



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Руководство по установке

37222406.501410.073 98

Листов 10

Москва
2022

АННОТАЦИЯ

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

Документ предназначен для администраторов – должностных лиц, обладающих знаниями и полномочиями, достаточными для того, чтобы устанавливать компоненты инфраструктуры виртуализации.

В документе описан порядок установки СПО «Аккорд-KVM».

Перед установкой СПО «Аккорд-KVM» рекомендуется внимательно ознакомиться с настоящим руководством.

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 Установка компонентов СПО «Аккорд-KVM»	7
2.1 Установка программного пакета «Аккорд-KVM».....	7
3 Техническая поддержка и информация о продукте	9
4 Перечень принятых сокращений.....	10

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 Общие сведения

1.1 Назначение СПО «Аккорд-KVM»

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

СПО «Аккорд-KVM» позволяет контролировать целостность компонентов VM (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 VM и обеспечивает выполнение контрольных процедур до ее запуска. СПО «Аккорд-KVM» поставляется в виде `rpm`-файла.

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 CentOS 7.4, CentOS 7.5, CentOS 7.6, CentOS 7.7, CentOS 7.9, CentOS 8.0, CentOS 8.3, Debian 10, Debian 11, Ubuntu 22.04, Ubuntu 20.04.3 LTS, AOS 5.15, «ROSA Virtualization» (ПСЮК.10102-01), «Р-виртуализация Linux 7.5», H3C CAS Virtualization Platform, программного комплекса «Средства виртуализации «Брест» (РДЦП.10001-02), 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 ВМ только одной гостевой ОС;
- объем свободного дискового пространства для размещения ПО на жестком диске – не менее 100 Мбайт (на сервере).

Также 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 Установка компонентов СПО «Аккорд-KVM»

2.1 Установка программного пакета «Аккорд-KVM»

ВНИМАНИЕ! До начала настройки СПО «Аккорд KVM» необходимо настроить инфраструктуру виртуализации: создать необходимые VM, сделать снапшоты и т. д.

Для установки программного пакета «Аккорд-KVM» в ОС CentOS и другие ОС, поддерживающие работу с rpm-пакетами, должен применяться файл `Accord-KVM-1.3-x.el7.centos.x86_64.rpm`, где 1.3-x – используемая версия пакета (например, 1.3-6). Установка выполняется по команде:

```
rpm -ivh accord-kvm-1.3-x.el7.centos.x86_64.rpm
```

В случае, если в системе уже существует скрипт для перехвата включения/миграции VM `qemu` из состава другого программного пакета, то для установки СПО «Аккорд-KVM» следует использовать команду с ключом `force`:

```
rpm -ivh accord-kvm-1.3-x.el7.centos.x86_64.rpm -force
```

Далее следует открыть установленный файл `/etc/libvirt/hooks/qemu` в текстовом редакторе и заменить строку «`exit 0`» на строку «`/etc/libvirt/hooks/qemu-orig $1 $2 $3`» (рисунок 1). В этом случае при включении/миграции VM сначала будут проведены процедуры контроля целостности СПО «Аккорд-KVM», и в случае успешного их прохождения будет выполнен скрипт другого программного пакета.

Для установки программного пакета «Аккорд-KVM» в ОС Debian и другие ОС, поддерживающие работу с deb-пакетами, должен применяться файл `Accord-KVM_1.3-x.deb`, где 1.3-x - используемая версия пакета (например, 1.3-6). Установка выполняется по команде:

```
dpkg -i Accord-KVM_1.3-x.deb
```

```

#!/bin/bash
RESULT=0
OUTPUT=
XML_PATH=/tmp/vm_desc
ACCORD_PATH=/etc/accordkvm/accordkvm

case "$2" in
start)
XML_DESC=$(cat)
echo "$XML_DESC" > $XML_PATH
OUTPUT=$(ACCORD_PATH start-vmcontrol $1 $XML_PATH)
RESULT=$?
;;
stopped)
XML_DESC=$(cat)
echo "$XML_DESC" > $XML_PATH
OUTPUT=$(ACCORD_PATH set-logvmoff $1 $XML_PATH)
RESULT=0
;;
--default)
RESULT=0
;;
esac

if [ $RESULT -ne 0 ]; then
echo "Task was blocked by Accord-KVM" >&2
echo "$OUTPUT" >&2
exit 5
else
exit 0
fi

```

```

#!/bin/bash
RESULT=0
OUTPUT=
XML_PATH=/tmp/vm_desc
ACCORD_PATH=/etc/accordkvm/accordkvm

case "$2" in
start)
XML_DESC=$(cat)
echo "$XML_DESC" > $XML_PATH
OUTPUT=$(ACCORD_PATH start-vmcontrol $1 $XML_PATH)
RESULT=$?
;;
stopped)
XML_DESC=$(cat)
echo "$XML_DESC" > $XML_PATH
OUTPUT=$(ACCORD_PATH set-logvmoff $1 $XML_PATH)
RESULT=0
;;
--default)
RESULT=0
;;
esac

if [ $RESULT -ne 0 ]; then
echo "Task was blocked by Accord-KVM" >&2
echo "$OUTPUT" >&2
exit 5
else
/etc/libvirt/hooks/qemu-orig $1 $2 $3
fi

```

Рисунок 1 – Изменения в файле /etc/libvirt/hooks/qemu

После установки СПО «Аккорд-KVM» следует перезапустить сервис libvirtd:

```
service libvirtd restart
```

Установленные на гипервизоре версии СПО «Аккорд-KVM», СПО СЗИ НСД «Аккорд-Х К» и пакетов libvirt и libguestfs¹ доступны к просмотру на терминале по команде

```
accordkvm info
```

или могут быть получены стандартными средствами ОС.

¹ Для работы «Аккорд-KVM» следует устанавливать библиотеку libguestfs версии не ниже 1.36.3

3 Техническая поддержка и информация о продукте

В случае необходимости консультации ЗАО «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, +7 (926) 235-89-17 или по адресу электронной почты support@accord.ru. Наш адрес в Интернете <http://www.okbsapr.ru>.

4 Перечень принятых сокращений

- БИ – безопасность информации;
- ИВ – инфраструктура виртуализации;
- ВМ – виртуальная машина;
- НСД – несанкционированный доступ;
- ПО – программное обеспечение;
- ПЭВМ – персональная электронно-вычислительная машина;
- СЗИ – средство защиты информации;
- СПО – специальное программное обеспечение.