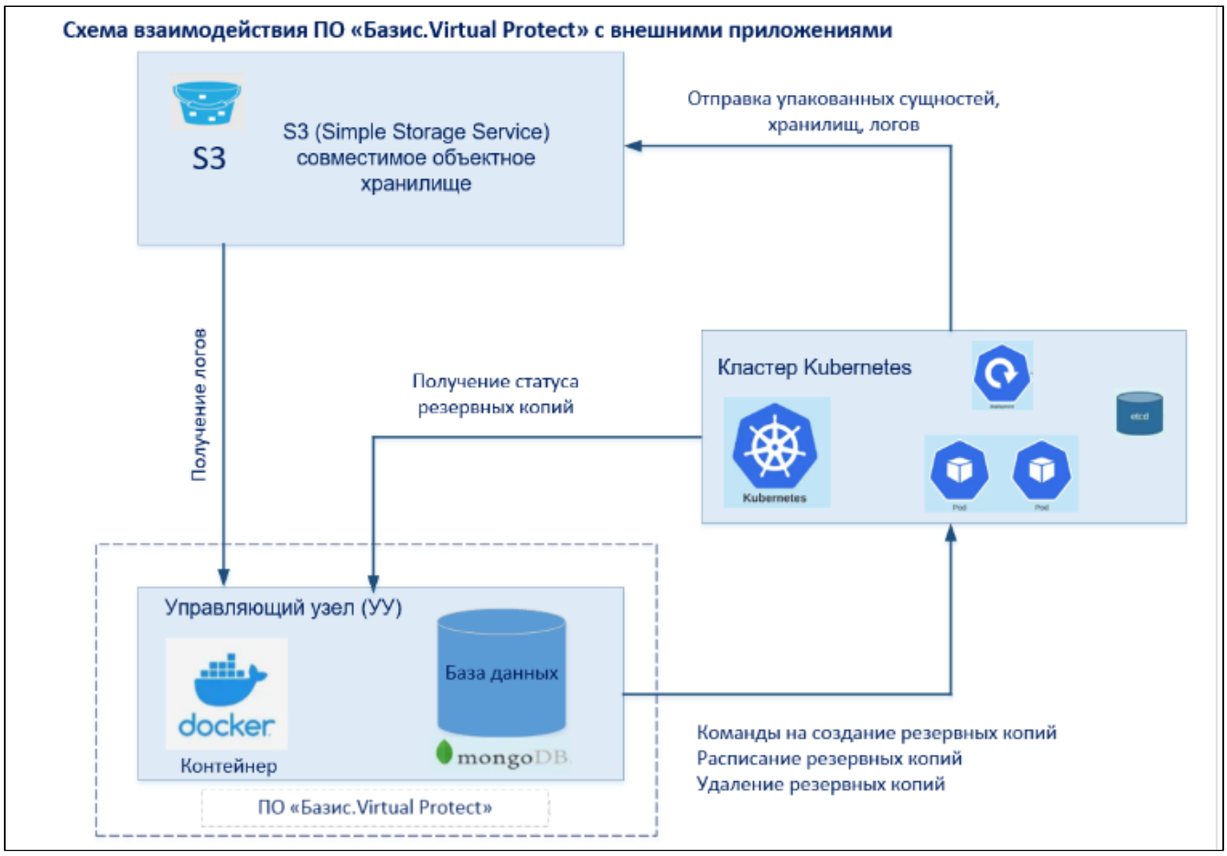


*Рисунок 1 - Схема взаимодействия ПО «Базис.Virtual Protect» с внешними приложениями*

## Функциональные возможности

Помимо прямых функций по резервному копированию и восстановлению, ПО «Базис.Virtual Protect» предоставляет пользователю следующие функциональные возможности:

- полнофункциональный графический интерфейс;

- встроенная возможность создавать S3-совместимое хранилище minIO на платформе DECORT с возможностью добавления к одному кластеру несколько независимых хранилищ;
- хранение данных в резервных копиях в сжатом виде, в определенных бакетах данного хранилища;
- автоматическое обслуживание копий архива (удаление копий, срок хранения которых истек);
- создание резервных копий нагрузок выбранных пространств имен (namespaces) и нагрузок определенных групп (groups) в кластерах K8s;
- выборочное восстановление из резервных копий нагрузок из определенных пространств имен и принадлежащим определенной группе API;
- поддержка мультикластерности, в рамках одного интерфейса, что позволяет добавлять в систему на обслуживание кластера k8s, а также удалять эти кластера из обслуживания;
- возможность интеграции с другими продуктами ООО "БАЗИС".

# Условия применения

ПО "Базис.Virtual Protect" эксплуатируется в вычислительной среде центра обработки данных (дата-центра), который может быть как централизованным, так и территориально-распределенным.

Основные компоненты составляющие типовой информационно-вычислительный центр (далее – дата-центр или ЦОД):

1. Приложение: компьютерная программа, задающая логику вычислительных операций.
2. Система управления базами данных (СУБД): ПО, обеспечивающее структурированный способ хранения банков (баз) данных.
3. Хост-система (главный компьютер): вычислительная платформа, состоящая из оборудования, программно-аппаратных средств и программного обеспечения, обеспечивающая работу управляющих приложений и СУБД.
4. Сеть: физические каналы обмена данными, обеспечение связи между различными устройствами, подключенными к сети.
5. Хранилище: устройство накопления и постоянного (длительного) хранения данных.

Приложения, наделенные бизнес-логикой, функционируют, как правило, в границах IaaS – изолированной от прямого вмешательства среде.

СУБД используются как для поддержания целостности модели инфраструктуры, так и для накопления и/или выборки данных. В зависимости от архитектуры применения приложений, использующих определенные СУБД, выбираются узлы, обеспечивающие наиболее благоприятные условия эксплуатации. Могут быть выбраны как серверные компьютеры, так и виртуальные машины, работающие под управлением ОС, обеспечивающей максимальную совместимость с оборудованием – подсистемами передачи и хранения информации, а также наиболее подходящие для выбора в качестве среды функционирования СУБД.

Качество электропитания, подводимого к хост-системе, сетевому оборудованию и системам хранения данных, равно как и прочим средствам ВТ, включенным в состав облачной инфраструктуры, должно соответствовать действующим нормам.

Обслуживающий персонал должен обладать общими знаниями электробезопасности, пройти необходимый инструктаж ОТ и ТБ, получить допуски к работе на электроприёмниках, в соответствии с Правилами Безопасной Эксплуатации Электроустановок и с учетом доступа в технические помещения.

Кроме того, оперативный персонал, эксплуатирующий оборудование ЦОД в той или иной степени, обязан соблюдать меры пожарной безопасности.

# Инструменты администратора

Деятельность администратора ПО не ограничена использованием одного компьютера (АРМ). В зависимости от характера возникающих задач администратор может использовать различные виды СВТ: от персонального компьютера (ноутбука) с установленной операционной системой Linux до тонкого клиента, с помощью которого пользователь VDI осуществляет подключение к VDI машине.

На СВТ, используемом администратором, должен быть установлен веб-браузер, поддерживаемый операционной системой (Windows, Ubuntu, CentOS и др.). Кроме того, должно быть установлено ПО, позволяющее осуществлять безопасное подключение к управляющим/вычислительным узлам инфраструктуры, а также к вспомогательным виртуальным машинам, если таковые интегрированы в облачную платформу для определенных (сервисно-профилактических) нужд.

Веб-браузер позволяет использовать веб-интерфейс ПО.

Рекомендуемые к использованию веб-браузеры: не рекомендуется применение браузера **Internet Explorer.**

# Удаленный доступ к информации

Удаленный доступ к информации должен обеспечивать безопасные технологии приёма и передачи данных. Например, если настраивается удаленный доступ к облаку, следует использовать SSH или организовывать дополнительные сетевые каналы, использующие VPN.

Необходимо соблюдать меры предосторожности и правила информационной безопасности, установленные в рамках отдела и/или организации. Администратор должен быть бдительным при выполнении авторизации с чужого рабочего места (ТК), так как некоторые веб-браузеры сохраняют вводимые пароли через куки или другими способами.

После того как администратор закончил работу в веб-браузере любого из СВТ, не закрепленного лично за ним, он обязан принять меры по устранению любых сохраненных учетных данных, связанных с доступом к средствам управления или отдельным компонентам облака (имена учетных записей, пароли к

ним и т.п.). Записные или электронные книги, равно как и данный документ, не должны находиться без присмотра в помещениях общего пользования.

> **Внимание**
>
> Не допускается случайная или основанная на личном доверии передача третьим лицам учетных данных, смарт-карт, электронных ключей и т.п. средств, позволяющих получить полный или частичный доступ к информации об инфраструктуре.

В конце рабочей смены все персональные компьютеры и СВТ, закрепленные за администратором, должны быть переданы по смене, с соответствующей отметкой в журнале технической эксплуатации, или заблокированы и заперты в специальном помещении, в зависимости от принятых на предприятии организационных мероприятий и политик безопасности.

Если используются АМДЗ, то электронные ключи должны храниться в сейфе или сдаваться под охрану, в с соответствии с действующими на предприятии должностными инструкциями по информационной безопасности.

## Техническое обслуживание, ремонт

Техническое обслуживание и ремонт средств вычислительной техники, коммутационного оборудования и систем хранения данных, а также источников бесперебойного питания осуществляются на основе паспортов и руководств по (сервисному) обслуживанию, соответствующих моделям и предоставленных предприятиями-изготовителями.

Персонал, осуществляющий техобслуживание/ремонт, должен пройти инструктаж по технике безопасности и обязан слаженно взаимодействовать с администратором, ответственным за эксплуатацию облачной инфраструктуры.

Администратор обязан вести журнал эксплуатации облачной инфраструктуры, оформлять все существенные события, начиная с момента завершения ПНР и приема-сдачи платформы в эксплуатацию.

Планово-профилактические работы должны быть тщательно спланированы вместе с оценкой рисков для эксплуатации. Рекомендуется имитация и отработка вероятных ситуаций на стенде, отдельно от продакшен, чтобы аварийные ситуации, не влияли на качество услуг.

# Проверка работоспособности ПО

После завершения развертывания ПО «Базис.Virtual Protect» произвести создание тестовой резервной копии и дальнейшее восстановление системы из резервной копии.

Успешность тестовой операции свидетельствует о работоспособности ПО.

Для того, чтобы в случае возникновения неопределенных обстоятельств в работе ПО было возможно эффективно взаимодействовать с Технической Поддержкой, предусмотрено логирование работы ПО.

# Общие указания

Для реализации функций безопасности среды функционирования ПО «Базис.Virtual Protect» должны выполняться следующие действия:

- необходимо регулярное обновление всех сред функционирования ПО «Базис.Virtual Protect» до актуальных версий с применением всех необходимых патчей безопасности с официальных сайтов разработчиков сред функционирования;
- компоненты операционной системы и сред функционирования ПО «Базис.Virtual Protect» должны быть максимально ограничены. Компоненты, которые не участвуют в функционировании ПО «Базис.Virtual Protect», должны быть отключены;
- должно обеспечиваться предотвращение несанкционированного доступа к идентификаторам и паролям администраторов среды виртуализации, которые необходимы для управления и технической поддержки среды функционирования ПО «Базис.Virtual Protect»;
- необходимо использовать на серверах, где развернута среда функционирования ПО «Базис.Virtual Protect», в качестве средств защиты информации от несанкционированного доступа, сертифицированных ФСТЭК России версий операционных систем с установленными обновлениями или наложенных средств защиты информации, прошедших сертификацию по требованиям безопасности информации в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00;
- должна быть обеспечена физическая сохранность серверной платформы с установленным ПО «Базис.Virtual Protect» и исключение возможности физического доступа к ней посторонних лиц.

# Действия по безопасной установке и настройке

Подробное описание установки ПО приведено в документе «ПО «Базис.Virtual Protect». Руководство по установке» RU.НРФЛ.00009-01.96.01.

# Обновление ПО

Варианты обновления:

1. в конфигурации docker-compose заменяются тэги образа (на новый);
2. Helm чарт устанавливается из обновленного репозитория.

Пример конфигурации (тега), указывающей на местоположение образа:

```
image:
  repository: ...
  pullPolicy: IfNotPresent
  # Overrides the image tag whose default is the chart appVersion.
  tag: "0.4.1"
```

Когда выпускается новая версия чарта или когда необходимо изменить конфигурацию релиза, можно использовать команду **helm upgrade**. Для обновления Dashboard, установленного с помощью **Helm**, выполните команду:

```
helm upgrade -n dashboard virtualprotec ./helm
```

# Аварийные ситуации

## Действия в случаях обнаружения несанкционированного вмешательства в данные

Несанкционированное вмешательство обнаруживается при помощи протокола нарушений безопасности.

В случаях обнаружения несанкционированного вмешательства в данные, необходимо установить логин пользователя, под которым была произведена аутентификация, затем сменить пароль для этого пользователя и проинформировать пользователя о смене пароля.

## Действия в других ситуациях

В других аварийных ситуациях необходимо обратиться в сервисную службу:

Электронный адрес: **support@basistech.ru**

# Описание функционирования

Описание совместного функционирования технических средств и ПО, описание организации входных и выходных данных, используемых при обслуживании технических средств и описание взаимодействий устройств с ПО приведено в эксплуатационных документах:

- RU.НРФЛ.00009-01.96.01«ПО «Базис.Virtual Protect». Руководство по установке;
- RU.НРФЛ.00009-01.95.01«ПО «Базис.Virtual Protect». Руководство администратора.

# Термины и определения

| Термин | Определение |
|---|---|
| CRON | Компьютерная программа в системах класса UNIX, использующаяся для периодического выполнения заданий в определённое время (автоматический запуск программ и скриптов на сервере в определённое время) |
| Docker | Проект с открытым исходным кодом для автоматизации развертывания приложений в виде переносимых автономных контейнеров, выполняемых в облаке или локальной среде |
| Golang | Компилируемый многопоточный язык программирования |
| Helm | Диспетчер пакетов, который упрощает настройку и развертывание приложений в кластерах Kubernetes (для разработчиков и операторов) |
| Kubernetes | Проект с открытым исходным кодом, предназначенным для управления кластером контейнеров Linux как единой системой. Kubernetes управляет и запускает контейнеры Docker на большом количестве хостов, а так же обеспечивает совместное размещение и репликацию большого количества контейнеров |
| MinIO | Высокопроизводительное хранилище объектов MinIO. MinIO - высокопроизводительное решение для хранения объектов, которое предоставляет API, совместимый с S3, и поддерживает все основные функции S3 |
| Чарт | Пакет для Helm, который содержит все определения ресурсов, необходимые для запуска приложения, инструмента или службы внутри кластера Kubernetes |

# Перечень сокращений

В документе использованы следующие сокращения:

| Сокращение | Определение |
|---|---|
| LDAP | (англ. Lightweight Directory Access Protocol) - протокол прикладного уровня для доступа к службе каталогов |
| USB | (англ. Universal Serial Bus) — «универсальная последовательная шина», последовательный интерфейс для подключения периферийных устройств к вычислительной технике |
| АМДЗ | Аппаратный модуль доверенной загрузки |
| ОТ | Охрана труда |
| ПО | Программное обеспечение |
| Пул | Логический объект СХД, объединяющий пространства нескольких физических накопителей в единое пространство хранения данных |
| СВТ | Средства вычислительной техники |
| СХД | Система хранения данных |
| ТБ | Техника безопасности |
| ЦОД | Центр обработки данных |