СПО СЗИ НСД «Аккорд-В.»

Средство защиты Vmware vSphere

ОКБ САПР
2022

Защита систем виртуализации

В виртуальных средах также, как и в физических, хранится огромное количество различного рода информации и совершается множество вычислений и действий. Поэтому **виртуальные среды нуждаются в защите наряду с физическими**.

Для защиты виртуальных сред также, как и для физических, необходимо построить **доверенную вычислительную среду**.

Назначение и состав «Аккорд-В.»

СПО «Аккорд-В.» предназначено для защиты инфраструктур виртуализации на базе платформы VMware vSphere 6.7.

В состав СПО «Аккорд-В.» входят:

- ✓ сервис регистрации событий;
- ✓ программное обеспечение (ПО) управления;
- ✓ агенты защиты ESXi серверов.

Назначение и состав «Аккорд-В.»

Схема взаимодействия СПО «Аккорд-В.»:

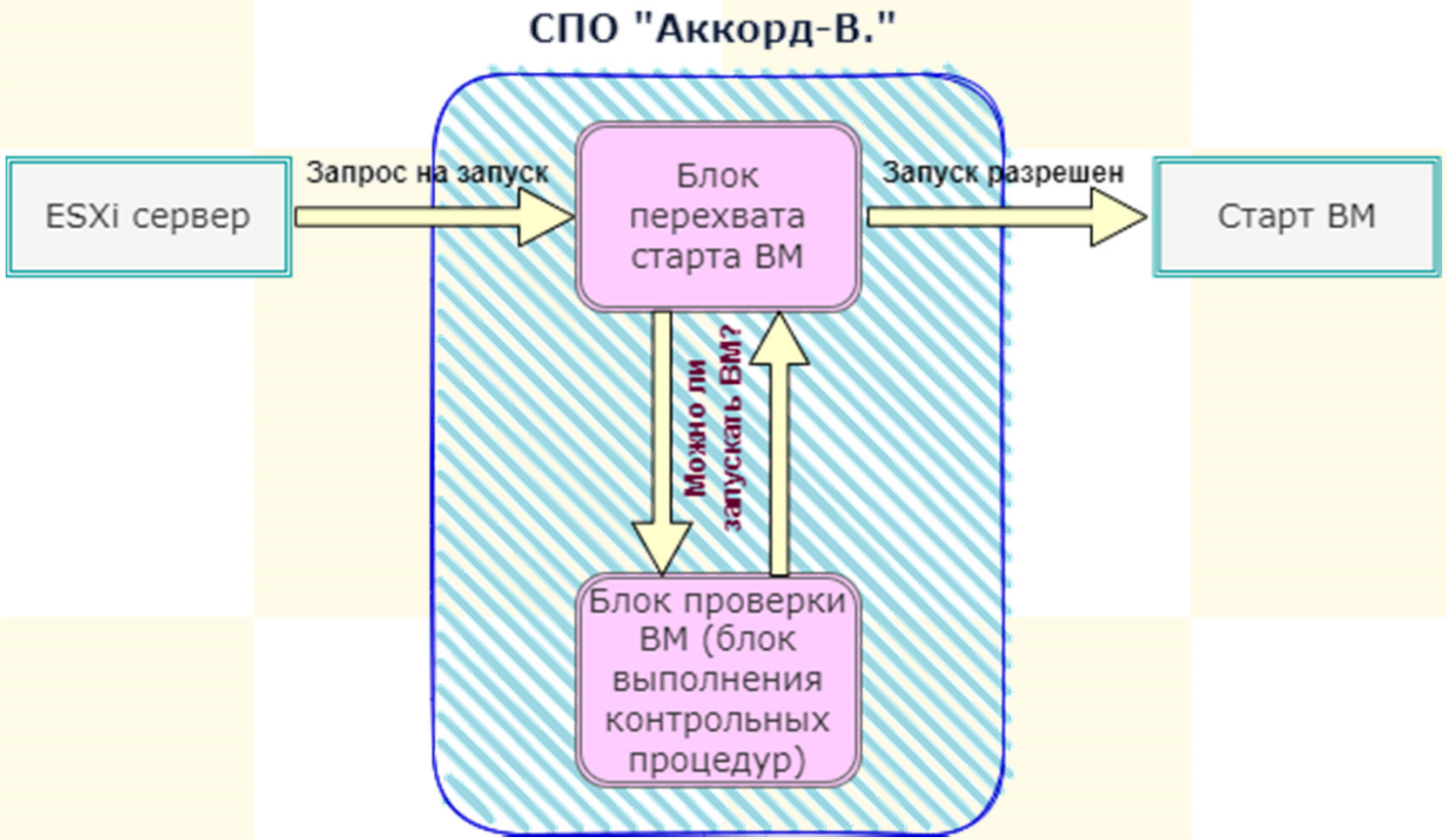
Основные функции «Аккорд-В.»

- ✓ доверенная загрузка всех элементов ВМ инфраструктуры виртуализации;
- ✓ контроль целостности оборудования ВМ, а также BIOS и MBR ВМ, выполняемого до их запуска;
- ✓ регистрация событий о действиях в инфраструктуре виртуализации (на серверах vCenter и ESXi), а также событий агентов СПО «Аккорд-В.»;

Основные функции «Аккорд-В.»

- ✓ идентификация и аутентификация администратора безопасности при входе на ESXi сервера;
- ✓ создание и восстановление резервных копий баз данных агентов СПО «Аккорд-В.» на ESXi серверах;
- ✓ управление размещением и перемещением исполняемых ВМ между контролируемыми серверами виртуализации путем контроля запуска ВМ.

Принцип работы



Совокупность решений «Аккорд-В.»

СПО «Аккорд-В.» легко установить и настроить. Интерфейс прост в восприятии и не вызывает серьезных затруднений в работе. СПО «Аккорд-В.» не помешает работе других сервисов и программ.

Однако СПО «Аккорд-В.» способен защитить только ВМ. Как быть, если для защиты системы потребуется обеспечить, доверенную загрузку ОС физического компьютера, на котором находится ВИ, или же ограничить доступ пользователей к ресурсам ПК и ВМ?

Совокупность решений «Аккорд-В.»

Чтобы привести защиту инфраструктуры виртуализации в соответствие требованиям регуляторов (руководящие документы и приказы ФСТЭК), необходимо полагаться не на один продукт, а на совокупность решений.

Совокупность решений (СР) «Аккорд В.» для защиты среды виртуализации – это решение, способное обеспечить доверенную вычислительную среду одновременно и в физической инфраструктуре, и в инфраструктуре виртуализации.

Назначение СР «Аккорд-В.»

СР «Аккорд-В.» дополняет СПО «Аккорд-В.» средствами обеспечения доверенной загрузки физической среды и средствами разграничения доступа персонала к ресурсам «реального» СВТ и ВМ.

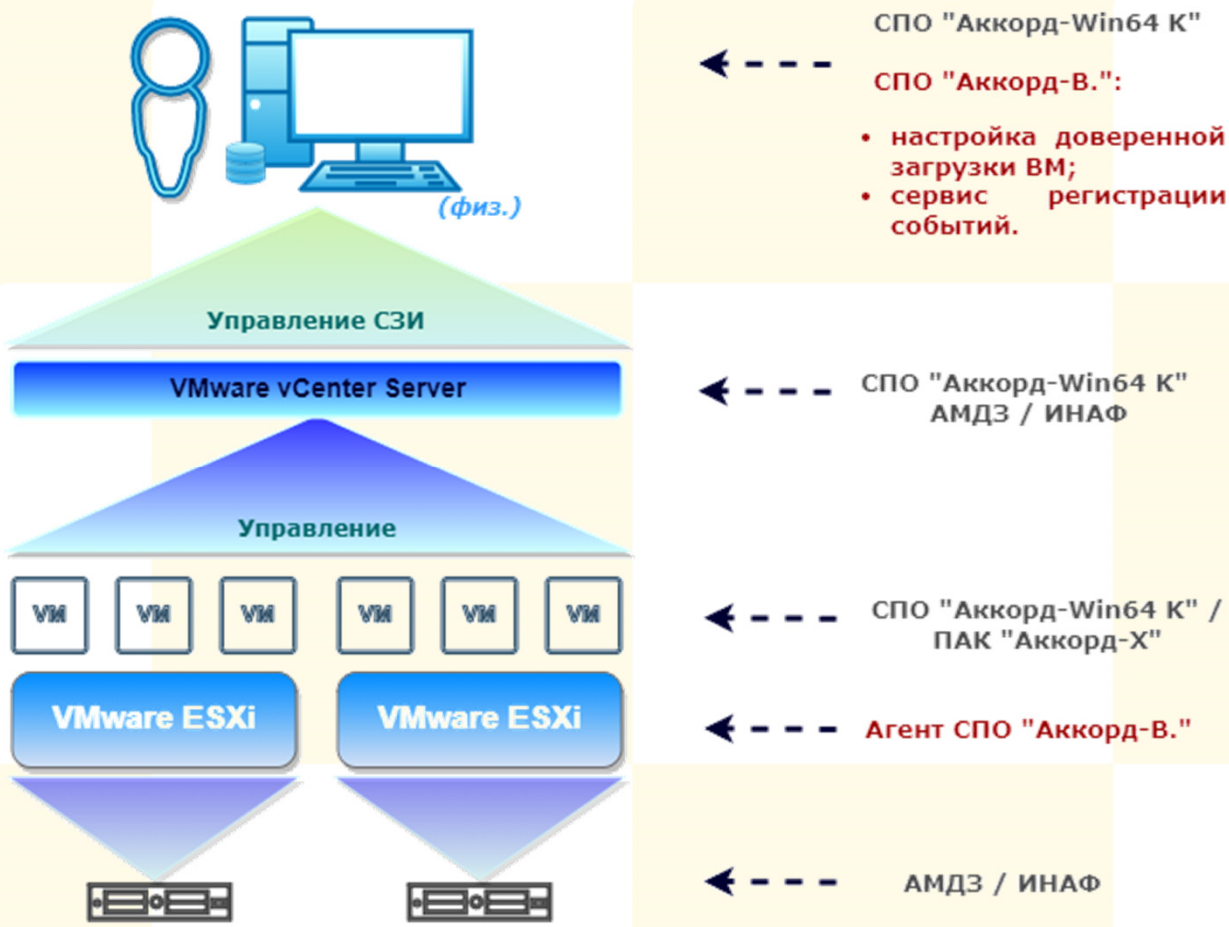
СР «Аккорд В.» – это комплексное решение, включающее в себя все необходимые элементы для реализации требований по защите информации.

Состав СР «Аккорд-В.»

СР «Аккорд-В.» *может состоять* из следующих компонентов:

- ✓ модули доверенной загрузки для физических АРМ – «Аккорд-АМДЗ» и «Инаф» (в различных вариациях);
- ✓ СПО «Аккорд-В.»;
- ✓ СПО «Аккорд-Win64 К»/ ПАК «Аккорд-Х» (применяются как для защиты ВМ, так и физических АРМ; данные решения применимы как для VDI, так и для терминальных серверов).

Состав СР «Аккорд-В.»



Красным шрифтом выделены компоненты, входящие в состав СПО «Аккорд-В.»;

Серым шрифтом выделены примеры решений, которые могут входить в состав СР «Аккорд-В.».

Принцип работы СР «Аккорд-В.»

Каждое из решений, входящих в состав СР «Аккорд-В.», является самостоятельным продуктом.

В совокупности эти решения становятся комплексом, основанным на принципе непрерывности контрольных процедур и обеспечивающим контроль целостности и доверенную загрузку как физического оборудования, так и инфраструктуры виртуализации.

Принцип работы СР «Аккорд-В.»

На физическом уровне СР выполняет контроль целостности оборудования физических серверов, затем – файлов ОС; на виртуальном уровне – проверяет файлы BIOS и конфигурации оборудования, затем MBR и файлы ОС ВМ.

Такой принцип действия позволяет получить доверенную изолированную программную среду внутри виртуальных машин. Попытка дискредитации хотя бы одного из «слоев» механизма контроля приводит к блокировке работы инфраструктуры виртуализации.

Возможности СР «Аккорд-В.»

- ✓ доверенная загрузка и контроль целостности всех элементов инфраструктуры виртуализации;
- ✓ разграничение доступа персонала СР (АБИ и АВИ);
- ✓ разграничение доступа пользователей внутри виртуальных машин;
- ✓ контроль доступа пользователей и процессов к защищаемым объектам (дискреционный и мандатный механизмы);

Возможности СР «Аккорд-В.»

- ✓ очистка оперативной и внешней памяти путём записи маскирующей информации в память при её освобождении (перераспределении);
- ✓ аппаратная идентификация всех пользователей и администраторов инфраструктуры виртуализации.

Выполнение требований регуляторов

Базовые меры 17-21 Приказов ФСТЭК России:

ИАФ: 1, 2, 3, 4, 5, 6;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 13, 15, 17;

ОПС: 1;

ЗНИ: 2, 5, 8;

РСБ: 1, 2, 3, 4, 5, 7;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 3, 4, 5;

ЗСВ: 1, 2, 3, 6, 7, 8;

ЗИС: 1, 5, 15, 21, 30;

ИНЦ: 2;

Выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры Приказов 17-21 ФСТЭК России:

ИАФ: 7;

УПД: 7, 12;

ОПС: 4;

ЗНИ: 4, 6, 7;

РСБ: 8;

ОЦЛ: 2, 5, 8;

ЗСВ: 5;

ЗИС: 6, 19, 29.

Выполнение требований регуляторов

Базовые меры 31 Приказа ФСТЭК России:

ИАФ: 1, 2, 3, 4, 5, 7;

УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11, 13;

ОПС: 1;

ЗНИ: 2, 5, 6, 7, 8;

АУД: 2, 4, 6, 7, 8, 9;

ОЦЛ: 1, 3, 4, 5;

ОДТ: 3, 4, 5;

ЗИС: 1, 13, 21, 33, 38, 39;

ИНЦ: 1, 2;

ОПО: 4;

ДНС: 4, 5;

Выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры 31 Приказа ФСТЭК России:

ИАФ: 6;

УПД: 7, 12;

ОПС: 3;

ЗНИ: 4;

ОЦЛ: 2;

ЗИС: 12, 22, 37.

Спасибо за внимание!

Если у вас возникли вопросы, то **напишите нам**.

Наш сайт в интернете:
www.okbsapr.ru