Инфраструктурные решения

ОКБ САПР
2022

Инфраструктурные решения на базе продуктов ОКБ САПР

Для решения задач защиты информации в распределенных инфраструктурах должны применяться специальные средства защиты – инфраструктурные решения.

ОКБ САПР представляет такие:

- ✓ ПАК «Центр-Т»;
- ✓ СУЦУ СЗИ НСД «Аккорд»;
- ✓ «Паспорт ПО»;
- ✓ Аккорд-KVM Control Point.

«Центр-Т»

«Центр-Т» предназначен для централизованной контролируемой загрузки образов ПО на клиентские рабочие станции, а также их централизованного администрирования.

В общем случае «Центр-Т» предполагает использование существующей в организации инфраструктуры – приобретать дополнительные СВТ не нужно.

Схема работы «Центр-Т»

«Центр-Т» организует взаимодействие терминалов удаленного доступа с сервером хранения и сетевой загрузки (СХСЗ).

Функции «Центр-Т»

✓ сетевая загрузка ПО на рабочие станции (РС):

- идентификация пользователей РС для начала работы с терминальным сервером по номерам клиентских устройств;
- двухфакторная аппаратная идентификация пользователей РС в ПАК «Аккорд» на терминальном сервере;
- передачу образов ПО РС с СХСЗ на РС по сети;
- проверку целостности и подлинности полученного образа Клиентом;

Функции «Центр-Т»

✓ централизованное администрирование:

- сборка образов ПО РС с нужными параметрами;
- сопоставление образов ПО РС учетным записям пользователей;
- настройка сетевых параметров;
- резервирование баз данных и настроек СХСЗ и Клиента;
- контроль периферийного оборудования в рамках терминальной сессии;
- контроль настроек образов ПО РС;
- восстановление ПО «Центр Т» из резервных копий при возникновении нештатных ситуаций;

Функции «Центр-Т»

- ✓ централизованный аудит событий:

- регистрация действий пользователей и администраторов СХСЗ в журналах загрузки образов ПО РС и журналах активности администраторов СХСЗ;
- регистрация пользователей и клиентских устройств.

«Центр-Т» реализует

Базовые меры 17-21 Приказов ФСТЭК:

ИАФ: 1, 2, 3, 4, 5;

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

ОПС: 1, 2, 3;

ЗНИ: 2, 5;

РСБ: 1, 2, 3, 5, 6, 7;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 2, 3;

ЗИС: 1, 5, 11, 15, 21, 22;

ИНЦ: 2;

УКФ: 2.

«Центр-Т» реализует

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

ИАФ: 7;

УПД: 7;

ОПС: 4;

ЗНИ: 6, 7;

ОДТ: 6;

РСБ: 8;

ЗИС: 4, 10, 14, 16, 18, 19, 25, 26.

СУЦУ СЗИ НСД «Аккорд»

СУЦУ СЗИ от НСД – система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд».

СУЦУ централизовано

- собирает и хранит зарегистрированные события доступа к ПКО,
- управляет средствами защиты информации от несанкционированного доступа «Аккорд», установленными на ПКО.

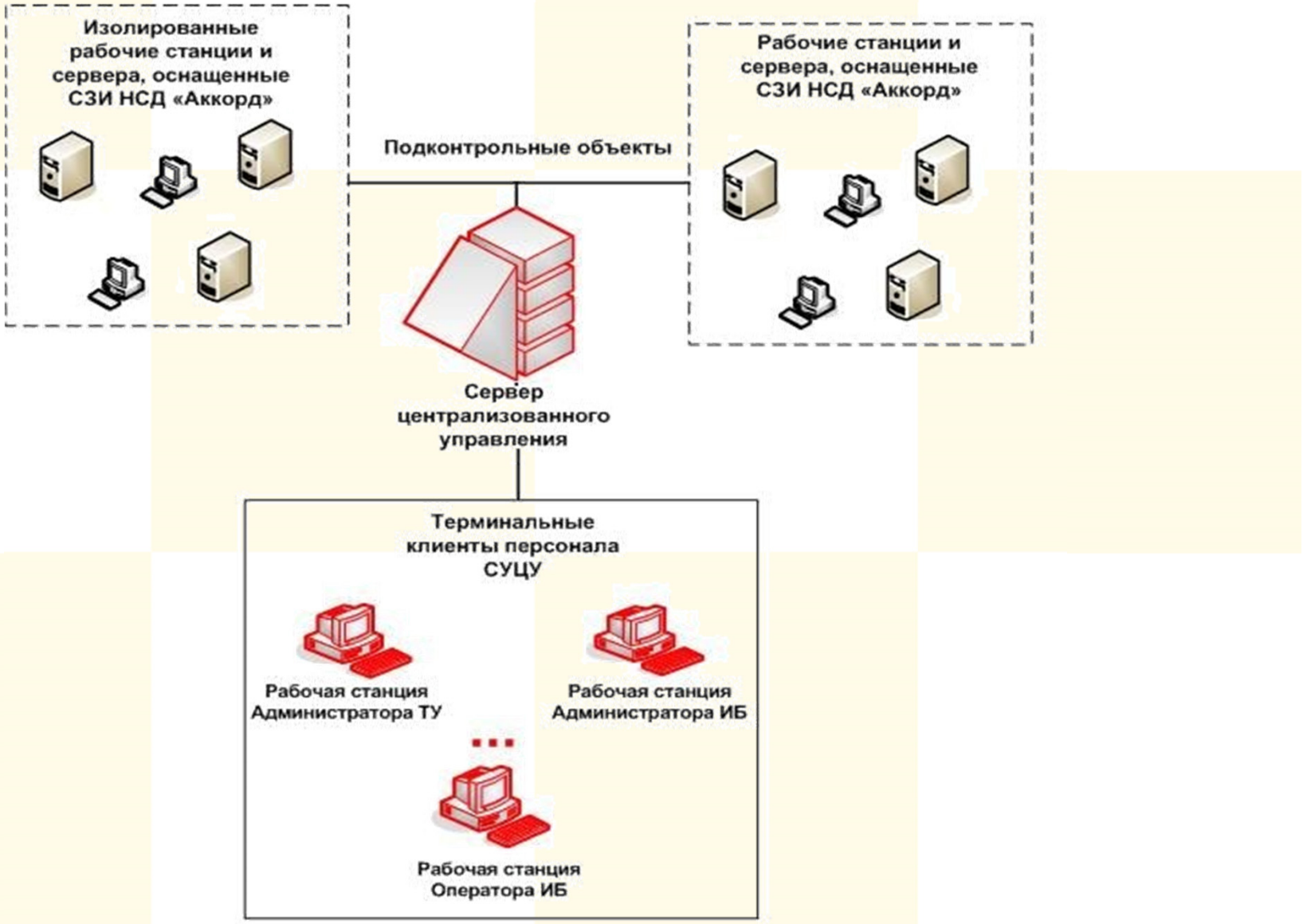
Функции СУЦУ СЗИ НСД

- ✓ информирует персонал о попытках НСД;
- ✓ предоставляет единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей;
- ✓ обеспечивает централизованный мониторинг событий ИБ;
- ✓ централизованно управляет подконтрольными объектами (компьютерами сотрудников) и средствами защиты информации от несанкционированного доступа «Аккорд»;

Функции СУЦУ СЗИ НСД

- ✓ поддерживает ролевую инфраструктуру (7 ролей), каждая отдельная роль обладает специфическим набором возможностей, нехарактерных для других ролей;
- ✓ обеспечивает управление ролями и учетными записями персонала;
- ✓ обеспечивает возможность интеграции с:
- продуктами типа Business Intelligence – в частности, с Tivoli, есть положительный опыт интеграции с продуктом Contour BI;
- с системой контроля и управления доступом СКУД.

Схема информационного взаимодействия



«Паспорт ПО»

Управляющий персонал системы должен знать, какое ПО установлено в системе, которой он управляет.

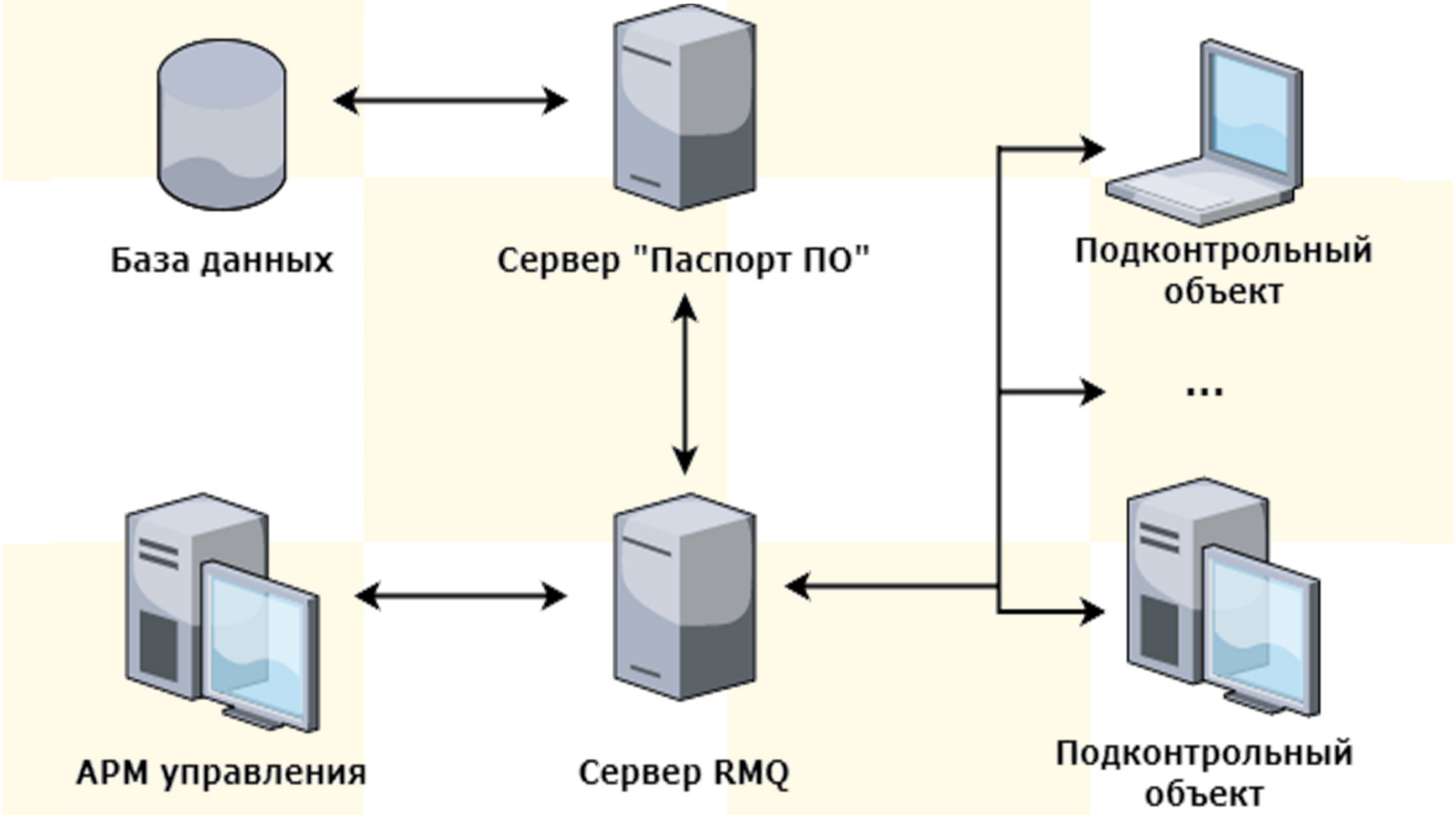
Для систематической (или внезапной, вне расписания) проверки состава ПО на рабочих местах предназначен программный продукт «Паспорт ПО».

Для каждого рабочего места «Паспорт ПО» создает и периодически проверяет «паспорт», в котором отражен перечень установленного ПО и его характеристики.

Состав «Паспорт ПО»

- ✓ сервер с базой данных, компонент управления (автоматизированное рабочее место – АРМ – управления);
- ✓ клиентский компонент, устанавливаемый на подконтрольные объекты (ПКО);
- ✓ сервис обмена сообщениями RabbitMQ, обеспечивающий взаимодействие по сети между всеми элементами.

Состав «Паспорт ПО»



Принцип работы «Паспорт ПО»

«Паспорт ПО» построен в соответствии с одной из концепций повышения защищённости информационной системы за счёт управления её конфигурациями: Security-Focused Configuration Management of Information Systems, SecCM.

«Паспорт ПО» автоматизирует

- контроль целостности состояния программной среды (именно состояния, а не среды как таковой, то есть основных характеристик файлов программного обеспечения)

- и контроль изменений состава ПО (установленные на средство вычислительной техники системные и прикладные программные продукты).

Порядок работы «Паспорт ПО»

1. Создается запись специального вида – проект паспорта ПО, которая фиксирует состояние конфигурации СВТ (программной среды вместе с совокупностью состава ПО).

2. Администратор заверяет проект паспорта и тот после этого становится паспортом ПО и представляет эталонное состояние конфигурации СВТ.

3. Фактическое состояние конфигурации сравнивается с эталонным (паспортом) по мере необходимости.

«Паспорт ПО»: выполнение требований регуляторов

Базовые меры 17-21 Приказов ФСТЭК России:

АНЗ: 2, 4;

ОЦЛ: 1;

ЗИС: 18.

Базовые меры 239 Приказа ФСТЭК России:

АУД: 1;

ОЦЛ: 1;

ОДТ: 8;

ОПО: 2.

«Аккорд-KVM Control Point»

«Аккорд-KVM Control Point» централизовано удаленно управляет СПО «Аккорд-KVM», установленным на серверах виртуализации, через web-интерфейс.

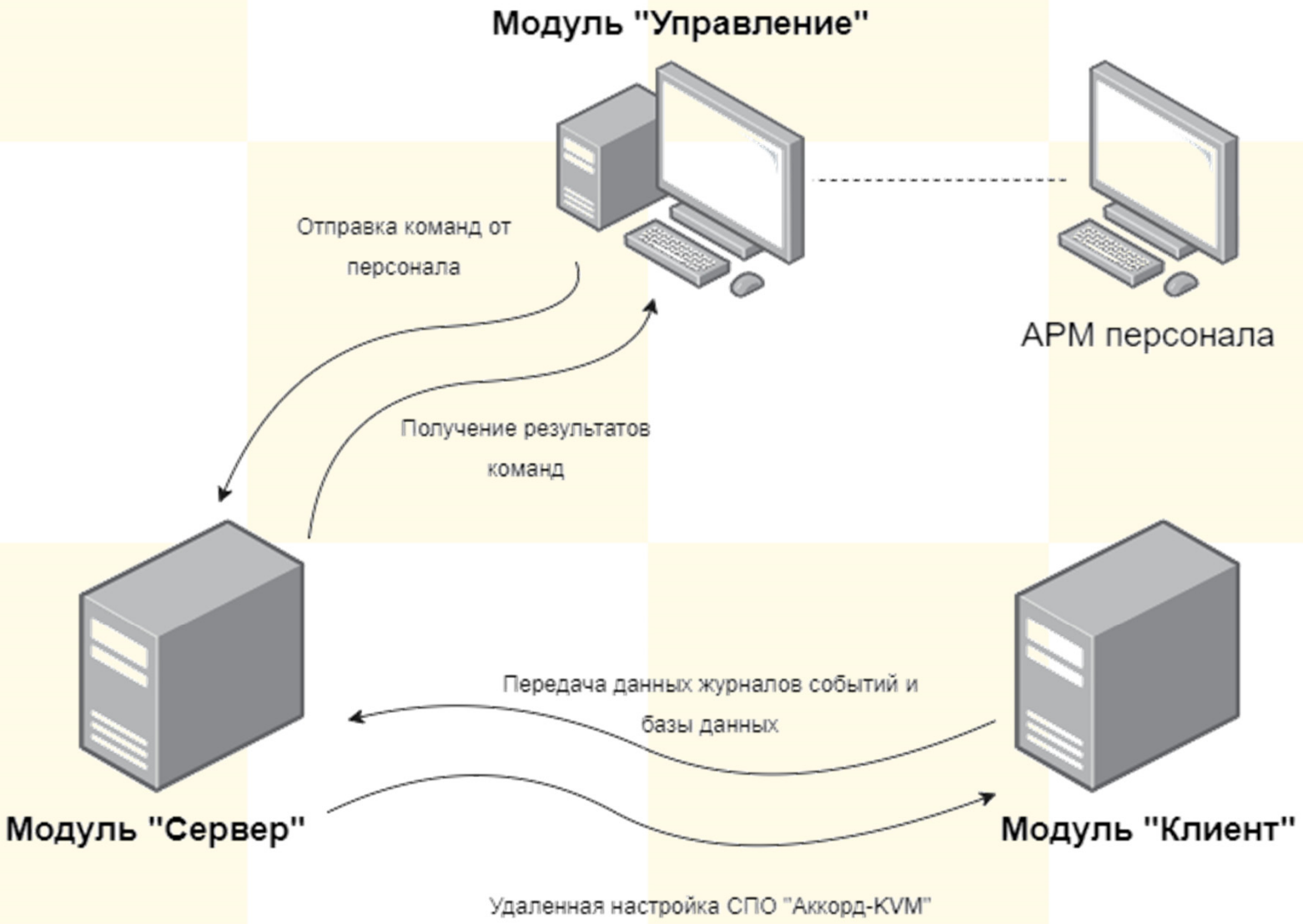
3 группы функций управления:

- ✓ настройка режима работы СПО «Аккорд-KVM» (обычный или мягкий);
- ✓ постановка на контроль и снятие с контроля в СПО «Аккорд-KVM» ВМ и их компонентов;
- ✓ удалённый сбор журналов событий СПО «Аккорд-KVM».

Структура «Аккорд-KVM Control Point»

- ✓ модуль «Управление»;
- ✓ модуль «Сервер»;
- ✓ модуль «Клиент».

Взаимодействие компонентов «Аккорд-KVM Control Point»



Функции «Аккорд-KVM Control Point»

- ✓ выбирать режим функционирования «Аккорд KVM» (обычный или «мягкий»);
- ✓ устанавливать ВМ на контроль с разрешением или запретом их включения;
- ✓ снимать ВМ с контроля;
- ✓ устанавливать на контроль оборудование ВМ;
- ✓ снимать оборудование ВМ с контроля;
- ✓ создавать список контролируемых файлов (создание файл-листа);

Функции «Аккорд-KVM Control Point»

- ✓ назначать списки контролируемых файлов ВМ (установка файлов ВМ на контроль);
- ✓ снимать файлы ВМ с контроля;
- ✓ проверять целостность контролируемой ВМ;
- ✓ собирать журналы событий;
- ✓ просматривать список ВМ;
- ✓ управлять пользователями (создавать/удалять/редактировать учетные записи пользователей, менять пароль, искать пользователя по имени учетной записи).

Порядок работы «Аккорд-KVM Control Point»

1. Пользователи подключаются к web-интерфейсу «Аккорд-KVM Control Point» через браузер.
2. На экране появляется окно идентификации/ аутентификации пользователя, в котором необходимо ввести идентификационные данные (имя пользователя и пароль).
3. После успешной идентификации и аутентификации пользователь получает доступ к графическому web-интерфейсу «Аккорд-KVM Control Point» и может выполнять функции централизованного управления СПО «Аккорд-KVM».

Спасибо за внимание!

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

Наш сайт в интернете:
www.okbsapr.ru