



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

**Специальное программное обеспечение
средств защиты информации
от несанкционированного доступа
«Аккорд-KVM»**

**Руководство (оператора)
пользователя**

37222406.501410.073 34

Листов 8

Москва
2025

АННОТАЦИЯ

Настоящий документ является руководством пользователя специального программного обеспечения «Аккорд-KVM» (далее по тексту - СПО «Аккорд-KVM»), предназначенного для защиты инфраструктур виртуализации, построенных на базе KVM.

В документе приведено описание особенностей работы пользователей инфраструктуры виртуализации, защищаемой с помощью СПО «Аккорд-KVM».

Перед началом эксплуатации СПО «Аккорд-KVM» рекомендуется внимательно ознакомиться с комплектом эксплуатационной документации, а также нормативными и методическими документами, регулирующими обеспечение безопасности информации (БИ), включая политику БИ предприятия или организации, эксплуатирующей СПО «Аккорд-KVM».

СОДЕРЖАНИЕ

1 Общие сведения	5
1.1 Назначение СПО «Аккорд-KVM»	5
1.2 Состав СПО «Аккорд-KVM»	5
1.3 Условия применения СПО «Аккорд-KVM»	5
1.3.1 Технические условия применения	5
1.3.2 Условия организационного и технологического характера	6
2 Работа пользователя	7
2.1 Режимы работы СПО «Аккорд-KVM»	7
2.2 Функции пользователей СПО «Аккорд-KVM»	7
3 Техническая поддержка	8

ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Администратор БИ – должностное лицо, имеющее особый статус и абсолютные полномочия (супервизор). Администратор БИ организует установку СПО «Аккорд-KVM» в ПЭВМ, настройку защитных механизмов СПО «Аккорд-KVM» в соответствии с правами доступа пользователей, осуществляет контроль за правильным использованием ПЭВМ с установленным СПО «Аккорд-KVM» и периодическое тестирование средств защиты.

Администратор инфраструктуры виртуализации (ИВ) – должностное лицо, отвечающее за настройку и обслуживание ВИ.

Виртуальная машина (ВМ) – полностью изолированный программный контейнер, который работает с собственной операционной системой (ОС) и приложениями подобно физическому компьютеру. Виртуальная машина работает полностью аналогично физическому компьютеру и обладает собственными центральным процессором, памятью, жестким диском и сетевым адаптером.

1 Общие сведения

1.1 Назначение СПО «Аккорд-KVM»

СПО «Аккорд-KVM» предназначено для защиты виртуальных инфраструктур, построенных на базе KVM и использующих библиотеку libvirt в качестве инструмента управления гипервизором.

СПО «Аккорд-KVM» позволяет контролировать целостность компонентов ВМ (файлов общего, прикладного ПО и данных), выполняемых до их запуска.

1.2 Состав СПО «Аккорд-KVM»

Специальное программное обеспечение «Аккорд-KVM», устанавливаемое в ОС каждого сервера виртуализации (далее – сервер), включает в себя:

- программный модуль `assordkvm`, отвечающий за контроль целостности виртуальных машин и их компонентов;
- программный модуль `qemu`, отвечающий за перехват старта виртуальной машин.

Пакет «Аккорд-KVM» контролирует включение ВМ и обеспечивает выполнение контрольных процедур до ее запуска.

1.3 Условия применения СПО «Аккорд-KVM»

1.3.1 Технические условия применения

Для установки СПО «Аккорд-KVM» требуется следующий минимальный состав аппаратных и программных средств:

- наличие инфраструктуры виртуализации под управлением операционных систем Debian 10, Debian 11, программного продукта среды виртуализации «РЕД Виртуализация» (RU.29926343.62.01.29-PBT-01) или платформы виртуализации HOSTVM (ХОСТ) версии 4, построенной на базе технологии KVM с использованием libvirt версии не ниже 1.2.8;
- тип подключаемых дисков ВМ – RAW и `qcow2`;
- тип сетевого соединения, установленного для ВМ – прямое подключение (`direct`), внутренняя сеть (`network`), или сетевой мост (`bridge`);
- наличие дополнительных библиотек, установленных в ОС сервера;
- соответствие каждой ВМ только одной гостевой ОС;
- объем свободного дискового пространства для размещения ПО на жестком диске – не менее 100 Мбайт (на сервере).

Также следует обратить внимание, что в СПО «Аккорд-KVM» не поддерживается контроль целостности файлов с зависимыми (thin/dependent) дисками.

Для эффективного применения средств защиты СПО «Аккорд-KVM» и поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов необходимо использование СПО СЗИ НСД «Аккорд-Х К» ТУ 509000-047-11443195-2011 или (в том случае, если для инфраструктуры виртуализации требуется применение меры «Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией» согласно руководящим документам ФСТЭК России) ПАК СЗИ НСД «Аккорд-Х» ТУ 4012-026-11443195-2008 на каждом сервере виртуализации.

1.3.2 Условия организационного и технологического характера

Для эффективного применения средств защиты и поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов необходимо:

- наличие администратора БИ. Обязанности администратора БИ по применению СПО «Аккорд-KVM» изложены в «Руководстве администратора безопасности информации» (37222406.501410.073 90);
- физическая охрана ПЭВМ и ее средств с помощью технических средств, специального персонала, или других организационно-технических мер;
- учет носителей информации и идентификаторов пользователей;
- периодическое тестирование средств защиты;
- использование в ПЭВМ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ.

2 Работа пользователя

2.1 Режимы работы СПО «Аккорд-KVM»

СПО «Аккорд-KVM» поддерживает два режима работы: обычный и «мягкий».

В обычном режиме работы запрещено включение/миграция ненастроенных ВМ, то есть машин, не поставленных на контроль. Также в обычном режиме блокируется включение/миграция ВМ, целостность которых нарушена.

При работе в «мягком» режиме СПО «Аккорд-KVM» разрешает включение/миграцию как ненастроенных ВМ, так и ВМ с нарушениями целостности.

2.2 Функции пользователей СПО «Аккорд-KVM»

Работа с СПО «Аккорд-KVM» предполагает две функциональные роли пользователей:

- администратор, выполняющий установку и настройку «Аккорд-KVM»;
- оператор, работающий в защищенной инфраструктуре виртуализации.

Функции администратора подробно описаны в документе «СПО «Аккорд-KVM» Руководство администратора 37222406.501410.073 90».

Пользователи, работающие на клиентских рабочих местах (операторы), для доступа в структуру виртуализации проходят процедуру идентификации и аутентификации, предъявляя персональный идентификатор, и далее выполняют свои функциональные обязанности в обычном режиме - каких-либо ограничений на работу пользователей с ВМ, которая находится в защищаемой инфраструктуре виртуализации, СПО «Аккорд-KVM» не накладывает.

При появлении во время работы операторов сообщений об ошибках или при любых сбоях в системе следует уведомить об этом администратора безопасности.

3 Техническая поддержка

В случае необходимости консультации АО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 17-00 (по московскому времени) обращаться по телефонам:

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 762-17-72

или по адресу электронной почты support@accord.ru.

Наш адрес в Интернете <http://www.okbsapr.ru>.