



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН

37222406.501410.073 31 - ЛУ

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

**Описание применения
37222406.501410.073 31**

Листов 16

Москва
2025

АННОТАЦИЯ

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

В документе приведено описание общих принципов и правил организации работы с СПО «Аккорд-KVM», защитных функций СПО, а также особенностей установки и применения.

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

СОДЕРЖАНИЕ

1 Назначение СПО «Аккорд-KVM»	5
2 Характеристики СПО «Аккорд-KVM»	6
3 Состав СПО «Аккорд-KVM»	7
4 Условия применения СПО «Аккорд-KVM»	8
4.1 Требования к аппаратным и программным средствам	8
4.2 Условия организационного и технологического характера	8
5 Описание задачи	10
5.1 Функции безопасности, реализованные в СПО «Аккорд-KVM»	10
5.2 Установка, настройка и использование СПО «Аккорд-KVM»	11
6 Входные и выходные данные	12
7 Комплект поставки СПО «Аккорд-KVM»	13
8 Управление защитой информации	14
9 Правовые аспекты применения СПО «Аккорд-KVM»	15
10 Техническая поддержка	16

ПРИНЯТЫЕ ТЕРМИНЫ

Администратор безопасности информации (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», 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 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.

2 Характеристики СПО «Аккорд-KVM»

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

СПО «Аккорд-KVM» предназначено для выполнения основных функций защиты на основе:

- контроля целостности программных компонентов виртуальной машины (далее по тексту - ВМ) (файлов общего, прикладного ПО и данных), выполняемого до их запуска;
- контроля целостности конфигурации ВМ, выполняемого до запуска ВМ;
- управления размещением и перемещением исполняемых ВМ между серверами виртуализации;
- регистрации событий безопасности в инфраструктуре виртуализации.

3 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 виртуальных машин.

Пакет «Аккорд-KVM» контролирует включение ВМ и обеспечивает выполнение контрольных процедур до ее запуска. СПО «Аккорд-KVM» поставляется в виде `rpm`-файла.

4 Условия применения СПО «Аккорд-KVM»

4.1 Требования к аппаратным и программным средствам

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

- наличие инфраструктуры виртуализации под управлением операционных систем ОС 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 VM – RAW и qcow2;
- тип сетевого соединения, установленного для VM – прямое подключение (direct), внутренняя сеть (network), или сетевой мост (bridge);
- наличие дополнительных библиотек, установленных в ОС сервера;
- соответствие каждой VM 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.

4.2 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.

5 Описание задачи

5.1 Функции безопасности, реализованные в СПО «Аккорд-KVM»

В СПО «Аккорд-KVM» реализованы следующие механизмы безопасности:

- механизм регистрации событий безопасности в инфраструктуре виртуализации;
- механизм управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- механизм контроля целостности инфраструктуры виртуализации и ее конфигураций.

1. Механизм регистрации событий безопасности в инфраструктуре виртуализации.

СПО «Аккорд-KVM» в процессе работы производит регистрацию следующих событий безопасности:

- о запуске и остановке СПО «Аккорд-KVM», а также сообщения о получении информации о режиме работы СПО «Аккорд-KVM»;
- о создании базы данных;
- о настройке режима работы СПО «Аккорд-KVM»;
- об добавлении/удалении ВМ и её компонентов на контроль;
- о проведении проверок целостности ВМ или её компонентов, в том числе о нарушениях целостности;
- о включении ВМ;
- о выключении ВМ;
- об ошибках в СПО «Аккорд-KVM».

2. Механизм управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

Оператором обеспечивается управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных обеспечиваются:

- управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных) в части контроля целостности конфигурации виртуальных машин;
- управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации в части обеспечения возможности разрешения или запрета запуска виртуальной машины на заданном хосте;
- управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных) в части контроля целостности конфигурации виртуальных машин.

Управление перемещением виртуальных машин (контейнеров) с помощью обеспечения возможности разрешения или запрета запуска виртуальной машины на заданном хосте предусматривает:

- полный запрет перемещения виртуальных машин (контейнеров);
- ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
- ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

3. Механизм контроля целостности инфраструктуры виртуализации и ее конфигураций.

СПО «Аккорд-KVM» обеспечивает контроль целостности файлов, содержащих параметры настройки виртуальных машин, а также системных и пользовательских файлов внутри ВМ.

5.2 Установка, настройка и использование СПО «Аккорд-KVM»

Установка СПО «Аккорд-KVM» осуществляется, как правило, специалистами **ЗАКАЗЧИКА (ПОТРЕБИТЕЛЯ)** в соответствии с требованиями эксплуатационной документации.

Установка СПО «Аккорд-KVM» описана в документе «Руководство по установке» (37222406.501410.073 98). Настройка и использование СПО «Аккорд-KVM» описаны в документе «Руководство администратора» (37222406.501410.073 90).

6 Входные и выходные данные

Входными данными программы являются:

- данные и управляющие воздействия, поступающие от устройств ввода (клавиатуры);
- содержимое базы данных */etc/accordkvm/database.sb*;
- данные о ВМ (их состоянии, конфигурации, дисках и т.д.), получаемые от библиотеки *libvirt*;
- содержимое файлов хостовой системы (файл лицензии */etc/accordkvm/license-kvm.lic*, конфигурационный файл */etc/accordkvm/accordkvmlog.config* и другие файлы, указываемые пользователем при вызове программы).

Выходными данными программы является содержимое базы данных */etc/accordkvm/database.sb* и каталога */var/log/accordkvm*.

7 Комплект поставки СПО «Аккорд-KVM»

СПО «Аккорд-KVM» поставляется в комплектности, соответствующей техническим условиям (ТУ 501410-073-37222406-2018):

- 1) программный пакет «Аккорд-KVM»;
- 2) лицензия на СПО «Аккорд-KVM»;
- 3) эксплуатационная документация на СПО «Аккорд-KVM»;
- 4) формуляр – 1 брошюра;
- 5) комплект упаковки.

8 Управление защитой информации

Создаваемая структура защиты информации с применением СПО «Аккорд-KVM» должна поддерживаться механизмом установления полномочий пользователям ПЭВМ и управлением их доступом к информации.

Для этого на предприятии (учреждении, фирме и т.д.) создается служба БИ или назначается ответственное лицо (администратор БИ), на которых возлагается разработка и ввод в действие организационно-правовых документов по применению ПЭВМ с внедренными СЗИ. Этими документами предусматривается ведение ряда учетных и объектовых документов (например, «Журнал учета выданных идентификаторов», «Инструкции по применению ПЭВМ» с установленными комплексами СЗИ «Аккорд» для различных категорий должностных лиц и др.). В разработке необходимой документации со стороны ОКБ САПР может быть оказана необходимая поддержка.

9 Правовые аспекты применения СПО «Аккорд-KVM»

СПО «Аккорд-KVM» и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора.

Любое использование данного продукта в нарушение закона об авторских правах или в нарушение положений эксплуатационной документации на СПО «Аккорд-KVM» будет преследоваться в установленном порядке.

Авторские права на СПО «Аккорд-KVM» принадлежат ОКБ САПР.

Разрешается делать архивные копии СПО для использования Потребителем, который приобрел комплекс в установленном порядке.

Ни при каких обстоятельствах поставляемое СПО не распространяется между другими предприятиями (фирмами) и лицами.

Удалять в продукции ОКБ САПР уведомление об авторских правах не допускается ни при каких обстоятельствах.

При необходимости применения СПО «Аккорд-KVM» для других целей решение этого вопроса возможно только при наличии письменного согласия разработчиков.

Предыдущие ограничения не запрещают легальным пользователям распространять собственные исходные коды или модули, связанные с применением СПО «Аккорд-KVM». Однако тот, кто получает такие исходные коды или модули, должен приобрести собственную копию нашего СПО, чтобы на законном основании использовать его и иметь сертификат соответствия.

При обнаружении ошибок или дефектов пользователь направляет подробную рекламацию в ОКБ САПР в установленном порядке.

СПО «Аккорд-KVM» поставляется по принципу «as is», т.е. владельцы авторских прав ни при каких обстоятельствах не предусматривают никакой компенсации за дополнительные убытки пользователя, включая любые потери прибыли, потери сохранности или другие убытки, вследствие аварийных ситуаций или их последствий, убытки, которые могут возникнуть из-за использования или невозможности использования нашей продукции.

При покупке и применении СПО «Аккорд-KVM» предполагается, что покупатель знаком с данными требованиями и согласен с положениями настоящего раздела.

10 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>.