



ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Специальное программное обеспечение «Аккорд-В.»

Руководство по установке

37222406.26.20.40.140.086 98

Листов 71

**Москва
2025**

АННОТАЦИЯ

Настоящий документ является руководством по установке специального программного обеспечения «Аккорд-В.» (далее по тексту – СПО «Аккорд-В.», «Аккорд-В.»), предназначенного для защиты инфраструктур виртуализации, построенных на базе платформы виртуализации VMware vSphere 6.7.

Документ предназначен для администраторов – должностных лиц, обладающих знаниями и полномочиями достаточными для того, чтобы настраивать и управлять инфраструктурой виртуализации VMware vSphere.

В документе приведены особенности установки и настройки СПО «Аккорд-В.».

Перед установкой и эксплуатацией СПО «Аккорд-В.» рекомендуется внимательно ознакомиться с настоящим Руководством.

Применение СПО «Аккорд-В.» должно дополняться общими мерами предосторожности и физической безопасности.

СОДЕРЖАНИЕ

1. Общие сведения.....	6
1.1. Назначение СПО «Аккорд-В.»	6
1.2. Состав СПО «Аккорд-В.»	6
1.3. Технические условия применения СПО «Аккорд-В.»	7
2. Начало работы	7
2.1. Типовые варианты построения инфраструктуры виртуализации.....	7
2.2. Расположение сервиса регистрации событий.....	9
2.3. Пример развертываемой инфраструктуры	9
2.4. Особенности установки ESXi	10
3. Установка и настройка компонентов СПО «Аккорд-В.»	12
3.1. Схема развертывания защищенной инфраструктуры виртуализации.....	12
3.2. Порядок установки и настройки СПО «Аккорд-В.»	13
3.3. Установка и настройка аппаратной части инфраструктуры	15
3.4. Установка и настройка ПО ПАК «ПИ ШИПКА» на физических АРМ (vCenter / АРМ АБИ) и ВМ	16
3.5. Установка и настройка ПО разграничения доступа на физических АРМ (vCenter / АРМ АБИ) и ВМ	16
3.5.1. Общие сведения.....	16
3.5.2. Разделение ролей администраторов, создание и настройка их учетных записей на vCenter.....	16
3.6. Установка и настройка модулей СПО «Аккорд-В.»	18
3.6.1. Начало процедуры установки	18
3.6.2. Установка модулей «Аккорд-В.»	19
3.6.3. Установка агентов «Аккорд-В.» на ESXi.....	23
3.6.4. Установка и настройка сервиса регистрации событий	30
3.6.5. Предъявление лицензии на работу с ПО управления	36
3.7. Работа с утилитой управления «Accord-V.»	37
3.7.1. Авторизация АБИ в системе.....	37
3.7.2. Настройка доверенной загрузки виртуальной машины с vCenter	41
3.7.3. Настройка доверенной загрузки ВМ	42
3.7.4. Особенности настройки доверенной загрузки ВМ при работе с Citrix XenDesktop	54
3.8. Настройка разграничения доступа на совмещенном АРМ АБИ/АИБ	57

4. Создание резервных копий	57
5. Включение режима ESXi Lockdown Mode.....	58
6. Порядок действий при обновлении гипервизора с установленным СПО «Аккорд-В.»	59
7. Интеграция СПО «Аккорд-В.» с IBM Security QRadar	59
8. Удаление ПО «Аккорд-В.».....	66
9. Лицензирование	68
10. Сервисные команды	70
11. Техническая поддержка	71

ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Администратор БИ (или АБИ) – администратор безопасности информации, привилегированный пользователь - должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ организует установку комплекса в ПЭВМ, настройку защитных механизмов комплекса в соответствии с правами доступа пользователей, осуществляет контроль за правильным использованием ПЭВМ с установленным комплексом и периодическое тестирование средств защиты комплекса.

Администратор ИВ (или АИВ) – администратор инфраструктуры виртуализации, привилегированный пользователь - должностное лицо, отвечающее за настройку и обслуживание инфраструктуры виртуализации.

АРМ - автоматизированное рабочее место.

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

Доверенная загрузка – загрузка ОС только после проведения контрольных процедур идентификации/аутентификации пользователей, проверки целостности технических и программных средств ПЭВМ (РС) с использованием алгоритма пошагового контроля целостности.

Идентификатор – специальное устройство, содержащее уникальный признак пользователя, с которым зарегистрированный пользователь входит в систему и который используется системой для определения его прав, а также для регистрации факта доступа и характера выполняемых им работ или предоставляемых ему услуг.

КЦ - контроль целостности.

Пользователь – субъект доступа к объектам (ресурсам) ПЭВМ/ВМ.

Ошибки – информация, выводимая на дисплей, указывающая на неправильность действий, сбои, аварии комплекса.

Примечания – замечания в описании некоторых команд, содержащие рекомендации администратору БИ по порядку использования этих команд. Пояснения выделены мелким шрифтом.

Сообщения - информация, выводимая на дисплей, которая сообщает о действиях, требуемых от пользователя, о состоянии программы и о корректно завершенных действиях.

1. Общие сведения

1.1. Назначение СПО «Аккорд-В.»

Специальное программное обеспечение «Аккорд-В.» предназначено для защиты инфраструктур виртуализации, построенных на базе платформы виртуализации VMware vSphere 6.7.

«Аккорд-В.» представляет собой программное средство, предназначенное для выполнения основных функций защиты от НСД на основе:

- доверенной загрузки всех элементов ВМ инфраструктуры виртуализации;
- контроля целостности оборудования ВМ, а также BIOS и MBR ВМ, выполняемого до их запуска;
- регистрации событий о действиях в инфраструктуре виртуализации (на серверах vCenter и ESXi), а также событий агентов СПО «Аккорд-В.»;
- идентификации и аутентификации администратора безопасности при входе на серверы ESXi;
- создания и восстановления резервных копий баз данных агентов СПО «Аккорд-В.» на серверах ESXi;
- управления размещением и перемещением исполняемых виртуальных машин между контролируемыми СПО «Аккорд-В.» серверами виртуализации путем контроля запуска ВМ.

1.2. Состав СПО «Аккорд-В.»

Система защиты «Аккорд-В.» полностью интегрируется в инфраструктуру виртуализации vSphere, поэтому для ее функционирования не требуются дополнительные серверы. В основу разработки «Аккорд-В.» положен принцип, согласно которому система защиты не должна принципиально ограничивать возможности инфраструктуры виртуализации, оставляя доступными все ее преимущества.

Программное средство «Аккорд-В.» включает в себя следующие модули:

а) *ПО управления*, устанавливаемое на АРМ АБИ и включающее следующие утилиты:

- «Installer-V.», предназначенную для развертывания агентов «Аккорд-В.» на ESXi. Агенты «Аккорд-В.», устанавливаемые на ESXi, предназначены для выполнения доверенной загрузки ВМ;
- «Accord-V.», предназначенную для настройки доверенной загрузки виртуальных машин;
- «LogViewer-V.», предназначенную для просмотра зарегистрированных событий;

б) *сервис регистрации событий*, устанавливаемый на АРМ АБИ или в ОС отдельного сервера (рекомендуемый вариант), предназначенный для сбора событий инфраструктуры VMware vSphere, а также с агентов «Аккорд-В.» на ESXi (для установки сервиса регистрации событий в ОС предназначена вспомогательная утилита LogServiceInstaller).

1.3. Технические условия применения СПО «Аккорд-В.»

Для установки СПО «Аккорд-В.» требуется следующий минимальный состав технических и программных средств:

- наличие инфраструктуры виртуализации, построенной на базе платформы VMware vSphere 6.7;
- наличие свободного слота PCI/PCI-X/Express/USB на материнской плате ПЭВМ (для всех ESXi и для vCenter, если он физический);
- объем свободного дискового пространства для размещения ПО на жестком диске около 50 Мбайт (на vCenter-сервере и на ESXi-сервере);
- реализация АРМ АБИ в виде физической машины под управлением ОС Windows, в которой установлены:
 - программная платформа Microsoft .NET Framework 3.5;
 - распространяемые пакеты (Redistributable Package) Microsoft Visual C++ 2008 (x86) и Microsoft Visual C++ 2010 (x86).

Для эффективного применения средств защиты СПО «Аккорд-В.» **необходимо** использование сертифицированных экземпляров СПО «Аккорд-Win64 К» или ПАК СЗИ НСД «Аккорд-Win32» (для 32-битных ОС Microsoft Windows) / ПАК СЗИ НСД «Аккорд-Win64» (для 64-битных ОС Microsoft Windows) на каждом сервере управления.

2. Начало работы

Перед началом установки и настройки СПО «Аккорд-В.» необходимо определиться с архитектурой развертываемой инфраструктуры виртуализации. Для этого следует ответить на следующие вопросы:

- 1) ESXi отдельные (без vCenter), или предполагается наличие vCenter?
- 2) vCenter физический или исполняемый на виртуальной машине (на Windows или VMware vCenter Server Appliance (vCSA))?
- 3) АРМ АБИ совпадает с vCenter или отдельный?
- 4) где располагается сервис регистрации событий (на vCenter или на отдельном АРМ (ВМ), например, АРМ АБИ)?

2.1. Типовые варианты построения инфраструктуры виртуализации

ВНИМАНИЕ! АРМ АБИ не может быть реализовано в виде виртуальной машины.

1. vCenter совмещен с АРМ АИВ/АБИ и располагается на физическом СБТ, на нем установлен «Аккорд-АМДЗ», СПО «Аккорд-В.» и ПО разграничения доступа для терминального режима из состава СПО «Аккорд-Win64 К» / ПАК «Аккорд-Win32» / ПАК «Аккорд-Win64».

При такой реализации возможны 2 варианта работы:

- 1) АИВ и АБИ работают локально на данном СБТ;
- 2) АИВ и АБИ работают удаленно, подключаясь к ОС с vCenter по RDP протоколу. В этом случае:
 - на АРМ, с которого будет происходить подключение, должен быть установлен терминальный клиент «Аккорд-ТК»;
 - на vCenter должно быть два сетевых интерфейса (один – для удаленных подключений, второй – для соединений с другими элементами инфраструктуры, такими как ESXi). На интерфейсе для удаленных подключений должен быть открыт только порт для RDP протокола (3389).

Примечание: Если данное действие предполагается реализовывать встроенным firewall в Windows, то необходимо учитывать, что политики применяются не к отдельным сетевым картам, а только к сетевым профилям.

При этом в ОС с vCenter необходимо, чтобы:

- доступ к ПО администрирования ПАК «Аккорд-Win64»/ ПАК «Аккорд-Win32» / СПО «Аккорд-Win64 К» и ПО «Аккорд-В.» был только у АБИ;
- доступ к браузеру (в случае использования WebClient) и vClient был только у АИВ.

2. АРМ АБИ/АИВ не совмещен с vCenter. На нем установлено СПО «Аккорд-В.» и ПО разграничения доступа для терминального режима из состава СПО «Аккорд-Win64 К» / ПАК «Аккорд-Win32» / ПАК «Аккорд-Win64». В таком случае **vCenter может быть любым (физическим / ВМ с гостевой ОС Windows / VCSA) или вообще отсутствовать.**

При такой реализации необходимо на каждом рабочем месте, имеющем связь с vCenter, установить ПО разграничения доступа и с его помощью ограничить доступ:

- к vClient и браузеру – для АБИ;
- к ПО администрирования «Аккорд-Win32»/«Аккорд-Win64»/«Аккорд-Win64 К» и ПО «Аккорд-В.» – для АИВ.

Примечание: АРМ АБИ и АРМ АИВ могут быть совмещены.

Следует учитывать, что работа с vCenter в качестве ВМ (VCSA или Windows) требует подключения к ESXi для выполнения настройки контроля целостности и доверенной загрузки (подробнее см. 3.7.2).

2.2. Расположение сервиса регистрации событий

ВНИМАНИЕ! При определении месторасположения сервиса регистрации событий необходимо учитывать требование обеспечить (в том числе организационными мерами) бесперебойность работы АРМ, на котором будет установлен сервис регистрации событий (данный сервис никогда не должен выключаться), поскольку в противном случае события, полученные с vCenter, могут быть пропущены.

Возможные варианты расположения сервиса регистрации событий:

1. На одном АРМ с АРМ АБИ;
2. На отдельном АРМ от АРМ АБИ (в том числе это может быть и vCenter).

Примечание: События агентов «Аккорд-В.» на ESXi также дублируются в syslog. В связи с этим, если в инфраструктуре используются централизованные системы регистрации событий (в том числе умеющие собирать события от vCenter), от сервиса регистрации событий можно отказаться.

2.3. Пример разворачиваемой инфраструктуры

Пример инфраструктуры представлен на рисунке 1.

ВНИМАНИЕ! В процессе создания виртуальных машин следует учитывать, что имя виртуальной машины не должно содержать символов кириллицы.

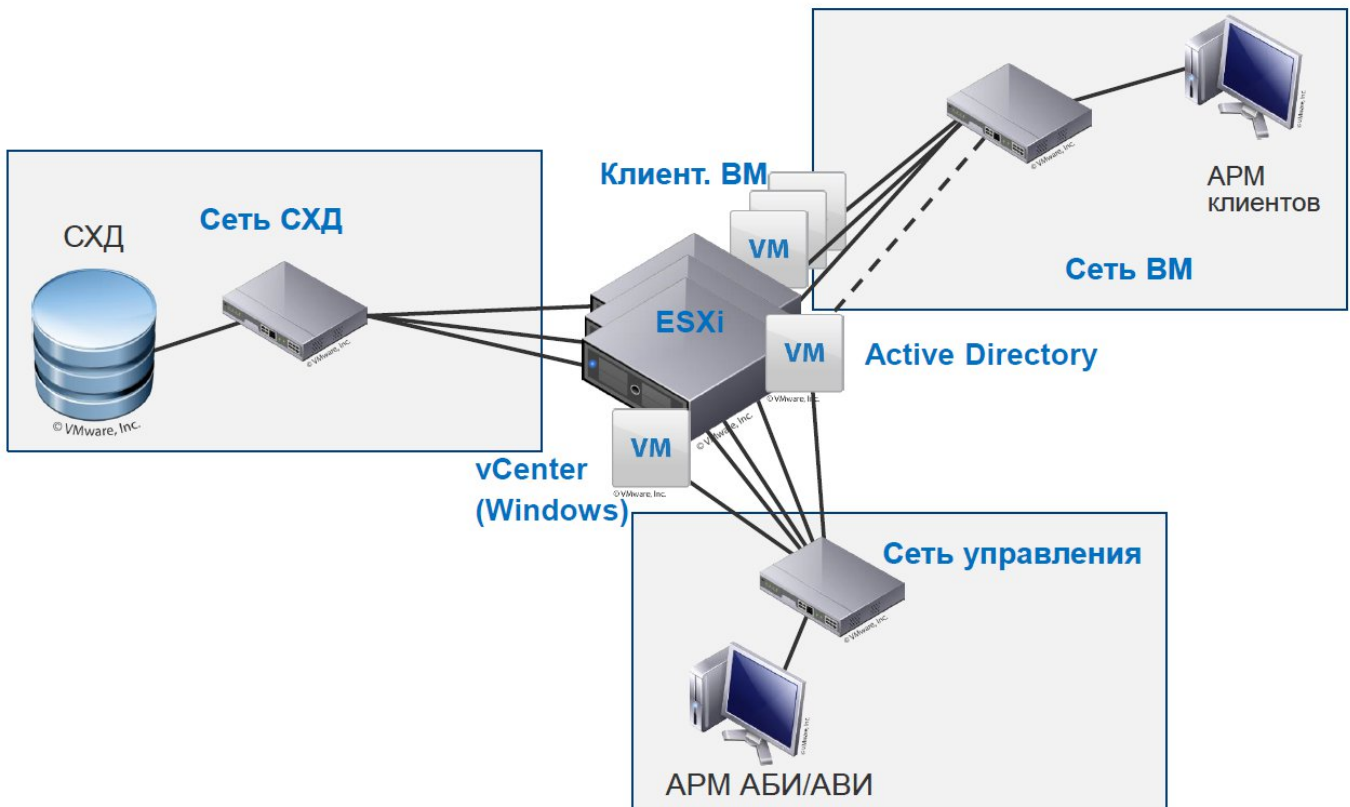


Рисунок 1 - Пример разворачиваемой инфраструктуры

2.4. Особенности установки ESXi

ВНИМАНИЕ! При использовании (в «Аккорд-АМДЗ») контроллеров Аккорд-5.5/5.5.e (не Linux) установка ESXi должна обязательно выполняться с использованием MBR. Это необходимо для корректной работы «Аккорд-АМДЗ». Это **не накладывает** ограничение в размере 2ТБ для новых подключаемых дисков – только на тот, на котором установлен ESXi!

Для того чтобы выполнить установку с MBR при старте инсталлятора ESXi, после появления в правом нижнем углу экрана сообщения о возможности нажать <Shift>+<O>(буква) следует нажать данную комбинацию и через пробел добавить команду «formatwithmbr» (по умолчанию на экране уже имеется команда «runweasel», ее удалять не нужно).

ВНИМАНИЕ! В случае работы с большой инфраструктурой (обычно более 100 VM по 100 файлов) следует выполнить процедуру расширения места под БД агентов на ESXi.

Для этого в vClient следует выбрать нужный хост и: Configuration -> System resource allocation -> Advanced -> Host (System -> Kernel -> kmanaged -> Visorfs -> etc).

Значения *limit* и *reservation* сменить с 28 до 50 Мб.

Выполнять данную процедуру можно "вживую", перезагрузка хоста не требуется. Проверка результата выполняется с помощью команды *vdf -h*.

Корректность установки можно проверить, подключившись к ESXi при помощи vClient и выбрав хост -> configuration -> storage и раздел, в который был установлен ESXi. Примеры ESXi с различными типами разметок представлены на рисунках 2, 3.

Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions

Hardware

- Health Status
- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile
- Host Cache Configuration
- System Resource Allocation
- Agent VM Settings
- Advanced Settings

View: Datastores Devices

Devices

Name	Identifier	Runtime Name	Operational State	LUN	Type
Local VMware, Disk (mpx.vmhba1:...	mpx.vmhba1:C0:...	vmhba1:C0:T0:L0	Mounted	0	disk
Local NECVMWar CD-ROM (mpx.v...	mpx.vmhba32:...	vmhba32:C0:T0:L0	Mounted	0	cdrom

Device Details

Local VMware, Disk (mpx.vmhba1:C0:...

Location: /vmfs/devices/disks/mpx.vmhba1:C0:.. ID: mpx.vmhba1:C0:T0:L0
 Type: disk Capacity: 40,00 GB
 Owner: NMP Partition Format: MBR

Primary Partitions

	Capacity
1. DOS 16-bit <32M	4,00 MB
2. DOS 16-bit >=32M	4,00 GB
3. VMFS	35,12 GB
4. Extended	896,00 MB

Logical Partitions

	Capacity
1. DOS 16-bit >=32M	250,00 MB

Transport

Parallel SCSI

Рисунок 2 - ESXi с MBR-разметкой

okb028-2 VMware ESXi, 5.5.0, 1331820

Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions

Hardware

- Health Status
- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features
- Time Configuration
- DNS and Routing
- Authentication Services
- Virtual Machine Startup/Shutdown
- Virtual Machine Swapfile Location
- Security Profile
- Host Cache Configuration
- System Resource Allocation
- Agent VM Settings
- Advanced Settings

View: Datastores Devices

Devices

Name	Identifier	Runtime Name	Operational State	LUN	Type	Drive Type
HP Serial Attached SCSI Disk (naa...	naa.600508b10...	vmhba2:C0:T0:L1	Mounted	1	disk	Non-SSD
Local HP RAID Ctrlr (mpx.vmhba1:C...	mpx.vmhba1:C0:...	vmhba1:C0:T0:L0	Mounted	0	array control...	Unknown
LIO-ORG ISCSI Disk (naa.60014052...	naa.60014052e...	vmhba32:C0:T0:L0	Mounted	0	disk	Non-SSD

Device Details

HP Serial Attached SCSI Disk (naa.60...

Location: /vmfs/devices/disks/naa.600508b10... ID: naa.600508b1001cc6f255b371d72af26277
 Type: disk Capacity: 1,00 TB
 Owner: NMP Partition Format: GPT

Primary Partitions

	Capacity
1. Legacy MBR	4,00 MB
2. Legacy MBR	250,00 MB
3. Legacy MBR	250,00 MB
4. VMware Diagnostic	110,00 MB
5. Legacy MBR	286,00 MB
6. VMware Diagnostic	2,50 GB

Transport

Block Adapter

Рисунок 3 - ESXi с GPT-разметкой

3. Установка и настройка компонентов СПО «Аккорд-В.»

3.1. Схема развертывания защищенной инфраструктуры виртуализации

На элементы инфраструктуры виртуализации vSphere должны быть установлены следующие компоненты:

1) на **АРМ АБИ**:

- «Аккорд-АМД3»;
- «Аккорд-Win32» / «Аккорд-Win64»;
- ПО управления «Аккорд-В.»;
- ПО ПАК «ПИ ШИПКА» (устанавливается опционально – если в качестве идентификатора используется ПИ ШИПКА);

2) на **сервер vCenter (если он физический)**:

- «Аккорд-АМД3»;
- «Аккорд-Win64 К» (терминальная версия) (если используется не vCenter Service Appliance);
- ПО ПАК «ПИ ШИПКА» (устанавливается опционально – если в качестве идентификатора используется ПИ ШИПКА);

3) на **ESXi-серверы**:

- «Аккорд-АМД3»;
- агенты «Аккорд-В.»;

4) на **виртуальные машины**:

- «Аккорд-Win64 К» (терминальная версия)¹;
- ПО ПАК «ПИ ШИПКА» (устанавливается опционально – если в качестве идентификатора используется ПИ ШИПКА);

5) на **сервер с сервисом регистрации событий (если он выполняется на отдельном АРМ)**:

- «Аккорд-АМД3»;
- «Аккорд-Win32» / «Аккорд-Win64»;
- ПО ПАК «ПИ ШИПКА» (устанавливается опционально – если в качестве идентификатора используется ПИ ШИПКА);

6) на **дополнительные серверы со службами VMware** (например, VMware Consolidated Backup) в зависимости от типа сервера, на который установлена служба:

- в случае использования физического сервера необходима установка «Аккорд-АМД3», а также ПО «Аккорд-Win32»/«Аккорд-Win64» или «Аккорд-Win64 К» (терминальная версия);
- при установке на виртуальную машину – аналогично остальным виртуальным машинам.

¹) в случае использования ВМ с установленными ОС семейства Linux в них устанавливается ПО «Аккорд-Х К», не входящее в состав СПО «Аккорд-В.»

Для наглядности, схема развертывания защищенной инфраструктуры виртуализации представлена на рисунке 4.

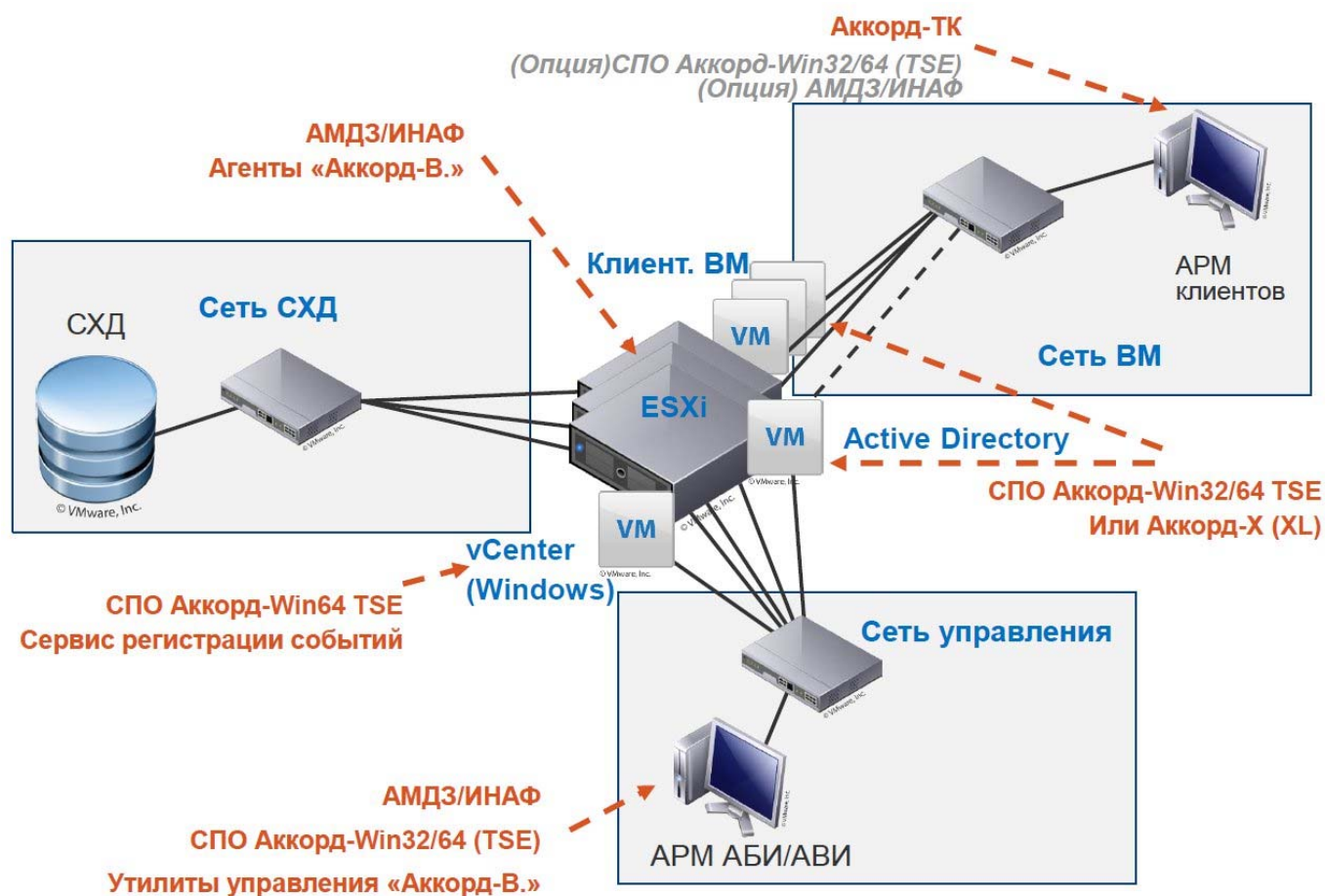


Рисунок 4 - Схема развертывания защищенной инфраструктуры виртуализации

3.2. Порядок установки и настройки СПО «Аккорд-В.»

ВНИМАНИЕ! Предполагается, что система виртуализации уже установлена и соответствующим образом сконфигурирована администратором инфраструктуры виртуализации.

Перед установкой и настройкой «Аккорд-В.» необходимо в комплексе vSphere зарегистрировать две «Read Only» учетные записи: администратора безопасности информации и сервиса регистрации событий (подробнее см. 3.5.2). Администратор БИ организует установку и настройку СПО, осуществляет контроль за правильным использованием ПЭВМ с установленным СПО и периодическое тестирование средств защиты.

Установка и настройка компонентов СПО «Аккорд-В.» осуществляется в соответствии с порядком, указанным в таблице 1.

Таблица 1 – Порядок установки и настройки СПО «Аккорд-В.»

№	Где найти подробное описание	Где выполняется действие				
		АРМ АБИ/АВИ	vCenter (если он физический)	Сервер с сервисом регистрации событий	ВМ	ESXi-серверы
1	п. 3.3	Установка и настройка аппаратной части инфраструктуры				Установка и настройка аппаратной части инфраструктуры
2	п. 3.4	Установка ПО ШИПКА ¹ (опционально)				
3	п. 3.5	Установка СПО разграничения доступа	Установка и настройка СПО разграничения доступа			
4	п. 3.6.2	Установка модулей «Аккорд-В.»				
5	п. 3.6.3	Установка агентов «Аккорд-В.» на ESXi				
6	п. 3.6.4			Установка и настройка сервиса регистрации событий		
7	п. 3.6.5	Предъявление лицензии на ПО управления				
8	п. 3.7.1	Авторизация АБИ				
9	п. 3.7.2	Настройка доверенной загрузки ВМ с vCenter				
10	п. 3.7.3	Настройка доверенной загрузки ВМ				
11	п. 3.8	Настройка разграничения доступа на совмещенном АРМ АБИ/АИБ				
12	п. 4	Создание резервных копий				
13	п. 5	Включение режима ESXi Lockdown Mode				

¹⁾ Выполняется в случае, если при работе с ПО разграничения доступа (подробнее см. 3.5) в качестве идентификаторов используется ШИПКА

3.3. Установка и настройка аппаратной части инфраструктуры

Установку и настройку аппаратной части инфраструктуры – «Аккорд-АМДЗ»² – необходимо выполнить:

- на серверах ESXi;
- на vCenter, если он физический;
- на АРМ АБИ/АИБ (он может совпадать с vCenter).

Процедура установки и настройки «Аккорд-АМДЗ» описана в соответствующей документации на «Аккорд-АМДЗ» («Руководство по установке» (11443195.4012-038 98), «Руководство администратора» (11443195.4012-038 90)). Ниже приведены только особенности настройки «Аккорд-АМДЗ» на ESXi-серверах.

После установки «Аккорд-АМДЗ» следует выполнить процедуру настройки параметров учетной записи АБИ (пользователь «Главный администратор» в группе «Администраторы») и, если необходимо, пользователей (группа «Обычные»).

В процессе настройки «Аккорд-АМДЗ» следует установить на контроль и рассчитать контрольные суммы (КС) для следующих элементов (минимальное количество файлов, которые необходимо установить на контроль, выделено жирным шрифтом):

1) **содержимое каталога bootloader (в списке разделов «Аккорд-АМДЗ» каталог bootloader отобразится разделом с файлами ldlinux.sys, syslinux.cfg; данный раздел недоступен самому ESXi);**

2) **содержимое каталога bootbank (и altbootbank, если он не пуст), в частности:**

- **imgdb.tgz – содержит описание всех используемых драйверов и их зависимостей;**
- файлы с расширениями v00/v01/v02 – драйверы;
- **boot.cfg – конфигурационный файл загрузчика, содержащий указание на ядро и модули;**
- **tboot.b00 – ядро гипервизора;**
- остальные файлы, расширение которых начинается на .b (модули гипервизора).

3) не относящиеся к специфике ESXi элементы:

- MBR;
- оборудование СБТ.

Примечание: файл state.tgz содержит настройки ESXi и постоянно обновляется, поэтому его не рекомендуется устанавливать на контроль (т.к. каждый раз придется пересчитывать его КС).

² В случае отсутствия на материнской плате ПЭВМ (для всех ESXi и для vCenter, если он физический) свободного слота PCI/PCI-X/PCI-Express вместо «Аккорд-АМДЗ» можно использовать СЗИ НСД «Инаф», подключаемый в свободный USB-порт ПЭВМ

Дополнительно рекомендуется устанавливать на контроль файлы с расширением .iso (vmwaretools) с раздела store (данная процедура не является обязательной, поскольку ESXi контролирует их самостоятельно).

ВНИМАНИЕ! В «Аккорд-АМД3» разделы могут отображаться дважды – достаточно установить на контроль только один экземпляр каждого раздела.

3.4. Установка и настройка ПО ПАК «ПИ ШИПКА» на физических АРМ (vCenter / АРМ АБИ) и ВМ

Если при работе с ПО разграничения доступа (подробнее см. 3.5) в качестве идентификаторов используется ПИ ШИПКА³, следующим этапом следует выполнить процедуру установки ПО ПАК «ПИ ШИПКА» на физические АРМ (vCenter / АРМ АБИ) и виртуальные машины, а также инициализацию и форматирование устройства ШИПКА.

Процедура установки и настройки ПО ПАК «ПИ ШИПКА» описана в соответствующей документации, входящей в комплект поставки ПАК «ПИ ШИПКА».

3.5. Установка и настройка ПО разграничения доступа на физических АРМ (vCenter / АРМ АБИ) и ВМ

3.5.1. Общие сведения

Процедура установки и настройки ПО разграничения доступа «Аккорд-Win64 К» (терминальная версия) / «Аккорд-Х К» описана в соответствующей документации.

ВНИМАНИЕ! Использование ПО разграничения доступа внутри ВМ потребует примерно 5 - 7% от производительности ВМ. Поэтому при расчете параметров ВМ следует учесть этот запас и добавить 10% по производительности к тому, что было рассчитано другими методиками.

ВНИМАНИЕ! СПО разграничения доступа **настраивается на АРМ АБИ/АИВ последним этапом** в связи с тем, что соответствующее ПО, к которому будет производиться разграничение доступа, появится только на следующем этапе.

3.5.2. Разделение ролей администраторов, создание и настройка их учетных записей на vCenter

В инфраструктуре виртуализации (в данном случае не рассматривается вариант без vCenter и Active Directory) необходимо выделить две роли: администратор безопасности информации (АБИ) и администратор инфраструктуры виртуализации (АИВ) (подробнее см. «Принятые термины, обозначения и сокращения»).

³) ПИ ШИПКА не входит в комплект поставки «Аккорд-В.» и приобретается по дополнительному заказу

Для этого на АРМ управления комплексом vSphere в Active Directory следует завести учетные записи АБИ и АИВ. Дополнительно следует завести также учетную запись для сервиса регистрации событий.

Для учетной записи сервиса регистрации событий рекомендуется отключить возможность локального входа в систему (параметры групповой политики в Active Directory).

АБИ должен быть администратором в СПО разграничения доступа и пользователем в Windows. И наоборот, АИВ должен быть пользователем в СПО разграничения доступа и администратором в Windows. В этом случае администратор безопасности имеет возможность управлять распределением прав доступа (механизмами СПО разграничения доступа), но не имеет доступа к самим ресурсам (в силу соответствующих настроек Windows).

Для АБИ и сервиса регистрации событий следует назначить «Read Only» права на vCenter (корневому элементу) с галочкой propagate, отвечающей за наследование (рисунок 5).

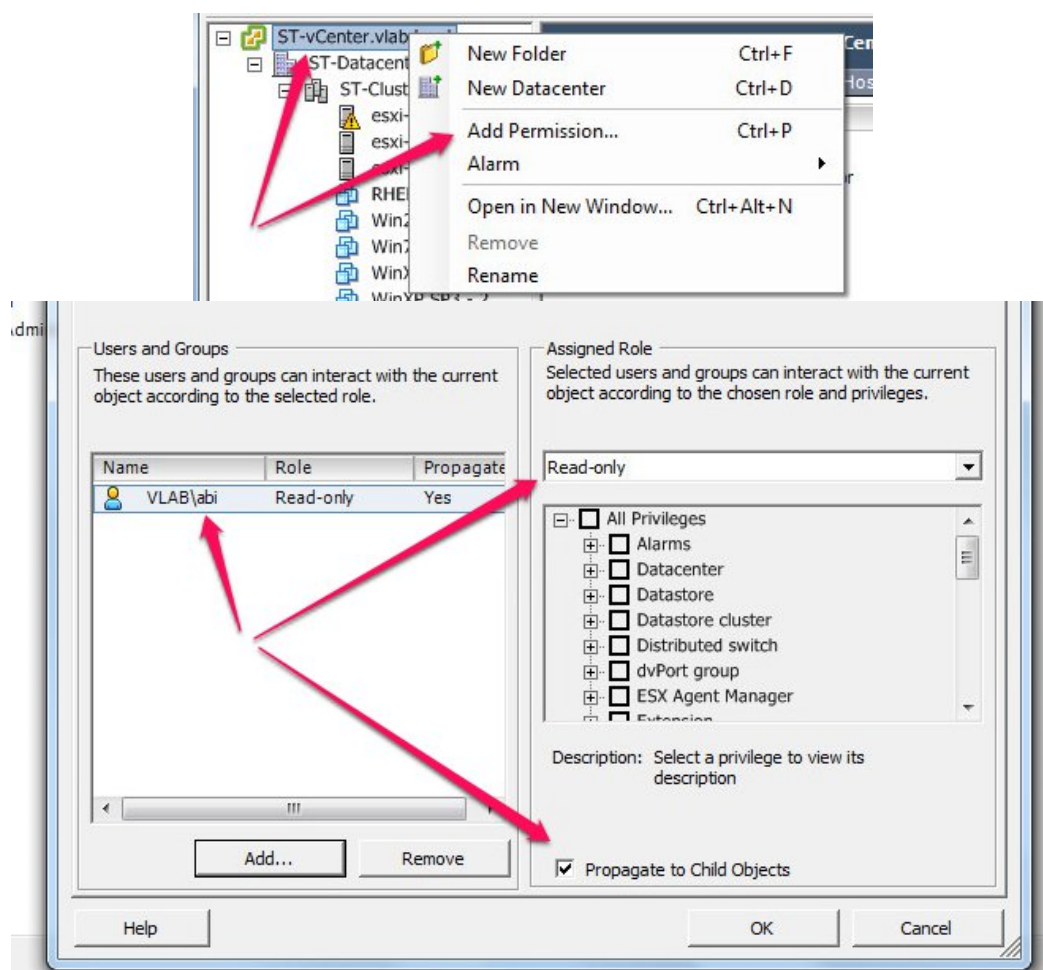


Рисунок 5 – Настройка учетных записей на vCenter

Учетная запись АБИ должна иметь полный доступ к папке с установленным ПО «Аккорд-В.»:

«C:\Program Files (x86)\OKB SAPR\Accord-V»

– данный пункт настраивается средствами ОС. Дополнительно необходимо с помощью СПО разграничения доступа «Аккорд-Win64 К» (терминальная версия) оставить эту папку доступной только для АБИ.

Назначаемая роль АИВ на vCenter зависит от должностных обязанностей (примером такой роли может служить роль Virtual Machine user (sample), которая дает права на взаимодействие с уже существующими ВМ; подробнее см. саму роль на vCenter).

3.6. Установка и настройка модулей СПО «Аккорд-В.»

3.6.1. Начало процедуры установки

ВНИМАНИЕ! Предполагается, что система виртуализации уже установлена и соответствующим образом сконфигурирована администратором инфраструктуры виртуализации .

ВНИМАНИЕ! Перед началом установки убедитесь, что:

- СПО разграничения доступа и ПО для ПИ ШИПКА уже установлено и соответствующим образом сконфигурировано;
- АРМ АБИ, на которое будет устанавливаться ПО управления, имеет связь по сети с ESXi и vCenter;
- время на всех ESXi-серверах и сервере vCenter синхронизировано (вручную или через ntp-сервер), и часовые пояса заданы корректно.
- в ОС АРМ АБИ открыты порты 51178 и 51179;
- в ОС с сервисом регистрации событий открыт порт 51179.

ВНИМАНИЕ! ПО «Аккорд-В.» использует для соединения протокол SSL, поэтому если время рассинхронизировано, компоненты ПО не смогут установить соединение между собой!

Примечание: На ESXi время отображается в формате UTC, но если через vClient открыть закладку времени (Configuration -> TimeConfiguration), то в нем будет отображаться время с пересчетом относительно локального времени на элементе инфраструктуры, на котором запущен vClient.

Чтобы начать установку системы управления, необходимо запустить с правами администратора исполняемый файл **Accord-V.exe**, который находится на диске с дистрибутивом, и дать согласие на внесение программой изменений в компьютере. Начнется процесс установки ПО.

В появившихся в процессе установки окнах установки распространяемого пакета Microsoft Visual C++ 2010 (x86)⁴ следует ознакомиться с лицензионным соглашением, принять его посредством установки галочки в соответствующем

⁴ Распространяемые пакеты (Redistributable Package) Microsoft Visual C++ 2008 (x86) и Microsoft Visual C++ 2010 (x86) включены в комплект поставляемого ПО «Аккорд-В.»

поле, нажать кнопку <Install> (рисунок 6), дождаться окончания процесса установки пакета и нажать кнопку <Finish>.

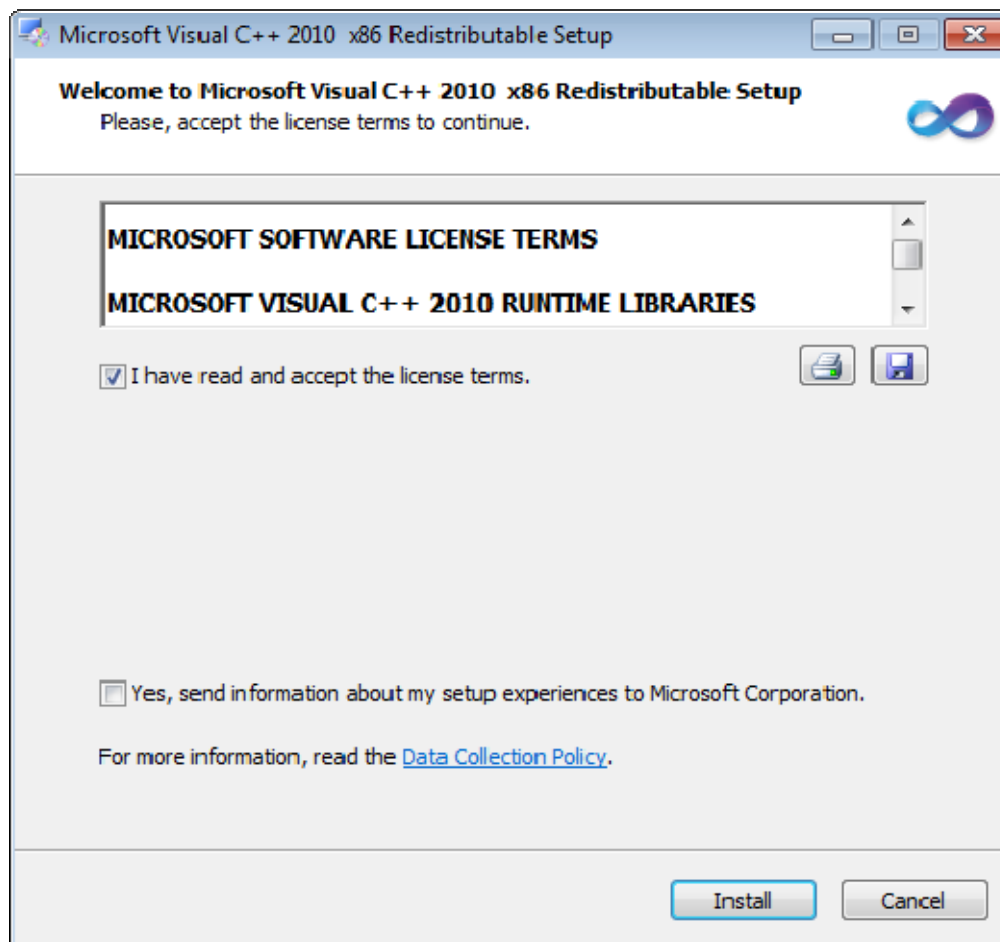


Рисунок 6 - Установка распространяемых пакетов Windows

Далее следует перейти к процедуре установки модулей «Аккорд-В.».

3.6.2. Установка модулей «Аккорд-В.»

В появившемся далее окне установки модулей «Аккорд-В.» необходимо указать путь к каталогу установки. По умолчанию установка всех программных компонентов выполняется в каталог **C:\Program Files (x86)\OKB SAPR\Accord-V**. Каталог, предлагаемый по умолчанию, может быть изменен посредством ручного редактирования или задан с помощью стандартного диалога ОС Windows, вызываемого при нажатии кнопки <Обзор...>. Если указанный каталог не существует, он будет создан программой установки автоматически. После выбора каталога установки следует ознакомиться с лицензионным соглашением, принять его посредством установки галочки в соответствующем поле и нажать кнопку <Далее> (рисунок 7).

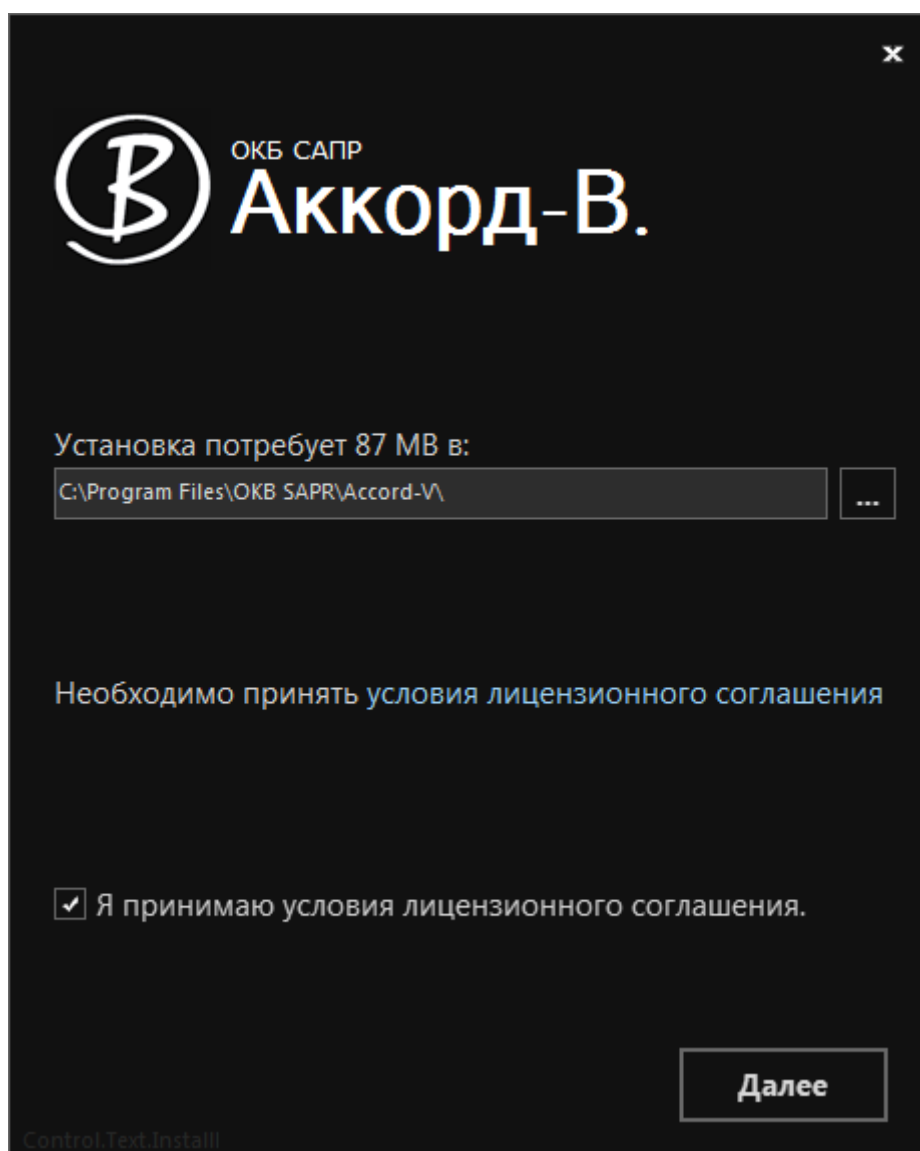


Рисунок 7 - Выбор пути установки

Далее необходимо выбрать компоненты устанавливаемого ПО и нажать кнопку <Установить> (рисунок 8).

Если выбран рекомендуемый вариант расположения сервиса регистрации событий (на отдельном АРМ), на данном этапе следует выполнить установку ПО без сервиса регистрации событий (данная процедура будет выполнена позже – см. 3.6.4).

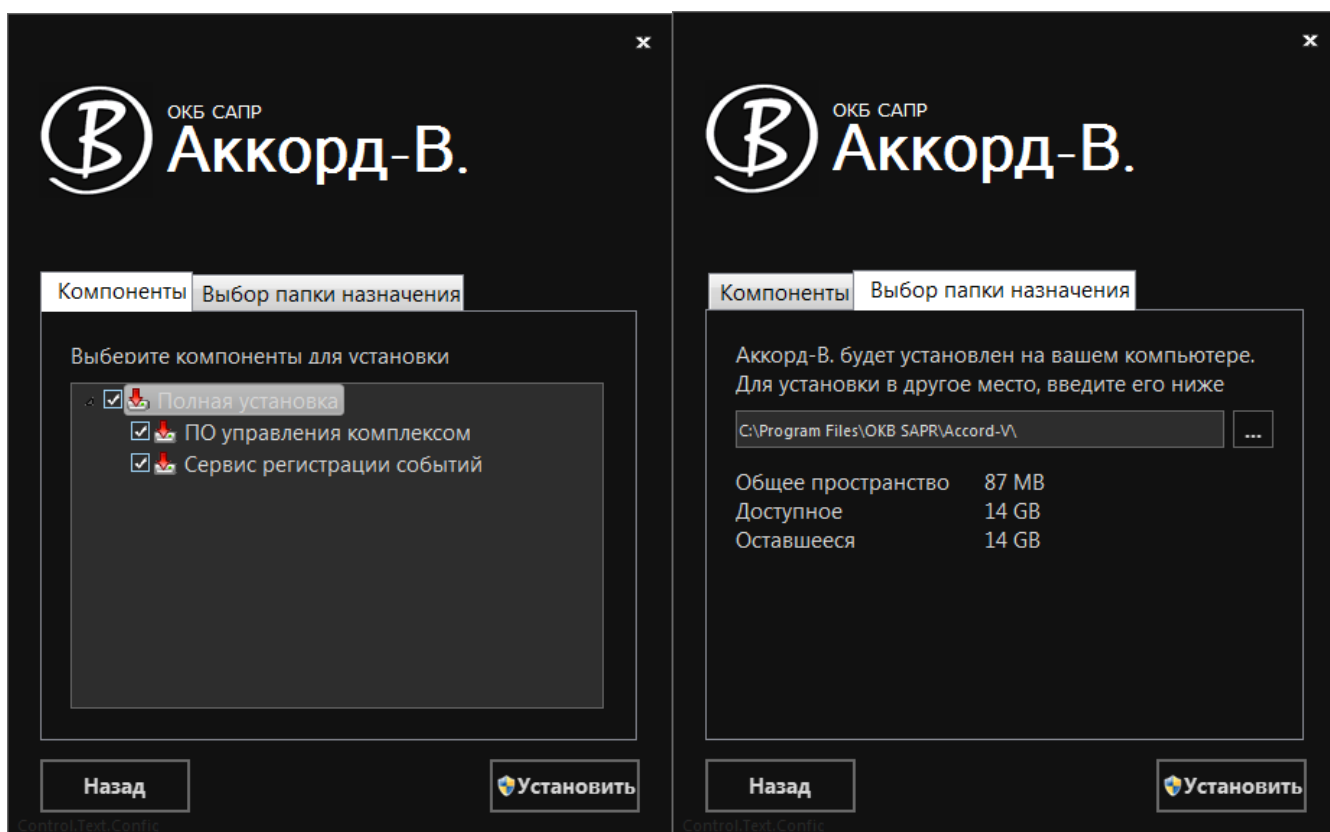


Рисунок 8 - Выбор компонентов установки

Начнется установка ПО, в процессе которой на рабочем столе ОС создаются ярлыки:

- «Installer-V.» – утилита для установки агентов «Аккорд-В.» на ESXi;
- «Accord-V.» – утилита управления «Аккорд-В.»;
- «LogViewer-V.» – утилита просмотра зарегистрированных событий.

По окончании процесса установки на экран выводится окно с соответствующим сообщением, в котором следует нажать кнопку «Готово».

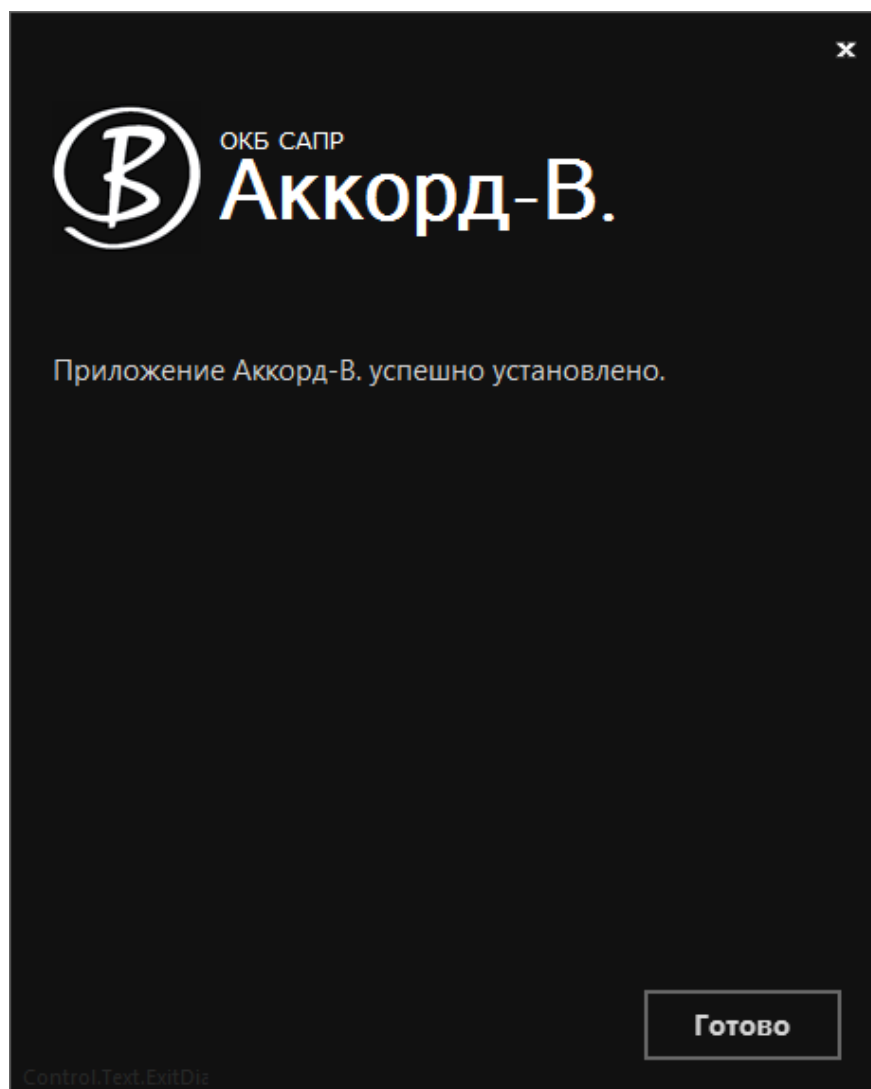


Рисунок 9 - Окончание процесса установки ПО «Аккорд-В.»

После установки необходимо настроить права доступа администраторам безопасности, учитывая следующее:

а) пользователь, запускающий «LogViewer-V.», должен иметь права на запись в файл LogConfig.xml и чтение/исполнение файлов в папке с установленным ПО «Аккорд-В.» (Accord-V). В данном случае указаны минимально требуемые права – данному пользователю можно также предоставлять права на всю папку Accord-V целиком;

б) для входа в утилиту «Accord-V.» должна использоваться учетная запись АБИ, имеющая полный доступ к инфраструктуре в режиме только для чтения (для vCenter в разделе настроек «Permissions» следует установить тип доступа «Read only» с флагом «Propagate»);

ВНИМАНИЕ! Если по каким-либо причинам в vSphere для учетной записи АБИ (в утилите «Accord-V.») назначается не вся видимость инфраструктуры, для корректной работы необходимо назначать права «Read Only»:

- на хосты, ВМ, хранилища с этими ВМ;
- на кластер (с наследованием прав) и на хранилища с ВМ.

в) пользователь, запускающий «Accord-V.», должен иметь полный доступ к папке Accord-V;

г) запуск утилиты установки сервиса (LogServiceInstall) требует административных прав;

д) пользователь, запускающий «Installer-V.», должен иметь права на запись в файл Config.xml, а также на чтение/исполнение файлов в каталоге с установленным ПО «Аккорд-В.» и в каталоге, в который будут сохраняться резервные копии (подробнее см. раздел 4). В данном случае указаны минимально требуемые права – данному пользователю можно также предоставлять права на всю папку Accord-V целиком.

3.6.3. Установка агентов «Аккорд-В.» на ESXi

Установка агентов «Аккорд-В.» на ESXi производится централизованно с АРМ АБИ.

Для выполнения процедуры установки агентов «Аккорд-В.» на ESXi необходимо запустить утилиту **Installer-V.exe** (ярлык на рабочем столе АРМ АБИ, созданный в процессе установки модулей «Аккорд-В.»).

ВНИМАНИЕ! АБИ, выполняющий установку агентов «Аккорд-В.», должен обладать достаточными правами на запись в папку с установленным ПО «Аккорд-В.» (см. 3.6.2).

Последовательность установки агентов зависит от используемой инфраструктуры.

1. Если в инфраструктуре используется vCenter, то в появившемся далее окне следует добавить vCenter, нажав на кнопку <Добавить сервер> (рисунок 10).

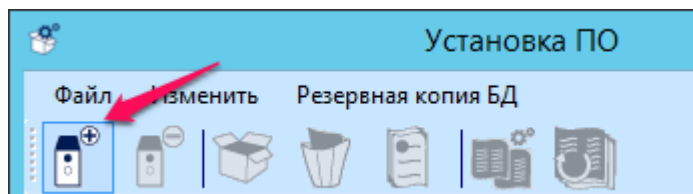
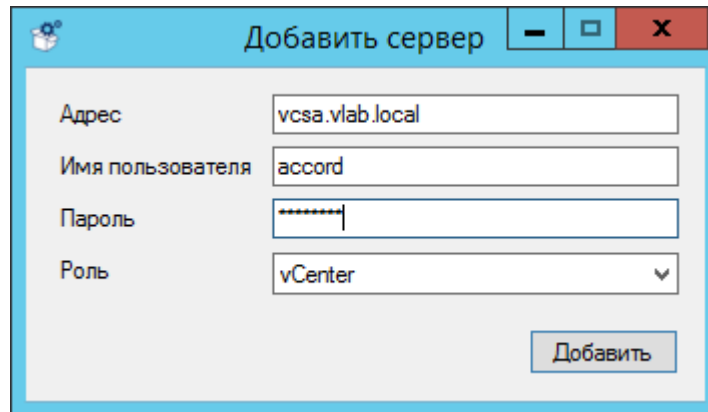


Рисунок 10 - Добавление vCenter

В появившемся далее окне (рисунок 11) следует ввести адрес добавляемого vCenter (IP-адрес или FQDN vCenter), а также имя и пароль для учетной записи АБИ (поля «Имя пользователя» и «Пароль»), в качестве роли сервера указать «**vCenter**» и нажать кнопку <Добавить>.



Добавить сервер

Адрес: vcsa.vlab.local

Имя пользователя: accord

Пароль:

Роль: vCenter

Добавить

Рисунок 11 - Ввод параметров добавляемого vCenter

По завершении процедуры добавления vCenter на экран выводится соответствующее сообщение (рисунок 12).

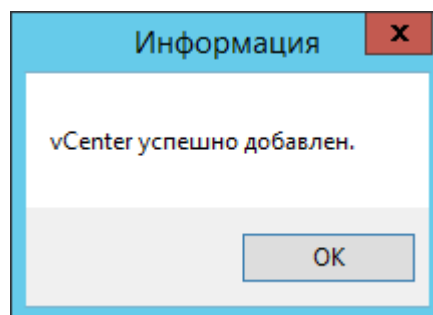


Рисунок 12 - Сообщение об успешном завершении процедуры добавления vCenter

При этом в главном окне программы появляется список ESXi, связанных с данным vCenter (рисунок 13).

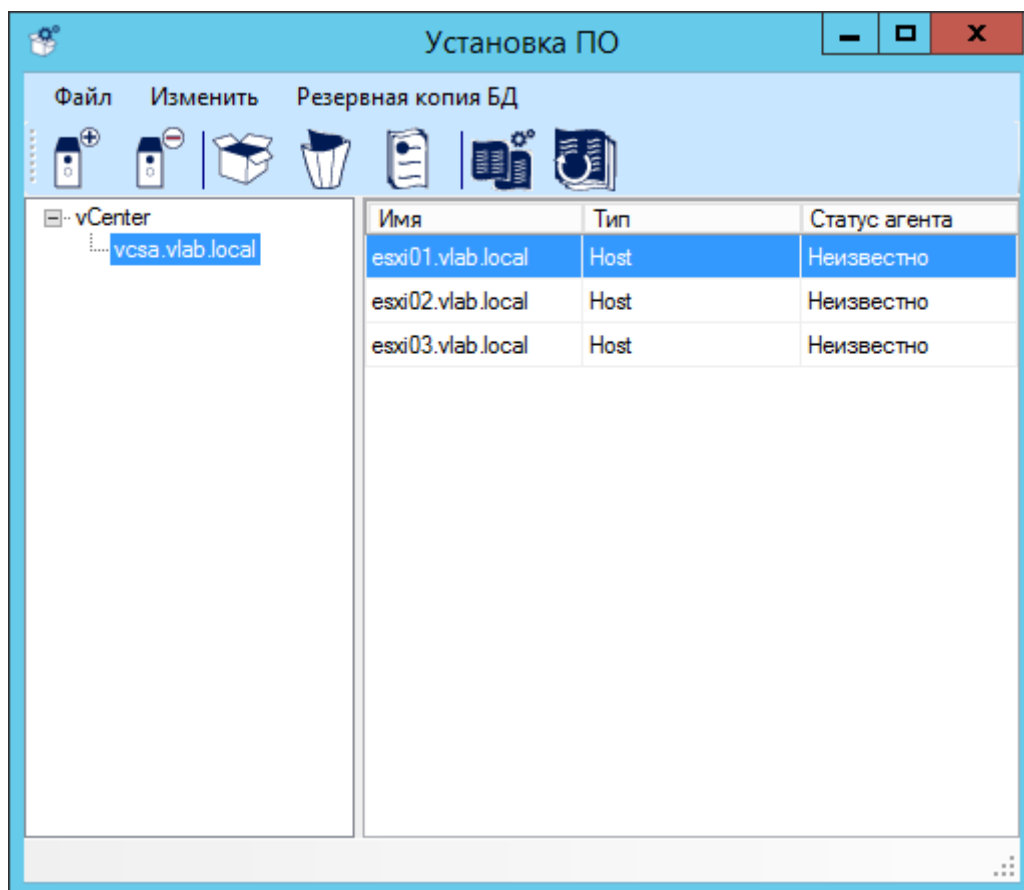


Рисунок 13 - Список ESXi, связанных с добавленным vCenter

2. Если используются отдельные ESXi (без vCenter), то в окне установки ПО необходимо нажать кнопку <Добавить сервер>, выбрать роль «ESXi» и ввести соответствующий IP-адрес (рисунок 14).

Добавить сервер

Адрес:

Имя пользователя:

Пароль:

Роль:

Добавить

Рисунок 14 - Кнопка <Добавить ESXi>

После добавления ESXi одним из указанных выше способов следует перейти к непосредственной процедуре установки агентов «Аккорд-В.» на ESXi.

Для этого в окне установки ПО следует выделить в списке нужный хост и нажать кнопку <Установить агент> (рисунок 15).

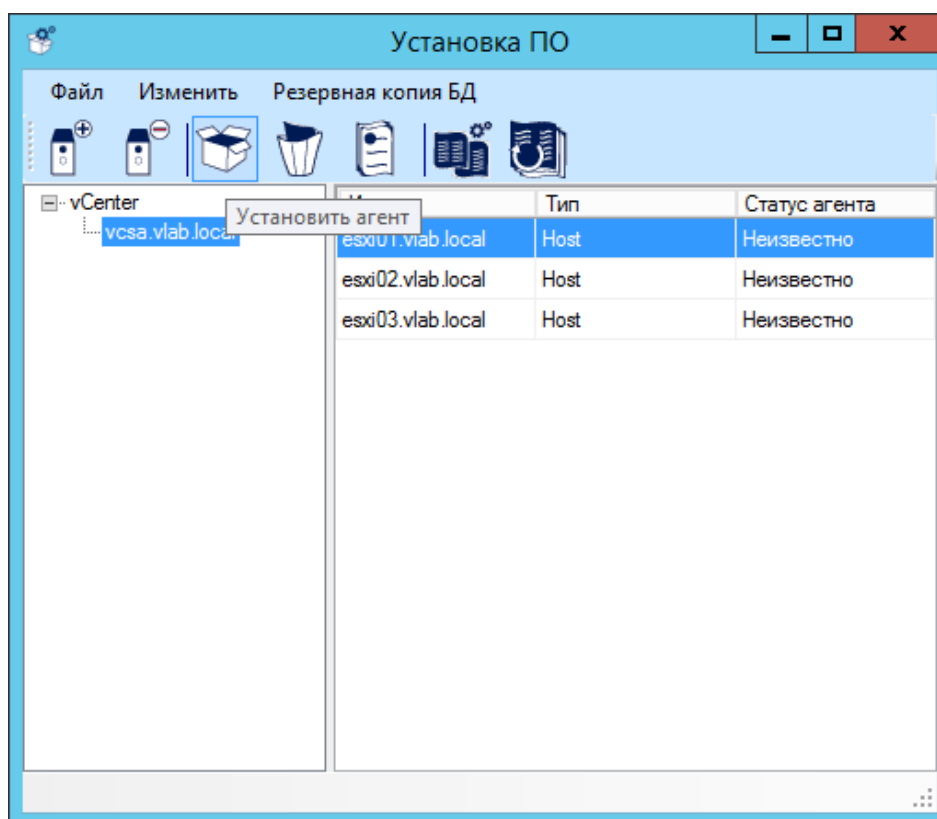


Рисунок 15 - Кнопка <Установить агент>

В появившемся далее окне (рисунок 16) необходимо ввести имя учетной записи на ESXi (root) и ее пароль для соответствующего хоста.

Для упрощения работы, в случае если на нескольких ESXi учетные записи root имеют одинаковые пароли, существует возможность выделить сразу несколько ESXi и в появившемся далее окне один раз ввести пароль учетной записи root, общий для всех выбранных ESXi.

ВНИМАНИЕ! Для всех выбранных хостов пароль от учетной записи root запрашивается **только один раз!** Таким образом, если пароли на хостах различны, следует выполнять установку на каждом ESXi отдельно, последовательно выделяя в списке нужный хост и нажимая кнопку <Установить агент>.

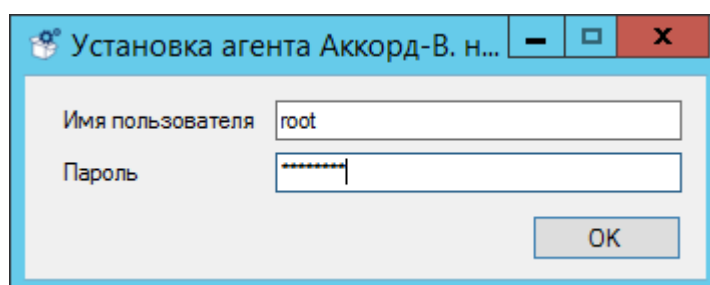


Рисунок 16 - Окно ввода параметров учетной записи root на ESXi

При нажатии кнопки <OK> в окне ввода пароля учетной записи root выполняется установка агентов «Аккорд-В.» на ESXi, в результате которой на экран выводится соответствующее сообщение (рисунок 17).

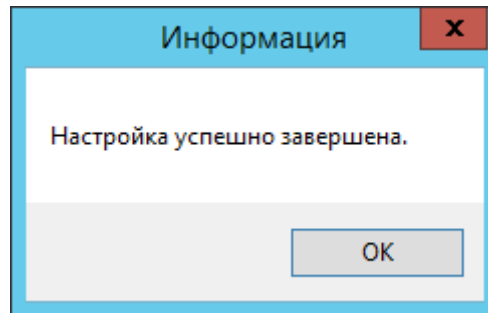


Рисунок 17 - Сообщение об успешном выполнении процедуры установки агентов «Аккорд-В.»

При этом статус для соответствующего хоста в окне установки ПО сменяется на «Установлен» (рисунок 18).

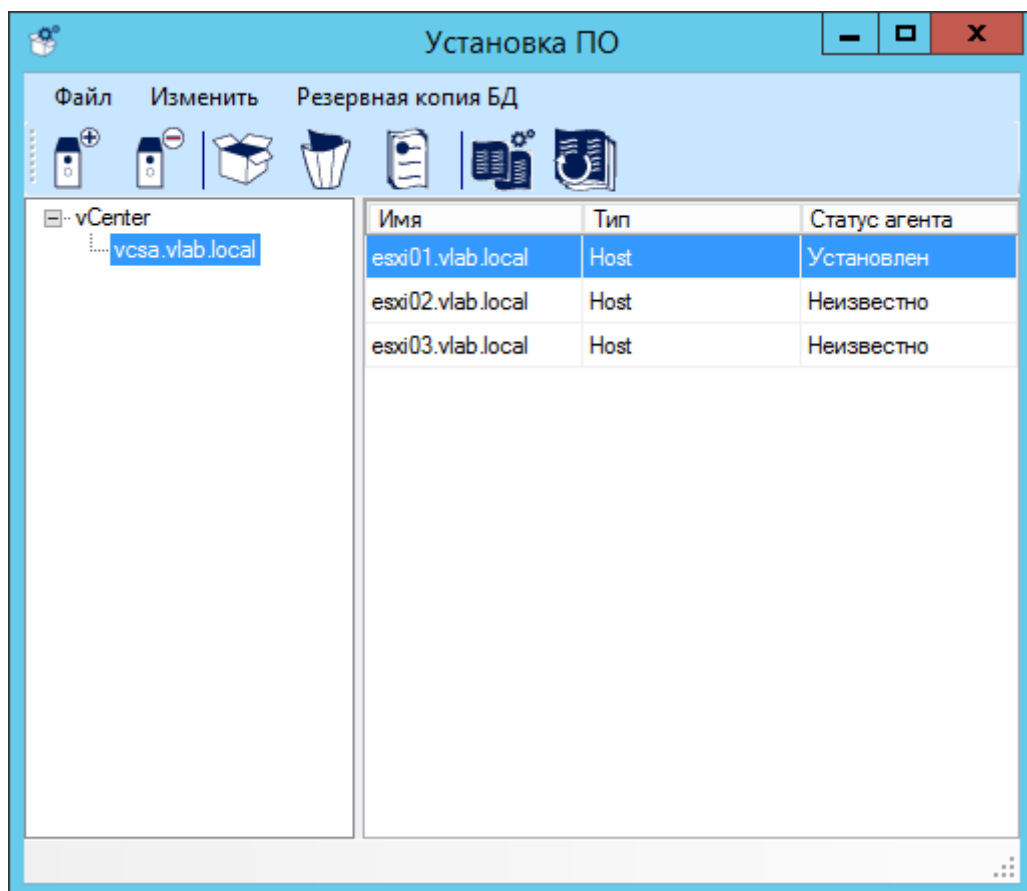


Рисунок 18 - Изменение статуса в окне установки ПО

ВНИМАНИЕ! Во время установки или удаления агента на ESXi работает SSH-сервис. Если перед установкой или удалением агента SSH-сервис на ESXi был отключен, по завершении этих действий может появиться окно ошибки, связанной с потерей соединения с сервером (рисунок 19). Следует нажать кнопку <Да>, после чего утилита выполнит попытку повторного подключения к ESXi и отключит SSH-сервис. В противном случае работа утилиты продолжится без повторного подключения к серверу, и SSH-сервис на ESXi останется запущенным.

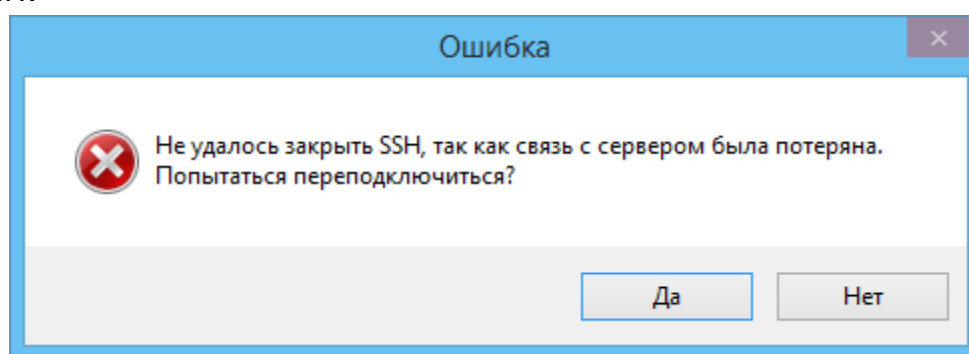


Рисунок 19 - Ошибка, связанная с потерей соединения с сервером

ВНИМАНИЕ! Действия, связанные с установкой или удалением агентов на ESXi, следует выполнять только с помощью утилиты «Installer-V.».

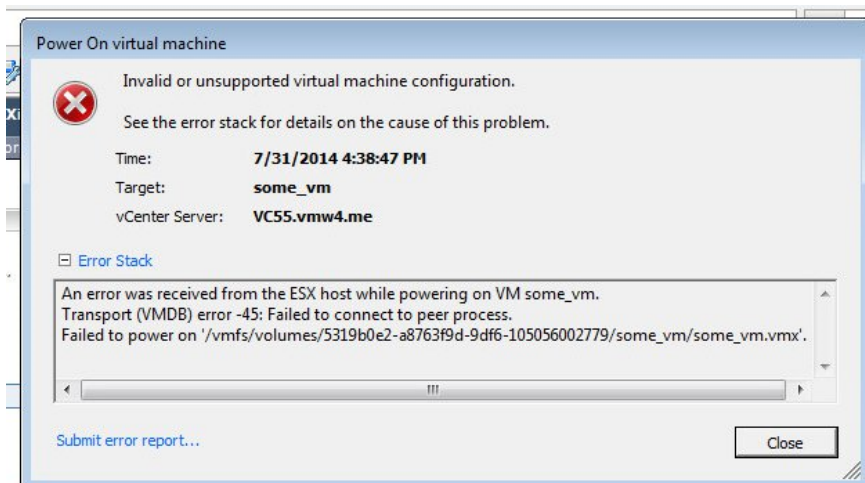
Следует учитывать, что статус установки агентов обновляется в окне утилиты «Installer-V.» только по факту установки или удаления агентов **с помощью данной утилиты**. Если агенты были удалены способом, отличным от указанного, статус их установки в утилите не изменится.

ВАЖНО! После установки агентов на ESXi включение ВМ на них будет заблокировано! При включении будут показываться следующие сообщения:

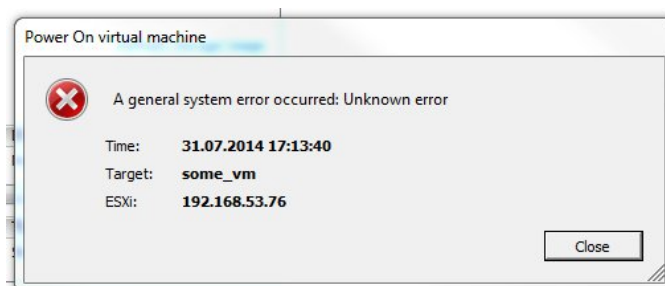
для vSphere 6.5:

 Failed to power on virtual machine some_vm. Transport (VMDB) error -45: Failed to connect to peer process. Click here for more details. - dismiss 

для vSphere 5.5, vSphere 6.0:



для vSphere 5.0 и 5.1:



После установки ПО «Аккорд-В.» на межсетевом экране ESXi (firewall) автоматически откроются два порта (подробнее см. подраздел «Security Profile» вкладки «Configuration» для соответствующего хоста):

- порт 51178, предназначенный для взаимодействия с ПО управления доверенной загрузкой ВМ (сервис «accordservice»);
- порт 51179, предназначенный для взаимодействия с сервисом регистрации событий (сервис «accordlog»).

Также порт 51179 необходимо открыть вручную в брандмауэре Windows там, где установлен сервис регистрации событий (см. 3.6.4), а также на других промежуточных межсетевых экранах между серверами.

ВНИМАНИЕ! Если агенты «Аккорд-В.» в дальнейшем будут установлены на новые хосты, необходимо перезапустить сервис регистрации событий и утилиту «Accord-V.».

Если APM АБИ и АИВ являются различными СБТ, рекомендуется настроить firewall на ESXi так, чтобы подключения к сервисам «Аккорд-В.» могли

выполняться только с АРМ АБИ. Пример подобной настройки показан на рисунке 20.

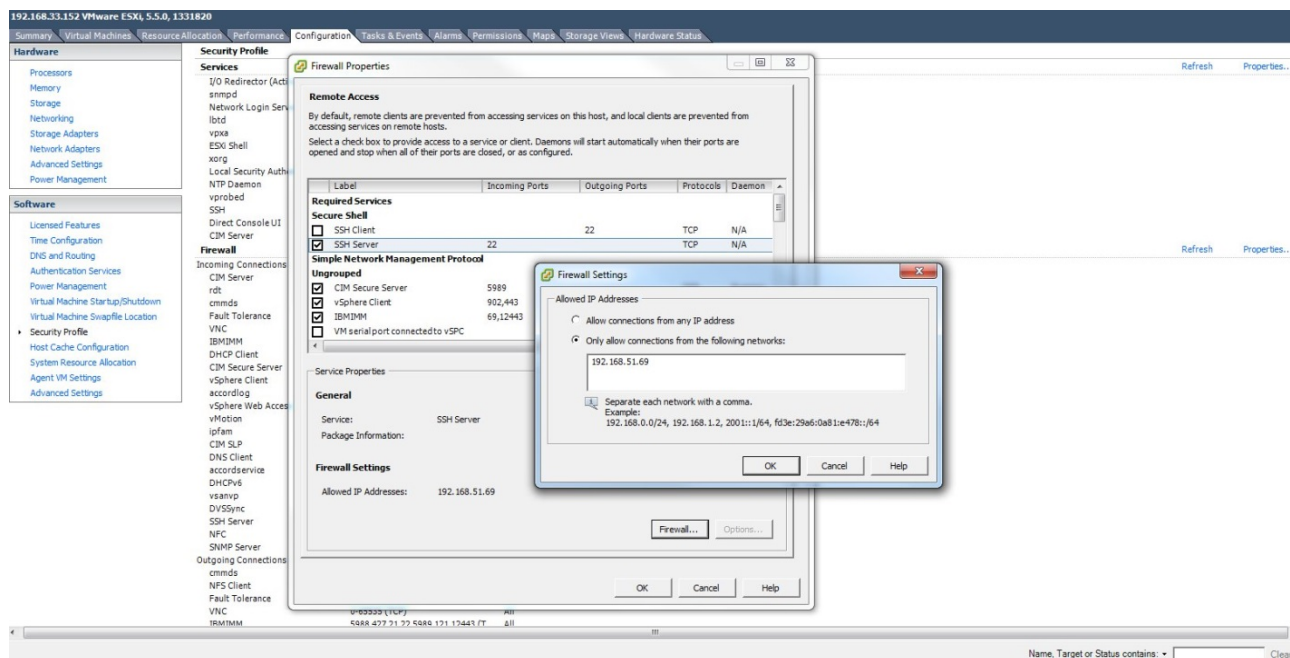


Рисунок 20 – Пример настройки firewall на ESXi

Следующим этапом необходимо выполнить установку сервиса регистрации событий.

3.6.4. Установка и настройка сервиса регистрации событий

3.6.4.1. Установка сервиса регистрации событий

Перед установкой сервиса регистрации событий необходимо создать для него отдельную учетную запись, назначить ей права «Read Only» в инфраструктуре VMware vSphere (см. 3.5.2), отключить для нее локальный вход в ОС (средствами домена) и назначить ей полный доступ к папке с установленным ПО «Аккорд-В.» (к папке Accord-V).

ВНИМАНИЕ! Если сервис регистрации событий устанавливается отдельно, то необходимо предварительно скопировать папку **«certs»** (убедившись при этом, что в ней уже содержатся сертификаты openssl.cfg, host_cert, host_key, cacert) и файл конфигурации **Config.xml** с АРМ АБИ, на котором установлено ПО управления, в корень папки с сервисом регистрации событий (взамен аналогичных, появившихся в папке после установки сервиса)!

Файл конфигурации содержит список хостов и vCenter, с которых будут собираться события. Если их количество увеличилось, или изменились их IP-адреса или имена, необходимо обновить данный конфигурационный файл (вручную или скопировав повторно с АРМ АБИ) и перезапустить сервис!

Примечание: агент «Аккорд-В.» записывает все события в /var/log/accordguard, а также дублирует их в syslog, если необходимо собирать события при помощи SIEM. Сервис регистрации событий постоянно забирает события с /var/log/accordguard (при этом удаляя их оттуда, но оставляя в syslog) и с vCenter.

Установка сервиса регистрации событий осуществляется при помощи утилиты **LogServiceInstall.exe** (расположена в папке с установленным ПО «Аккорд-В.», по умолчанию:

C:\Program Files(x86)\OKB SAPR\Accord-V\LogServiceInstall.exe).

Созданному ранее пользователю, от имени которого будет работать сервис регистрации событий (сервисная учетная запись – см. п. 3.5.2), необходимо назначить полные права на папку с установленным ПО. Подробнее о правах этого пользователя см. в пункте 3.6.4.2 настоящего Руководства.

После этого следует запустить утилиту **LogServiceInstall.exe** с правами администратора и начать установку сервиса регистрации событий, настроив при этом следующие параметры (рисунок 22):

- поля «*Пользователь*» и «*Пароль*» – параметры учетной записи, от имени которой будет работать сервис регистрации событий;
- поле «*IP адрес*» – содержит значение IP-адреса, который будет использовать сервис (в дальнейшем в утилите просмотра журнала событий «**LogViewer-V.**» необходимо будет указывать именно этот адрес). Данный пункт реализован в виде выпадающего списка, в котором отображаются IP-адреса всех доступных сетевых интерфейсов;
- поле «*Режим*» – выбор способа авторизации сервиса. По умолчанию предлагается использовать режим *SSPI* – в этом случае учетные данные пользователя, от имени которого работает сервис, используются только один раз, в процессе настройки. **При этом требуется, чтобы учетная запись существовала на APM, с которого выполняется авторизация, и была доступна vCenter. Для нее должны быть назначены права «Read Only» в инфраструктуре VMware vSphere, отключен локальный вход в ОС (средствами домена) и даны права на запись в файл EventDatabase.db, а также на чтение и создание файлов в папке Accord-V.**

В некоторых случаях целесообразно вместо режима *SSPI* использовать режим *CredentialStore* (например, в случае работы с *VCSA*, когда не работает авторизация при помощи *vClient* с использованием опции *use windows session credentials*). Данный режим позволяет использовать *APM*, не состоящее в домене (и при этом использовать для авторизации доменную учетную запись). В таком случае сервис запускается от имени локальной службы. Поэтому перед установкой в данном режиме необходимо предоставить полные права на папку с установленным ПО («Аккорд-В.») пользователю «LOCAL SERVICE» (рисунок 21).

ВНИМАНИЕ! При выборе режима *CredentialStore* запрещается использовать учетные записи *vSphere*, имеющие права, отличные от «Read only». Предполагается также, что доступ к папке с установленным ПО разграничивается средствами ОС или наложенными средствами разграничения доступа (СПО «Аккорд-Win64 К»).

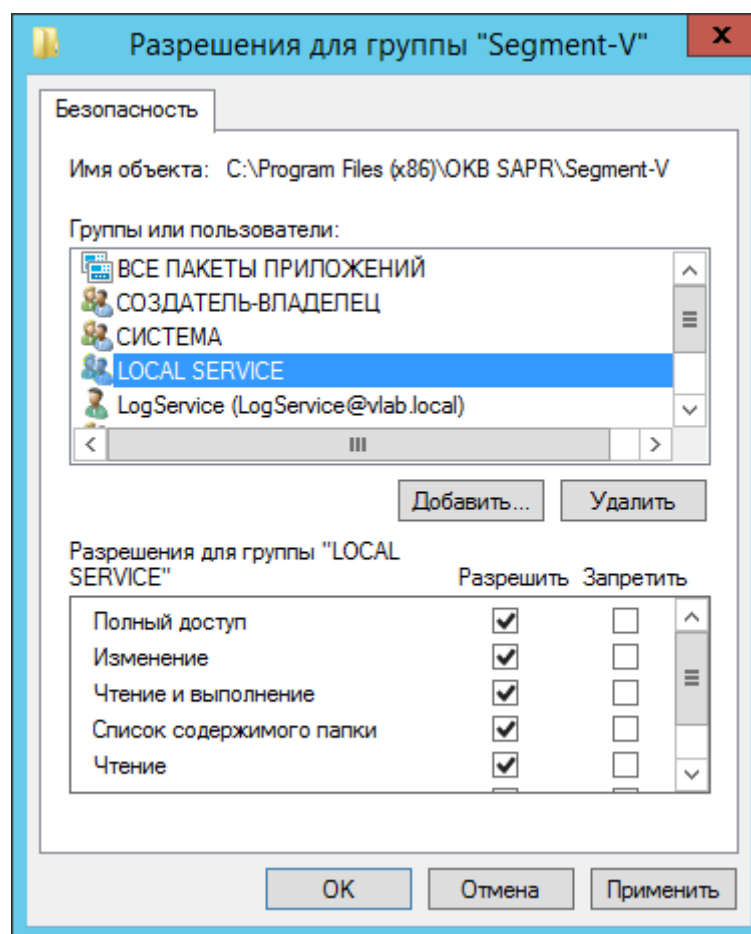


Рисунок 21 - Назначение прав сервисной учетной записи на папку с установленным ПО

- поле «Статус» – содержит сведения о текущем состоянии сервиса регистрации событий. Для данного поля доступны состояния «Не установлен», «Устанавливается», «Установлен». Если при попытке установки утилита не обнаружит необходимых элементов (файл конфигурации, сертификаты, база данных), будет выдано соответствующее предупреждение;
- галочка «Сервис на одном сервере с vCenter». Данную опцию необходимо активировать, если сервис регистрации событий установлен на одном сервере с vCenter. В этом случае для данного сервиса будет добавлена соответствующая зависимость по запуску: сначала запускается сервис «vpxd» (т.е. vCenter), затем – сервис регистрации событий.

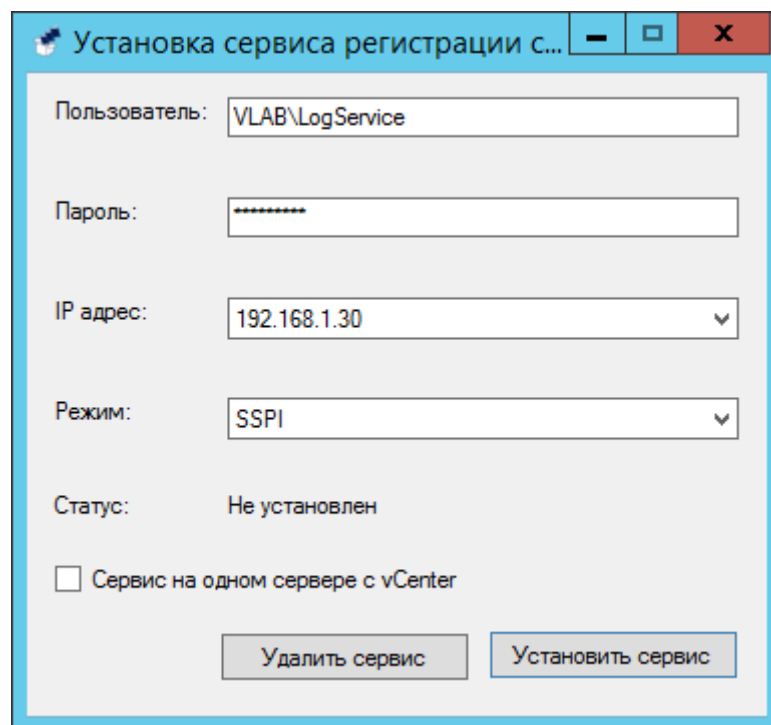


Рисунок 22 - Установка сервиса регистрации событий

При нажатии кнопки <Установить сервис> значение поля «Статус» сменится на «Устанавливаем...», затем, если все условия были выполнены, утилита отобразит сообщение «Сервис успешно установлен и готов к работе!», и в списке сервисов добавится «LogService-V» (рисунок 23).

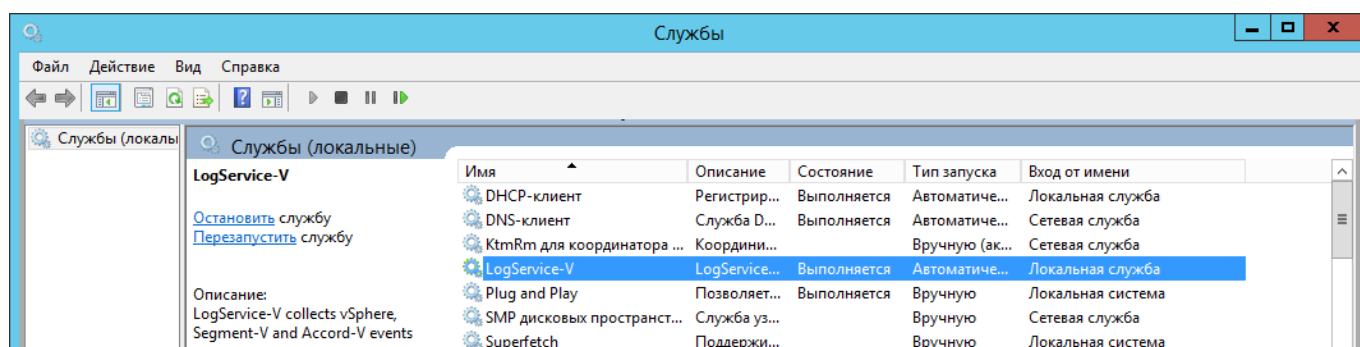


Рисунок 23 - Проверка запуска сервиса

Далее для настройки работы с сервисом регистрации событий следует запустить с правами администратора утилиту «**LogViewer-V.**» на АРМ АБИ и открыть окно настроек, нажав на кнопку <Настройки> (рисунок 24).

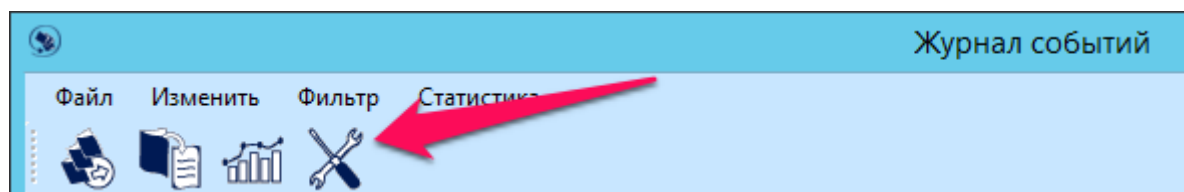


Рисунок 24 – Кнопка <Настройки>

В появившемся далее окне следует указать IP-адрес сервиса регистрации событий (выбранный ранее в утилите LogServiceInstall) и выполнить подключение, нажав кнопку <Принять> (рисунок 25).

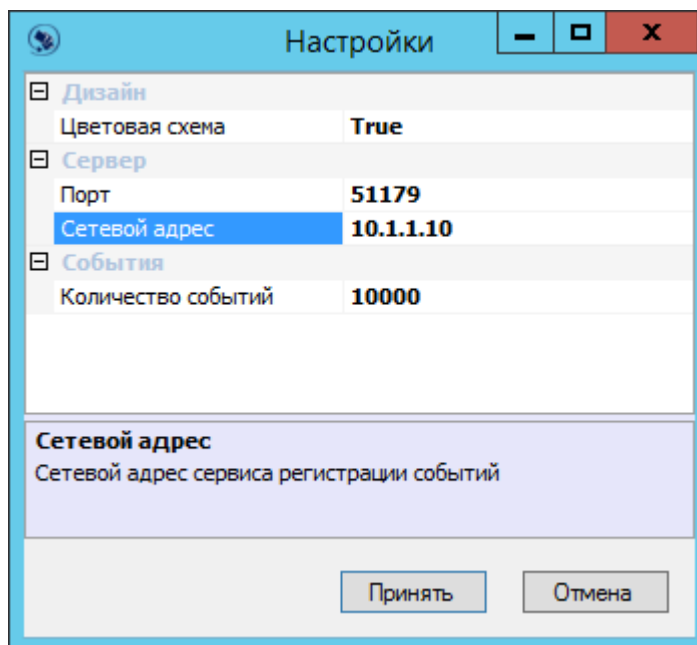


Рисунок 25 - Настройка IP-адреса сервиса регистрации событий

ВНИМАНИЕ! При задании IP-адреса сервера с установленным сервисом регистрации событий значения «127.0.0.1» и «localhost» не поддерживаются!

Далее в главном окне журнала регистрации событий следует нажать кнопку <Получить события> (рисунок 26) (либо выбрать пункт меню «Файл»/«Получить события», либо нажать кнопку F5).

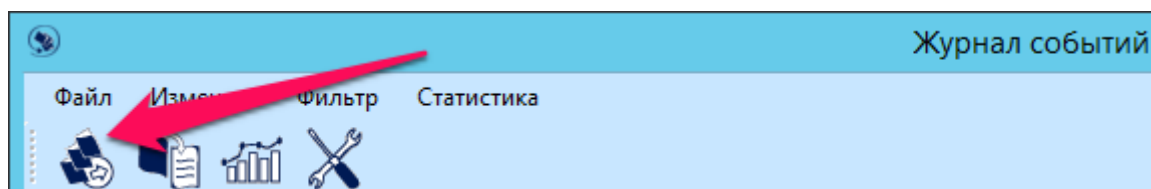


Рисунок 26 – Кнопка <Получить события>

На экран выводится список всех выполненных событий.

ВНИМАНИЕ! События в журнале регистрации событий не обновляются автоматически – для получения актуальной информации необходимо выполнять процедуру их получения.

ВНИМАНИЕ! В списке полученных событий после первого старта сервиса отображаются события о подключении к vCenter и агентам «Аккорд-В.» на ESXi (тип «ConnectionEvent» показывает, что соединение с указанными в файле конфигурации элементами прошло успешно). Необходимо удостовериться, что события подключения существуют для всех заданных элементов (всех агентов ESXi и vCenter)!

Возможной причиной, по которой соединение может быть не установлено, является рассинхронизированное время (подробнее см. раздел 2).

В дальнейшем, если соединение потеряно, сгенерируется событие с типом «ConnectionEvent» и результатом «Error»:

Журнал событий						
Файл Изменить Фильтр Статистика						
Время	Пользователь	Адрес	Компонент	Тип	Результат	Сооб
17.03.2015 20:25	VLAB\ABI	10.1.1.10		UserLoginSessionEvent	Success	User
17.03.2015 20:15		ST-vCenter.vlab.local	vCenter ST-vCenter.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 20:14		esxi-1.vlab.local	HostSystem esxi-1.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 20:14		esxi-2.vlab.local	HostSystem esxi-2.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 20:14		esxi-3.vlab.local	HostSystem esxi-3.vlab.local	ConnectionEvent	Success	Conn

ВНИМАНИЕ! Конфигурационный файл считывается только при запуске сервиса! Если в процессе работы агенты были установлены на дополнительные ESXi, необходимо перезапустить сервис (в случае отдельно установленного сервиса необходимо заменить конфигурационный файл на новый).

Примечание: В дальнейшем для работы удобно пользоваться фильтрами. Можно загружать существующие фильтры или создавать и сохранять собственные. Для создания фильтра достаточно перетащить из ячейки слева значение в область фильтра и повторно получить список событий (рисунок 27).

3. получаем повторно события с учетом фильтра

1. жажимаем левую клавишу мыши

2. переносим в эту область

Время	Пользователь	Адрес	Компонент	Тип	Результат	Сооб
17.03.2015 20:25	VLAB\ABI	10.1.1.10		UserLoginSessionEvent	Success	User
17.03.2015 20:15		ST-vCenter.vlab.local	vCenter ST-vCenter.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 20:14		esxi-1.vlab.local	HostSystem esxi-1.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 20:14		esxi-2.vlab.local	HostSystem esxi-2.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 20:14		esxi-3.vlab.local	HostSystem esxi-3.vlab.local	ConnectionEvent	Success	Conn
17.03.2015 19:58	root	st-abi-avi.vlab.local	HostSystem 10.1.1.101	PamSSH_Task	Success	Login
17.03.2015 19:58	root	st-abi-avi.vlab.local	HostSystem 10.1.1.102	PamSSH_Task	Success	Login
17.03.2015 19:58	root	st-abi-avi.vlab.local	HostSystem 10.1.1.103	PamSSH_Task	Success	Login

Рисунок 27 – Создание фильтра

Работа с сервисом регистрации событий выполняется администратором безопасности информации и более подробно описана в «Руководстве администратора» СПО «Аккорд-В.».

Примечание: Причины возникающих неполадок в процессе работы сервиса регистрации событий «Аккорд-В.» выводятся также в стандартную утилиту просмотра событий операционной системы: Start -> Administrative tools -> Event Viewer.

В случае необходимости для смены учетной записи, от которой будет запускаться сервис, следует запустить утилиту LogServiceInstall.exe. При запуске утилита проверяет, установлен ли на СБТ сервис регистрации событий; если сервис установлен, вместо кнопки <Установить сервис> в окне утилиты отображается кнопка <Сменить настройки> (рисунок 22). Для смены учетной записи следует в главном окне утилиты ввести новые учетные данные (поля «Пользователь» и «Пароль») и нажать кнопку <Сменить настройки>.

После успешной установки модулей защиты «Аккорд-В.» на ESXi-серверы следует перейти к процедуре предъявления лицензии.

3.6.4.2. Сервисная учетная запись

Сервисная учетная запись, предназначенная для запуска сервиса регистрации событий, должна обладать следующими правами:

1) учетная запись должна быть доменной в случае использования режима подключения «SSPI» (в случае установки на одном АРМ с vCenter допускается локальная учетная запись), в случае использования режима «CredentialStore» сервис запускается от учетной записи «Локальная служба»;

2) на vCenter (в случае его использования) и на ESXi-хостах (в случае standalone) для данной учетной записи должны быть заданы ReadOnly Permissions;

3) на АРМ, на котором работает сервис регистрации событий, учетная запись, от имени которой он запускается, должна обладать полными правами на папку с установленным ПО «Аккорд-В.»;

4) рекомендуется запретить локальный и удаленный вход на ПК для сервисной учетной записи.

3.6.5. Предъявление лицензии на работу с ПО управления

Для работы с утилитой настройки доверенной загрузки ВМ («Accord-V.») требуется лицензия. Она выдается производителем и поставляется на компакт-диске в составе комплекта поставки продукта или иным способом

ВНИМАНИЕ! Файл лицензии для СПО «Аккорд-В.» версии 1.3.357 и старше несовместим с более новыми версиями СПО «Аккорд-В.», поэтому при обновлении СПО «Аккорд-В.» на более новые версии потребуется запросить новую лицензию.

При этом обновление СПО «Аккорд-В.» с версии 1.3.357 на более новую возможно только посредством полного удаления старой версии СПО «Аккорд-В.» (модули «Аккорд-В.», агенты «Аккорд-В.» на ESXi, сервис регистрации событий) и установки новой версии СПО «Аккорд-В.».

Информация о версии СПО «Аккорд-В.» доступна в разделе «Помощь»-> «О программе» утилиты настройки доверенной загрузки ВМ (**Accord-V.exe**).

Для предъявления лицензии потребуется скопировать с компакт-диска файл лицензии в корень папки с установленным ПО:

C:\Program Files (x86)\OKB SAPR\Accord-V

Подробнее о системе лицензирования см. в разделе 9.

3.7. Работа с утилитой управления «Accord-V.»

3.7.1. Авторизация АБИ в системе

После предъявления лицензии следует на АРМ АБИ запустить с правами администратора утилиту **«Accord-V.»** и авторизоваться в системе – ввести учетные данные АБИ или воспользоваться функцией «использовать учетные данные текущей сессии» (рисунок 28).

Примечание: Следует помнить, что у учетной записи АБИ должны быть права на запись в базу данных ManagedDatabase.

Поле сервер, содержащее IP-адрес vCenter или ESXi, с которым будет происходить работа, заполняется автоматически из файла конфигурации. **Его изменение может привести к неправильной работе ПО!**

Адрес подключения к vCenter может быть изменен только с помощью утилиты **Installer-V.exe**.

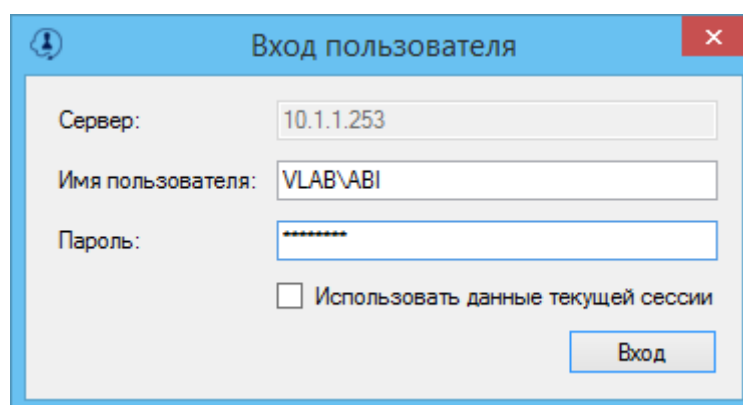


Рисунок 28 – Авторизация АБИ в системе

Если работа происходит с несколькими элементами (например, с несколькими ESXi), то запрос на авторизацию будет произведен для каждого из них.

После авторизации на экран выводится главное окно утилиты управления, в области задач которого появляются задачи на подключение к агентам «Аккорд-В.» на ESXi-серверах (рисунок 29).

Примечание: Для задач в «Accord-V.» со статусом «ошибка»/«предупреждение» возможно получение дополнительной информации (двойной клик на надписи статуса).

Задачи		
Имя	Состояние	Описание
Подключение к серверу	Завершено	Подключение к серверу esxi-1.vlab.local
Подключение к серверу	Завершено	Подключение к серверу esxi-3.vlab.local
Подключение к серверу	Завершено	Подключение к серверу esxi-2.vlab.local

Рисунок 29 – Задачи на подключение к агентам

При этом состояния подключений могут быть выделены различными цветами:

- зеленый – соединение установлено;
- желтый – соединение установлено, но на данном хосте установлена небезопасная политика работы с ВМ (в настройках выбран небезопасный режим работы с ВМ – политика по умолчанию);
- красный – соединение не удалось установить. В этом случае следует выяснить причину отсутствия соединения и нажать кнопку <Подключить> (рисунок 30).

ВНИМАНИЕ! При потере соединения с агентом «Аккорд-В.» во время работы с утилитой «Accord-V.» (потеря соединения сопровождается сообщением «Ошибка соединения с хостом» при выполнении задач) статус соединения не обновится – необходимо перезапустить утилиту!

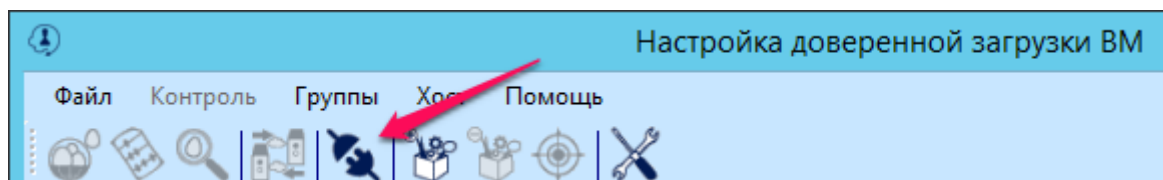


Рисунок 30 - Кнопка <Подключить>

Главное окно утилиты управления (рисунок 31) содержит следующие кнопки на панели задач:

- 1) <Поставить на контроль> - установка на контроль необходимых элементов ВМ;
- 2) <Пересчитать> – пересчет КС необходимых элементов;
- 3) <Проверить> – проверка целостности необходимых элементов;
- 4) <Миграция> – настройка ESXi серверов, на которые разрешено мигрировать данной ВМ (разрешено включаться);
- 5) <Подключить> – подключение к агенту «Аккорд-В» на ESXi, с которым не было установлено соединение при включении «Accord-V.»;
- 6) <Добавить группу> – создание новой группы;
- 7) <Удалить группу> – удаление группы;
- 8) <Добавить в группу> – добавление элементов (ВМ) в группу;

9) <Настройка> – настройка политик безопасности для хостов.

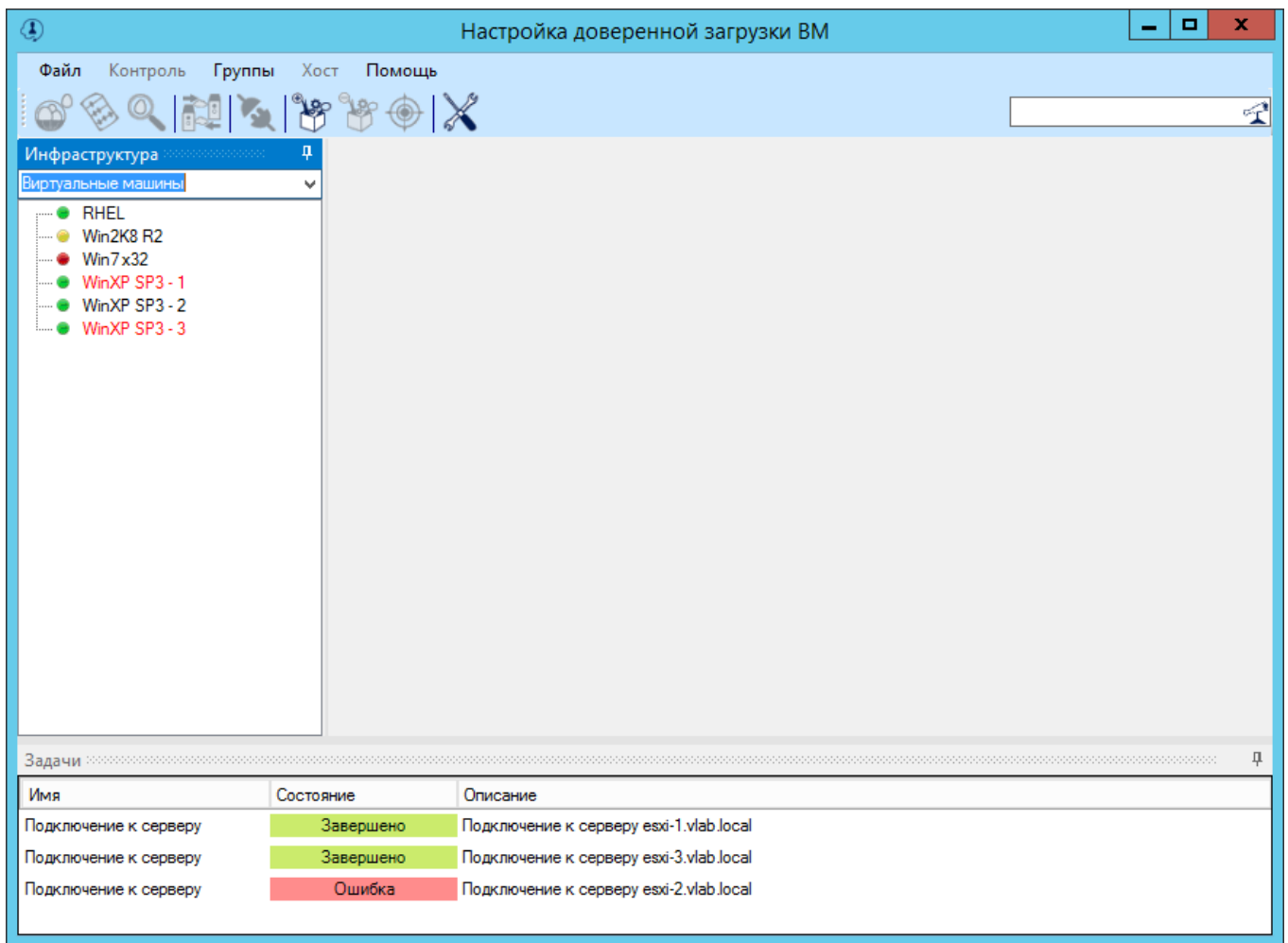


Рисунок 31 - Главное окно утилиты управления

По умолчанию в главном окне утилиты управления открывается вкладка инфраструктуры, содержащая список виртуальных машин (рисунок 31). Ее содержимое обновляется автоматически.

ВНИМАНИЕ! При наличии в инфраструктуре более 1000 VM возможно длительное получение инфраструктуры (порядка нескольких минут).

Для VM возможны следующие состояния:

- 1) зеленый маркер – VM выключена;
- 2) красный маркер – VM включена (операции с ней запрещены);
- 3) желтый маркер – VM в состоянии «Suspend»;
- 4) имя VM отмечено серым – VM удалена или конвертирована в шаблон. В случае если VM удалена или переведена в шаблон, она помечается серым цветом как неактивная. При следующем включении «Accord-V.» данная VM уже не будет отображаться;
- 5) имя VM отмечено красным – недостаточно информации о VM (например, VM находится в одном из статусов orphaned, inaccessible, unknown, disconnected);

- 6) ВМ помечена как «Unloaded virtual machine». Если ВМ находится в группе, то при включении утилиты «Accord-V.» в инфраструктуре будут отображаться unloaded virtual machine. После подключения к инфраструктуре эти элементы пропадут из списка. Ситуация, когда такие записи остаются в списке, означает, что ВМ, состоящие в группе, были удалены, и их необходимо удалить из группы (в этом случае подобные записи будут удалены из списка при повторном входе в ПО).

ВНИМАНИЕ! Возможна работа только с выключенными ВМ и ВМ в состоянии «Suspend».

ВНИМАНИЕ! Если ВМ использует LVM, будет виден только загрузочный (boot) раздел.

ВНИМАНИЕ! ВМ, не имеющие vmx/vmsd/vmdk (или удаленные некорректно), помечаются в утилите «Accord-V.» как валидные, но работа с ними невозможна.

ВНИМАНИЕ! Более 4 разделов на диске не отображаются (в ситуациях, когда последний диск указывается в MBR как расширенный).

На вкладке инфраструктуры «Хосты» главного окна утилиты управления отображаются (рисунок 32):

- список ESXi, доступных в данной учетной записи (если используется vCenter);
- список ESXi, на которые устанавливался агент «Аккорд-В.» (если используются отдельные ESXi).

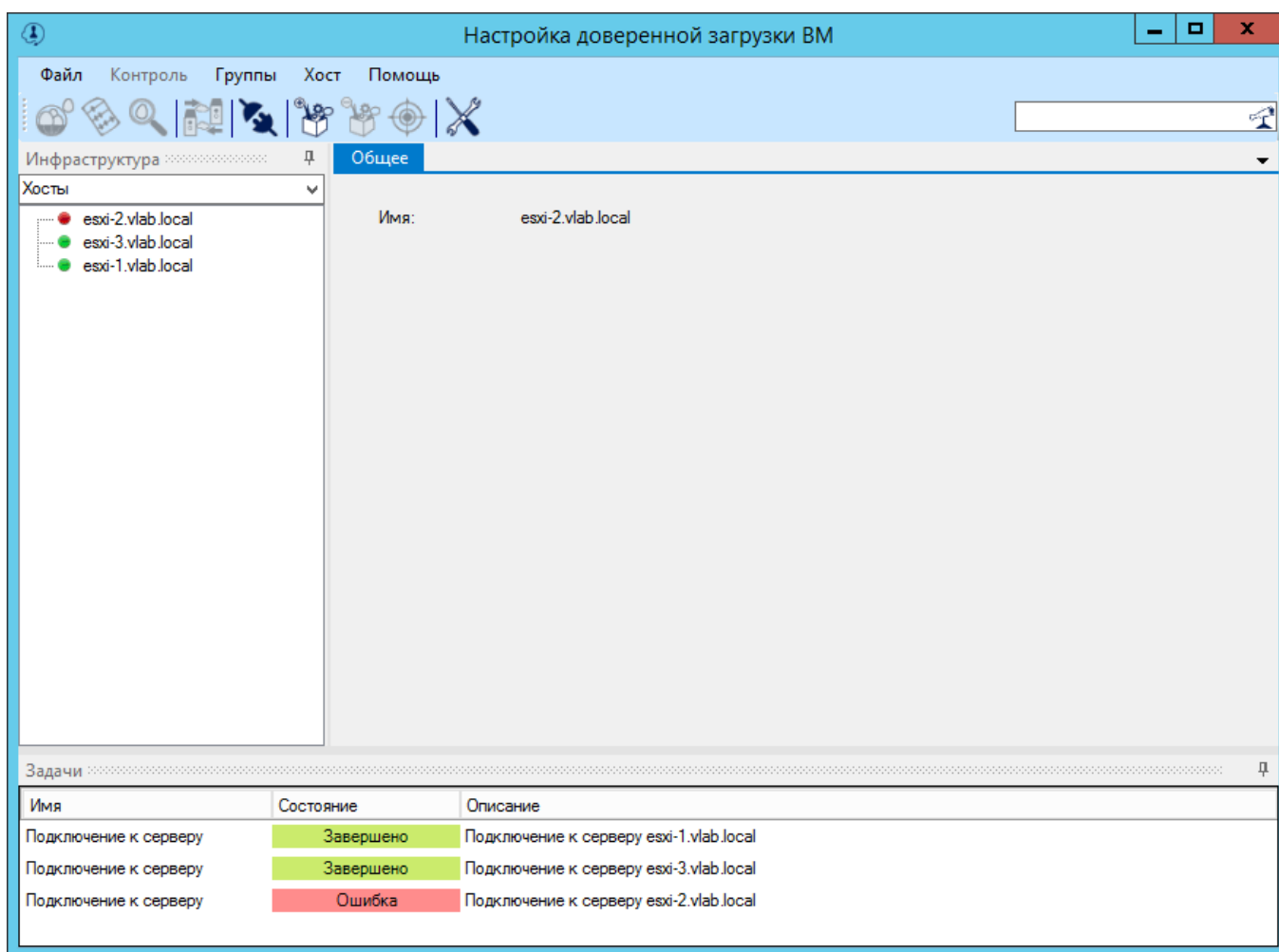


Рисунок 32 - Главное окно утилиты управления. Инфраструктура хостов

После выполнения процедуры авторизации АБИ следует перейти к настройке доверенной загрузки виртуальных машин.

3.7.2. Настройка доверенной загрузки виртуальной машины с vCenter

Настройка доверенной загрузки виртуальной машины с vCenter (если vCenter реализован в качестве VM) имеет ряд существенных особенностей.

Поскольку контроль целостности и доверенную загрузку нельзя настроить для **включенной** виртуальной машины, необходимо ее выключить, однако после этого подключиться к данному vCenter в «Accord-V.» будет невозможно.

Поэтому для vCenter на виртуальной машине предлагается особый вариант настройки:

- 1) до выключения VM с vCenter зайти в утилиту «Accord-V.» и включить мягкий режим для тех хостов, на которые разрешена миграция виртуальному vCenter;
- 2) выйти из утилиты «Accord-V.» и выключить VM с vCenter;
- 3) отредактировать файл конфигурации Config.xml, заменив в строке "InfoServer name" IP-адрес vCenter на IP-адрес ESXi;

4) включить утилиту «Accord-V.» и подключиться к ESXi, введя учетные данные ESXi пользователя;

5) выбрать виртуальную машину с vCenter и поставить ее на контроль, разрешив миграцию на данный хост и посчитав КС контролируемых компонентов;

6) выйти из утилиты «Accord-V.»;

7) если виртуальной машине с vCenter разрешено мигрировать на другие хосты, то после шага 6 для каждого из ESXi выполнить следующее:

- зайти через vClient на ESXi, на котором в данный момент находится vCenter, и разрегистровать с него виртуальную машину с vCenter (Remove from Inventory);

8) подключиться к другому ESXi, на который разрешена миграция для ВМ с vCenter, и добавить виртуальную машину, открыв хранилище и выбрав соответствующий vmx файл (Add to Inventory);

9) повторить шаги 3-6 уже для этого ESXi.

10) вернуть в Config.xml текущий IP-адрес vCenter в поле "InfoServer name";

11) подключиться к ESXi и включить vCenter;

12) включить утилиту «Accord-V.» и отключить мягкий режим для хостов.

ВНИМАНИЕ! После такой настройки верная информация о текущих компонентах контроля виртуальной машины с vCenter будет отображаться **только при подключении к последнему ESXi, на котором выполнялась настройка vCenter**. Данная виртуальная машина будет отображаться как неконтролируемая, для остальных виртуальных машин информация будет корректной. Включение и проверка компонентов будет происходить в штатном режиме.

3.7.3. Настройка доверенной загрузки ВМ

3.7.3.1. Работа с ВМ по отдельности

Настройка доверенной загрузки ВМ осуществляется при помощи утилиты управления «**Accord-V.**» после авторизации АБИ в системе (см. 3.7.1).

ВНИМАНИЕ! Перед первым сеансом работы с пользовательским интерфейсом управления «Аккорд-В.» необходимо предварительно настроить инфраструктуру виртуализации, в том числе создать необходимые виртуальные машины, установить в них СПО разграничения доступа (см. 3.5).

ВНИМАНИЕ! В «Аккорд-В.» по умолчанию предусмотрена политика, когда неконтролируемые ВМ не включаются. Т.е. **после установки агента на ESXi никакие ВМ нельзя будет включить** (при этом работающие ВМ продолжат работу).

Изменить данную политику можно в настройках утилиты «**Accord-V.**» (режим включения новых ВМ и «мягкий» режим – подробнее см. «Руководство администратора»). Изменение режимов считается небезопасным, события агентов в таком случае выводятся со статусом «Warning».

ВНИМАНИЕ! Процедура настройки доверенной загрузки ВМ выполняется только после предъявления лицензии (подробнее см. 3.6.5).

ВНИМАНИЕ! Основные задержки по времени и ограничения по производительности, связанные с использованием «Аккорд-В.», возникают на этапе постановки ВМ на контроль целостности. Установка на контроль производится массово и единоразово. В дальнейшем процедура постановки на контроль целостности выполняется только для новых ВМ, что, как правило, занимает единицы минут.

При каждом старте ВМ выполняется процедура контроля целостности, и время задержек очень сильно зависит от количества установленных на контроль файлов ВМ: если набор установленных на контроль файлов минимален (например, загрузчик, основные файлы ОС, модули разграничения доступа), речь идет о секундах.

ВНИМАНИЕ! В каталоге с установленным ПО «Аккорд-В.» имеется подкаталог Addons, в котором расположены списки рекомендованных к контролю целостности файлов для соответствующих ОС, установленных в виртуальных машинах. Данный список можно импортировать при постановке виртуальной машины на контроль и затем применить для конкретного логического диска данного vmdk-файла виртуальной машины.

Для настройки доверенной загрузки ВМ необходимо выполнить следующие действия:

1. Настроить для необходимых ВМ параметры миграции (эта настройка отвечает за то, на каких ESXi ВМ смогут включиться; если вычислить КС для ВМ, но не разрешить миграцию никуда, то она не включится!). Для этого следует:

- 1) выбрать необходимую ВМ (**должна быть в состоянии *suspend* или *выключена***) и нажать кнопку <Миграция> (рисунок 33) (или выбрать соответствующий пункт контекстного меню, вызываемого посредством нажатия на ВМ правой клавишей мыши);

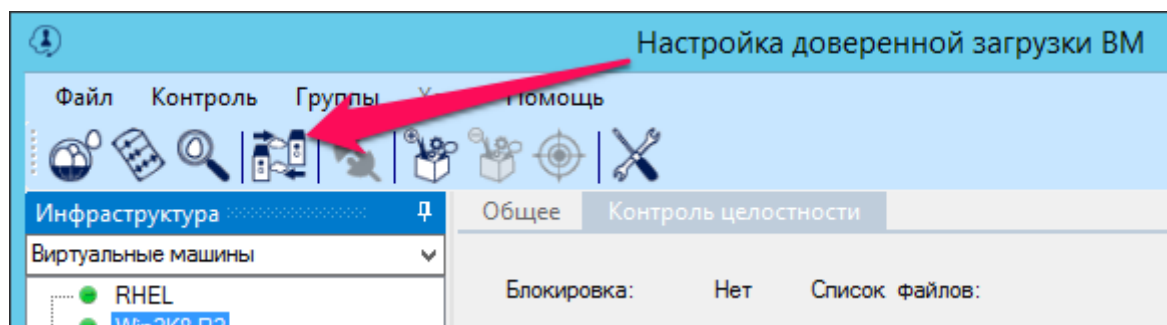


Рисунок 33 – Кнопка <Миграция>

- 2) в появившемся далее окне добавить ESXi-серверы, на которые миграция будет разрешена. Для этого в левой области окна следует выбрать нужные хосты (в том числе при помощи клавиш <Shift> и <Ctrl>), нажать кнопку <+> для добавления в список разрешенных (правая часть окна), применить настройку, нажав кнопку <Применить> (рисунок 34), и дождаться завершения данной задачи.

ВНИМАНИЕ! В процессе выполнения процедуры настройки параметров миграции для ВМ применяются текущие настройки контроля целостности.

ВНИМАНИЕ! При установке параметров миграции ВМ необходимо выбирать только те хосты, которые имеют доступ к хранилищу с данной ВМ. Если ВМ размещена на локальном хранилище, следует указывать только тот хост, который имеет данное хранилище.

Контроль миграции в настоящий момент реализован следующим образом. Если ВМ на момент миграции **включена**, а также:

- **ее оборудование не изменилось, и на втором гипервизоре разрешена ее работа**, то ВМ успешно мигрирует;
- **контроль ее оборудования не пройден, и/или на втором гипервизоре работа этой ВМ запрещена**, то «Аккорд-В.» останавливает попытку миграции (миграция завершится ошибкой timeout); при этом ВМ продолжает работу на сервере, на котором была запущена. В журналах «Аккорд-В.» фиксируется учетная запись, от имени которой была дана команда на миграцию, а также информация о том, что «Аккорд-В.» остановил попытку запуска ВМ на другом хосте. В случае если вместе с «Аккорд-В.» используется также модуль «Сегмент-В.», на экран АРМ администратора, инициировавшего миграцию, выводится окно с сообщением о том, что операция была запрещена «Сегмент-В.».

Если ВМ **выключена или находится в состоянии suspend**, команда на миграцию будет передана, ВМ мигрирует на второй гипервизор (в случае использования вместе с «Аккорд-В.» модуля «Сегмент-В.» – не мигрирует). Если **работа ВМ** на этом гипервизоре:

- предварительно **разрешена**, ВМ успешно запустится;

- предварительно **не разрешена**, то после миграции VM не запустится, пока запуск не будет разрешен в агенте «Аккорд-В.».

«Сегмент-В.» защищает (блокирует) от попыток миграции VM, выполняемых пользователем, т.к. перехватывает действия к vCenter; а «Аккорд-В.» защищает от миграции VM, выполняемой системой без участия пользователя (DRS / HA). При этом «Аккорд-В.» для выключенной VM запрещает не миграцию, а только включение.

ВНИМАНИЕ! Если миграция не разрешена ни на один хост, то вне зависимости от настроек КЦ VM нигде не включится!

ВНИМАНИЕ! Рекомендуется включать не более 10 VM одновременно.

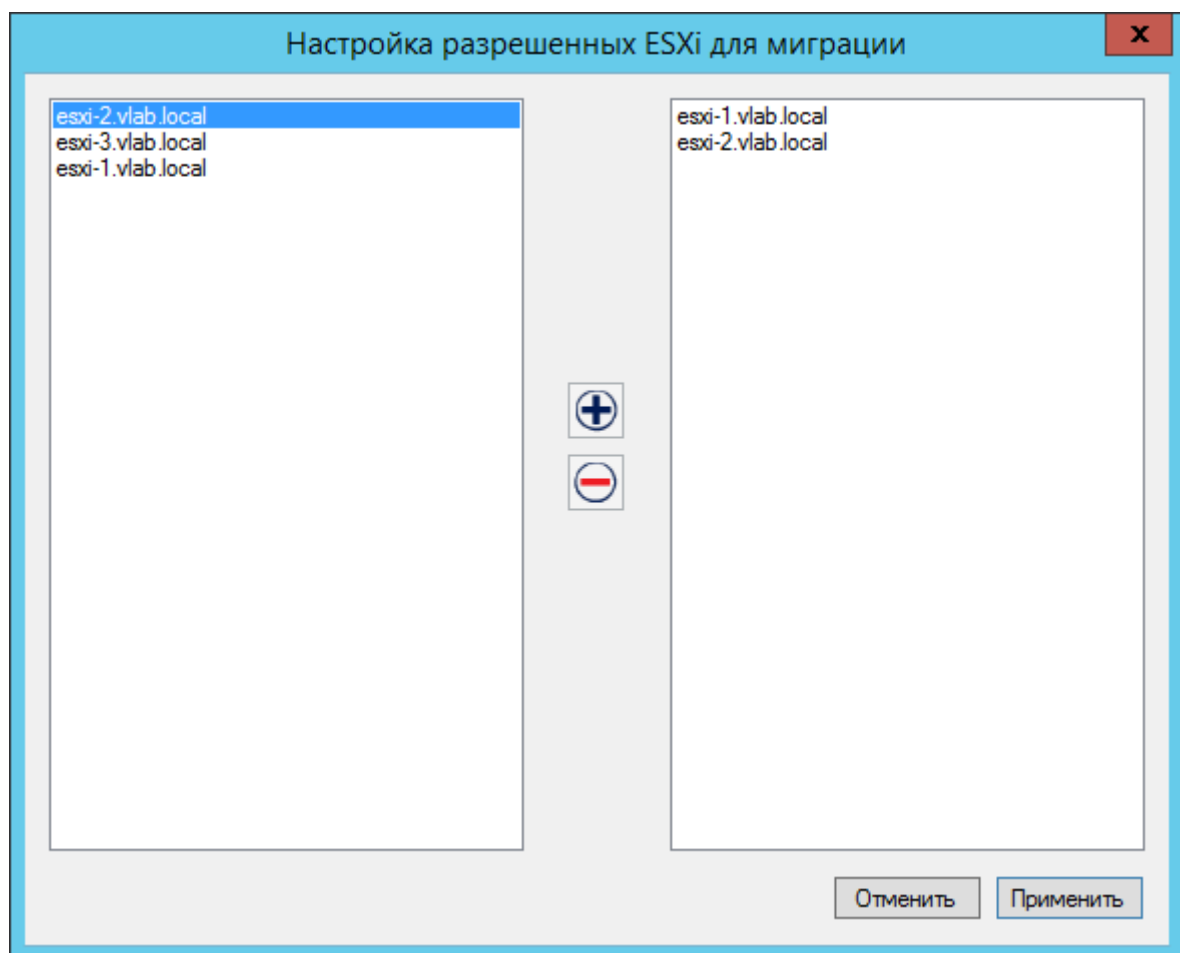


Рисунок 34 - Настройка списка ESXi серверов, на которые будет разрешена миграция VM

2. Вычислить КС необходимых элементов VM. Для этого следует:

- 1) выбрать VM и нажать кнопку <Установить> (рисунок 35) (или выбрать соответствующий пункт контекстного меню, вызываемого посредством нажатия на VM правой клавишей мыши);

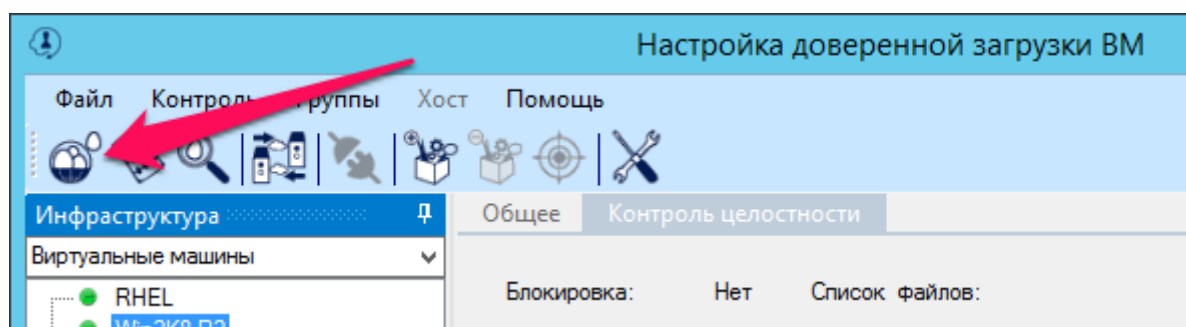


Рисунок 35 - Кнопка <Установить>

2) в появившемся далее окне (рисунок 36) выбрать для установки на контроль необходимые компоненты из следующего списка:

- «Оборудование» (vmx);
- «BIOS» – при каждом включении VM будет использоваться BIOS, поставленный на контроль;
- «MBR» – контролируется на каждом vmdk текущего состояния VM;
- «Файлы» – файлы, контролируемые при запуске (список отображается в колонке «Список файлов»).

Примечание: Для гостевых ОС существуют списки рекомендованных файлов для установки на контроль. Также существует возможность сохранять/загружать собственные списки файлов.

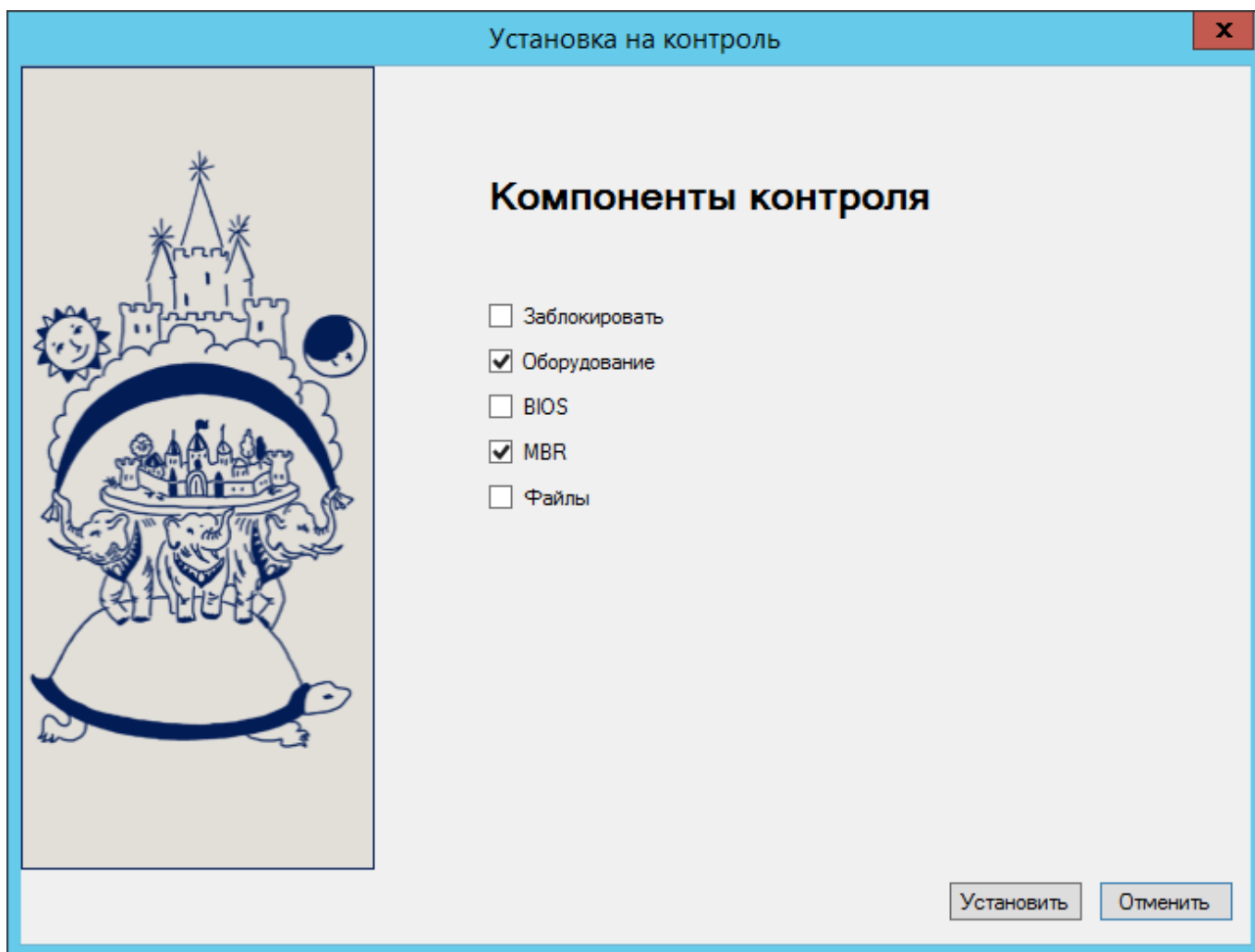


Рисунок 36 - Выбор компонентов контроля

- 3) в случае если на контроль не предполагается устанавливать файлы, нажать кнопку <Установить> (рисунок 36) и дождаться завершения процедуры расчета КС.

ВНИМАНИЕ! Нажимая кнопку <Установить>, Вы удаляете предыдущие настройки для ВМ!

- 4) в случае если на контроль устанавливаются файлы, следует нажать кнопку <Далее> (рисунок 37);

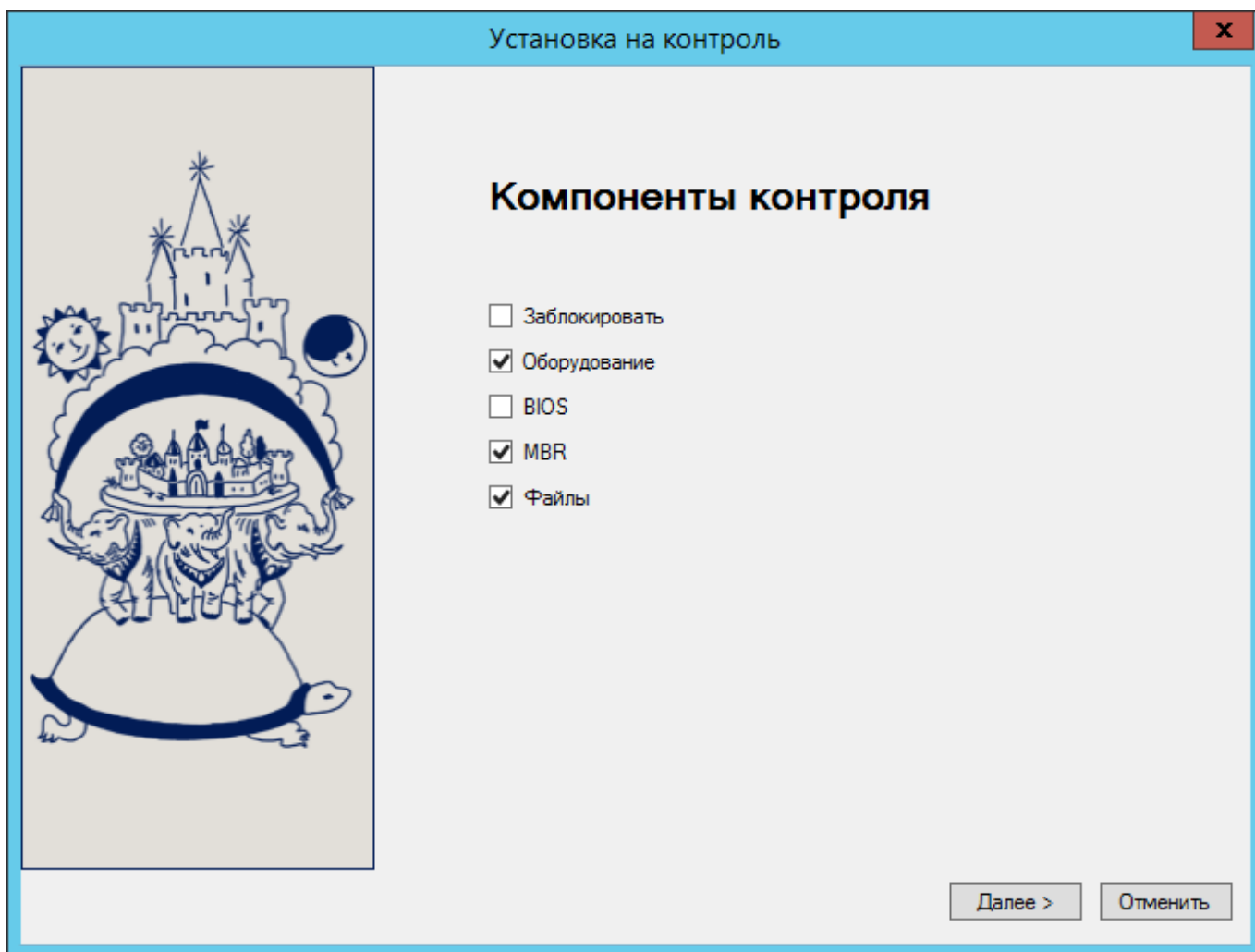


Рисунок 37 - Выбор компонентов контроля

- 5) в появившемся далее окне (рисунок 38) следует установить на контроль необходимые файлы. Для этого в левой области окна для соответствующих vmdk, принадлежащих данной ВМ, необходимо выбрать нужные файлы гостевой ОС (в том числе при помощи клавиш <Shift> и <Ctrl>) и нажать кнопку <+> для добавления в список контролируемых (правая часть окна). Список файлов отображается в отсортированном по имени виде;

ВНИМАНИЕ! Контрольные суммы рассчитываются для следующих параметров:

- для критичных параметров оборудования ВМ – CPU/ ОЗУ / диски и внешние устройства (usb / floppy / serial / parallel) и т.п.;
- для выбранных файлов гостевой ОС ВМ;
- для MBR.

ВНИМАНИЕ! Файлы, зашифрованные встроенными средствами Windows, не рекомендуется устанавливать на контроль. Это не относится к файлам, зашифрованным сторонними СКЗИ – их целостность контролируется аналогично стандартным файлам.

ВНИМАНИЕ! Если для ВМ миграция не разрешена ни на один ESXi, список файлов получить будет невозможно.

Полученный список можно экспортировать в файл (кнопка <Экспорт>). Для импорта в дальнейшем необходимо выбрать vmdk, к которому будет применяться этот список, и нажать кнопку <Импорт>.

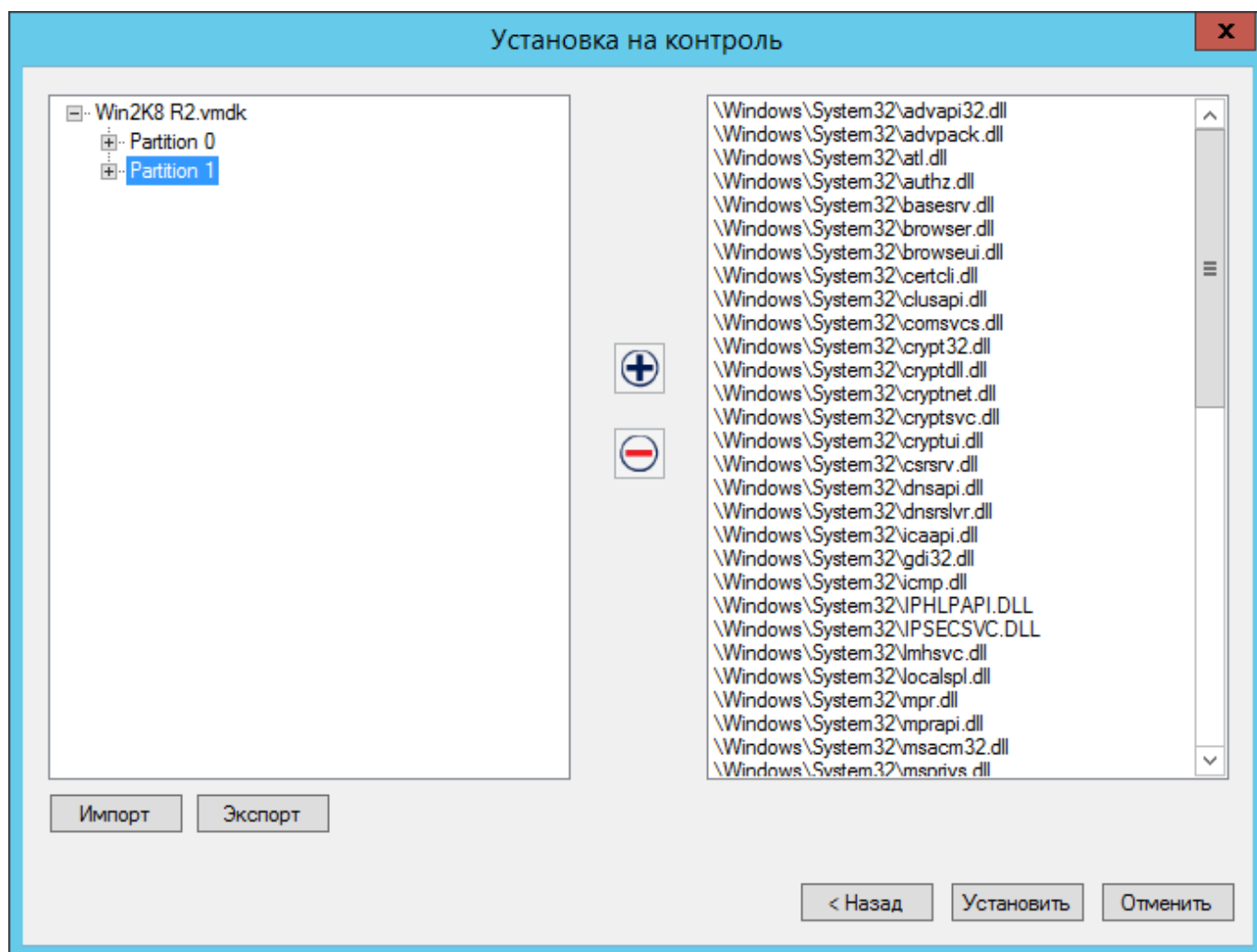


Рисунок 38 - Установка файлов на контроль

6) в завершение следует нажать кнопку <Установить> и дождаться окончания процедуры расчета КС (рисунок 39).

ВНИМАНИЕ! Нажимая кнопку <Установить>, Вы удаляете предыдущие настройки для ВМ!

ВНИМАНИЕ! В процессе расчета КС не включайте ВМ, иначе операция будет прервана!

ВНИМАНИЕ! По истечении 120 секунд исполнение задачи на ESXi будет прервано (т.е. если во время установки на контроль произошла ошибка, через 120 секунд в «Accord-V.» появится сообщение о проблеме передачи данных). Не закрывайте «Accord-V.» в момент исполнения задач! Дождитесь таймута!

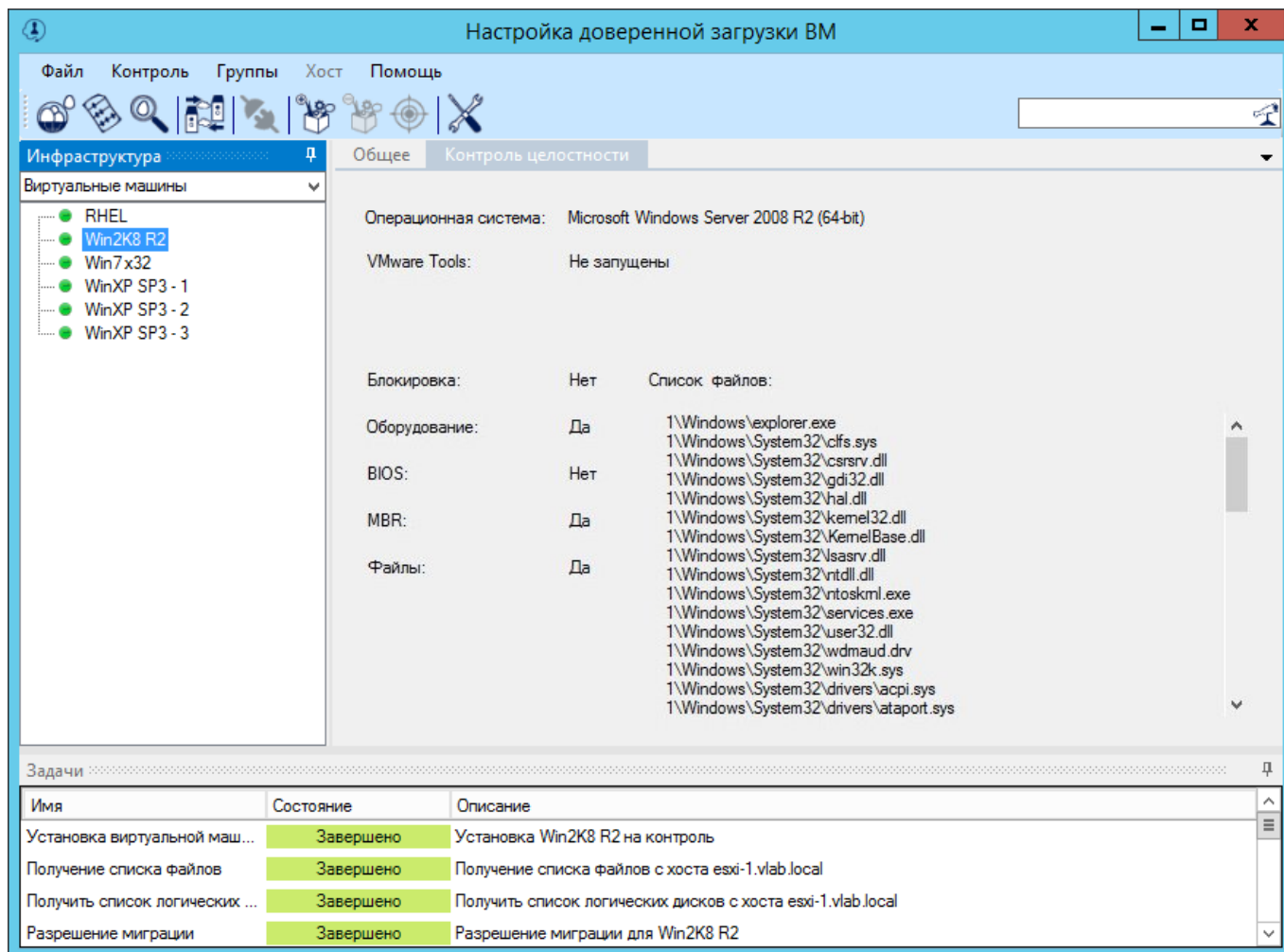


Рисунок 39 - Процесс установки на контроль

ВНИМАНИЕ! Fault Tolerance VM отображаются как две отдельные VM (обе нужно устанавливать на контроль).

ВНИМАНИЕ! Размер файлов, устанавливаемых на контроль, не должен превышать 300Мб.

ВНИМАНИЕ! В случае если при постановке на контроль файлов утилита «Accord-V.» сообщает о том, что они не обнаружены (при этом достоверно известно, что файлы имеются на диске), рекомендуется выполнить дефрагментацию MFT. Это можно сделать, например, с помощью утилиты UltraDefrag: скачать утилиту с сайта https://sourceforge.net/projects/ultradefrag/?source=typ_redirect

(в зависимости от разрядности ОС необходимо скачивать соответствующую версию дистрибутива), установить и запустить ее, выбрать проблемный диск и нажать кнопку <Оптимизировать MFT> (рисунок 40).

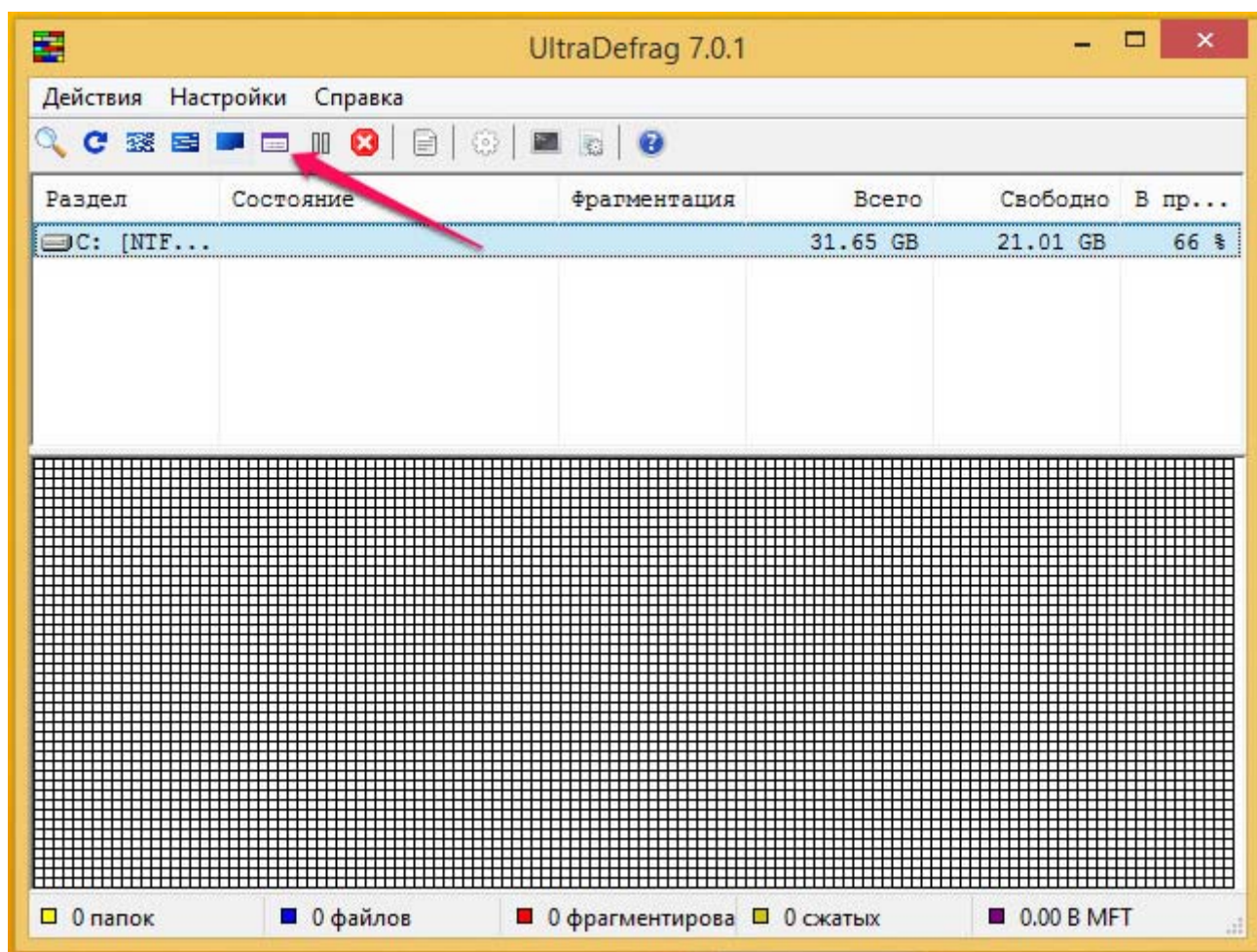


Рисунок 40 - Оптимизация MFT

ВНИМАНИЕ! Работа с MBR/Файлами у VM, работающих с RDM, не поддерживается.

ВНИМАНИЕ! Если для VM были сделаны снапшоты, и ее необходимо повторно установить на контроль, следует перезапустить утилиту «Accord-V.».

ВНИМАНИЕ! Если во время функционирования утилиты «Accord-V.» для VM, с которой предполагается работа, был сделан снапшот, рекомендуется перезапустить утилиту.

ВНИМАНИЕ! Если контролируемая VM сменила хранилище, для дальнейшей работы с ней (пересчет КС, изменение контролируемых параметров) требуется полная перепостановка VM на контроль.

ВНИМАНИЕ! Если к контролируемой ВМ в дальнейшем потребуется добавить USB-контроллер, необходимо выполнять следующую последовательность действий:

1. Выключить ВМ;
2. Добавить USB-контроллер;
3. Вычислить КС оборудования;
4. Включить ВМ;
5. Подключить USB к ВМ;
6. Выключить ВМ;
6. Пересчитать КС (т.к. добавятся новые строчки!);
7. Включить ВМ (теперь возможна полноценная работа с USB в ВМ).

Подключение USB-контроллера «на горячую» завершится ошибкой. При следующем включении ВМ не включится из-за изменившегося оборудования.

3.7.3.2. Работа с группами

В случае наличия множества однотипных ВМ (VDI) можно воспользоваться механизмом групп: вкладка «Группы» предназначена для объединения ВМ с едиными настройками.

ВНИМАНИЕ! При работе с группами следует учитывать, что ВМ должны соответствовать следующим требованиям:

1. Если не предполагается устанавливать на контроль файлы, то BIOS должен существовать или отсутствовать на всех группируемых ВМ (BIOS создается при первом включении ВМ);
2. Если предполагается установка MBR/файлов на контроль, то у группируемых ВМ должны совпадать: тип гостевых ОС, количество vmdk и снапшотов, их порядок, порядок логических разделов внутри vmdk (соответственно, и устанавливаемые на контроль файлы должны существовать внутри vmdk).

Порядок работы с группами следующий:

- 1) создать группу, нажав кнопку <Добавить группу> (рисунок 41);

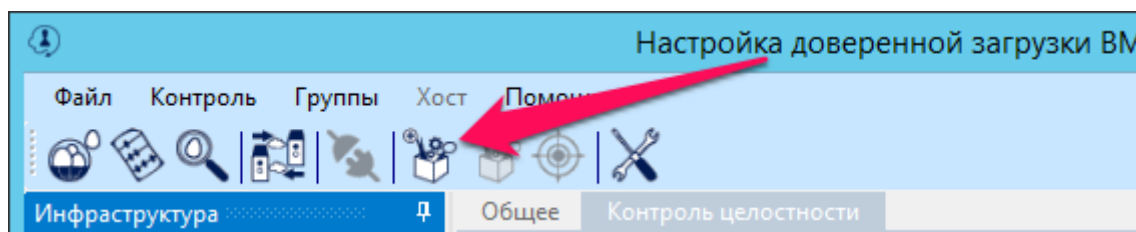


Рисунок 41 – Добавление группы

- 2) добавленную группу переименовать, нажав на нее правой клавишей мыши и выбрав пункт контекстного меню «Переименовать»;

ВНИМАНИЕ! При задании имени следует принимать во внимание ряд следующих ограничений на формат имени группы:

- имя группы не должно содержать символов кириллицы;
- имя группы не должно содержать менее трех символов;
- при задании имени группы возможно использование цифр, однако имя всегда должно начинаться с буквы.

3) добавить элементы (ВМ) в группу: нажать на кнопку <Добавить в группу> (рисунок 42), переместить нужные ВМ в правую часть появившегося окна (рисунок 43) и нажать кнопку <Применить>;

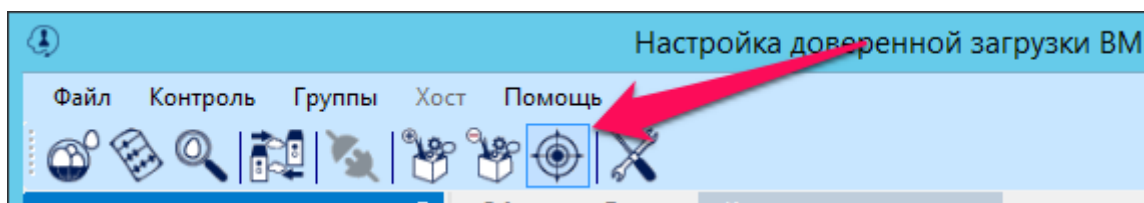


Рисунок 42 - Кнопка <Добавить в группу>

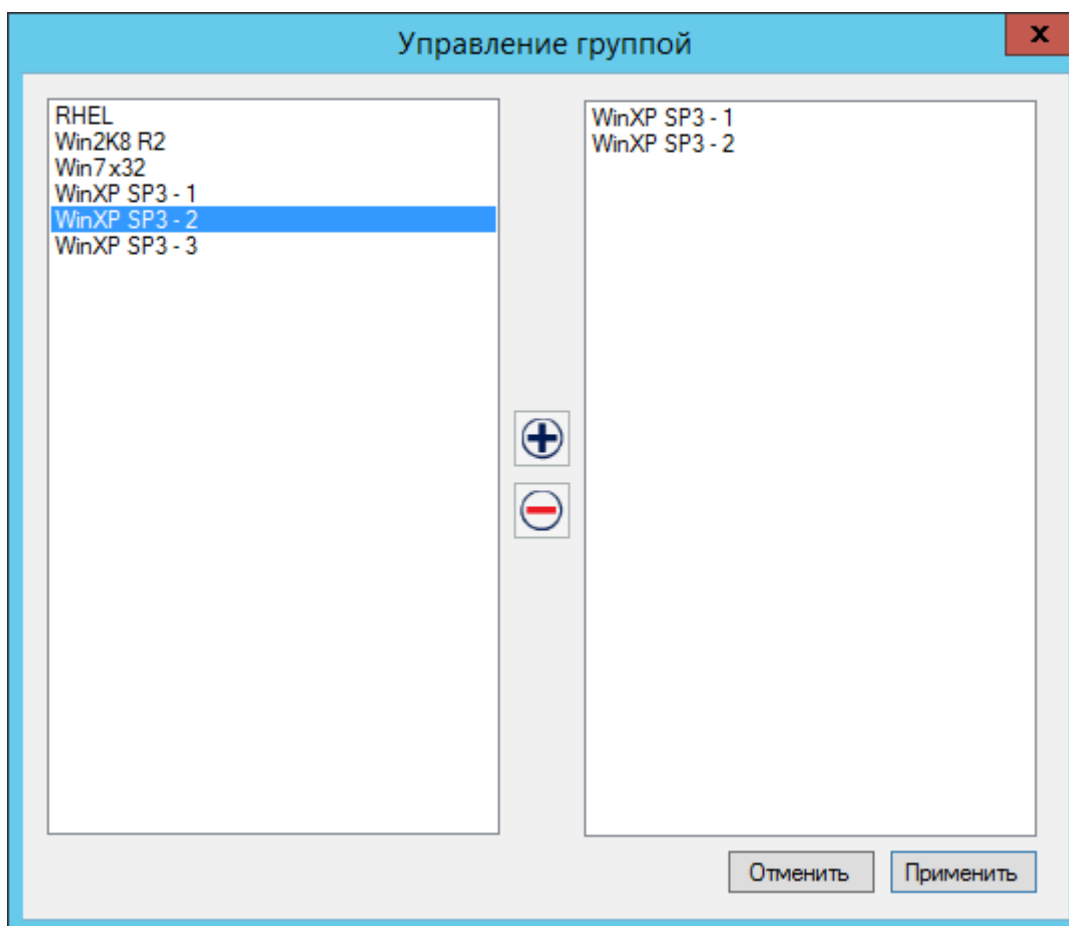


Рисунок 43 - Окно управления группой

4) выбрать группу в списке и настроить для нее параметры миграции – описание настройки параметров миграции см. выше;

5)вычислить КС необходимых элементов в сгруппированных ВМ, выбрав группу в списке и нажав кнопку <Установить>, – описание настройки параметров контроля см. выше.

В дальнейшем применяемые настройки миграции и параметры контроля для группы будут применяться для всех элементов в группе.

Примечание: После добавления ВМ в группу при включении утилиты «Accord-V.» в инфраструктуре будут отображаться незагруженные ВМ (unloaded vm). Они пропадут из списка после получения инфраструктуры.

ВНИМАНИЕ! Если для ВМ отдельно выполнить установку на контроль, то она автоматически будет выведена из группы!

ВНИМАНИЕ! В процессе добавления в группу новой ВМ групповые настройки для нее наследуются автоматически.

Группа в группе полностью наследует настройки от «родителя».

ВНИМАНИЕ! Если ВМ удалена в инфраструктуре виртуализации, необходимо удалить эту ВМ из группы (иначе в «Accord-V.» будет отображаться unloaded vm).

3.7.4. Особенности настройки доверенной загрузки ВМ при работе с Citrix XenDesktop

3.7.4.1. Настройка доверенной загрузки ВМ при работе с Citrix XenDesktop

Поскольку XenDesktop ВМ в качестве основного образа с ОС используют отдельный общий диск, настройка их доверенной загрузки имеет некоторые особенности.

Включение первой XenDesktop ВМ на ESXi-сервере инициирует блокировку на чтение/запись общего диска с ОС. В этом случае для любой другой выключенной XenDesktop ВМ (находящейся на хосте, отличном от того, где запущена первая ВМ) общий диск также будет заблокирован, и при попытке получить с любого другого хоста список файлов (рисунок 38) в окне установки на контроль будет выведено сообщение «Доступ на чтение заблокирован» (рисунок 44).

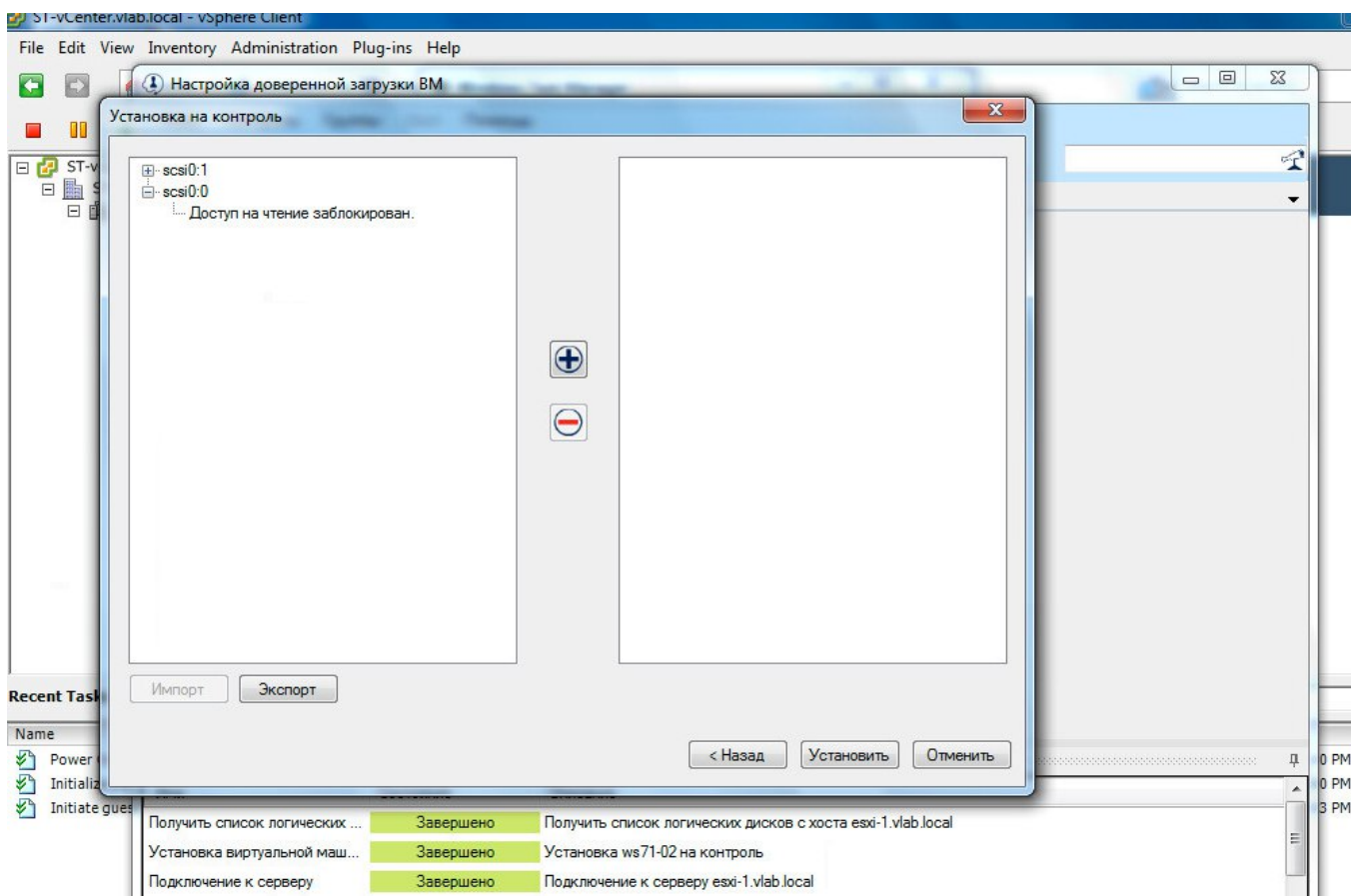


Рисунок 44 - Блокировка доступа к диску на чтение

Однако включение на другом хосте хотя бы одной XenDesktop VM, также использующей указанный общий диск, добавляет права на его чтение, в том числе и для ПО «Аккорд-В.».

При получении списка файлов в утилите **«Accord-V.»** выполняется обращение к агенту на хосте, **первом** из списка миграции. Список файлов отображается в двух случаях:

- все VM, использующие общий диск, выключены. В этом случае процедура постановки на контроль файлов не отличается от обычной;
- на **первом** хосте из списка миграции уже включена какая-либо VM, использующая общий диск (то есть добавлено разрешение на чтение для хоста, через который происходит обращение к общему диску).

Полный цикл создания и контроля целостности XenDesktop VM при этом выглядит следующим образом:

- создание VM (они выключены);
- установка VM на контроль (на данном этапе нет блокировок);
- включение первой VM -> для нее проверяются файлы (так как ничего пока не заблокировано) -> общий диск становится доступен только на чтение («Read Only») (или вообще недоступен, если на хосте еще не находится включенных XenDesktop VM);

- **для последующих ВМ, использующих этот диск, проверки не требуются, так как общий диск доступен только на чтение, и выполнение процедуры записи в нем невозможно;**
- в дальнейшем нет смысла в пересчете КС для одной ВМ, так как все XenDesktop ВМ используют общий диск (и если что-то изменится, то для всех ВМ; то есть необходимо выключить все ВМ);
- если же количество ВМ увеличится, то при настройке ее доверенной загрузки необходимо учитывать, что первый разрешаемый хост для миграции должен быть уже с правами «Read Only».

3.7.4.2. Особенности работы со средой Personal vDisk

Работа с дисками Personal vDisk обладает следующими особенностями:

- часть данных ОС (содержимое диска C:\) перенаправляется в .vhd-файл (данный файл отображается для пользователя в Windows как диск C:\);
- при этом пользовательские данные (содержимое каталога C:\Users) это не затрагивает, и они могут быть установлены на контроль в «Аккорд-В.».

Таким образом, доверенная загрузка гостевой ОС осуществляется с помощью «Аккорд-В.», но дальнейшие преобразования в ОС отследить уже не представляется возможным (гарантируется загрузка ОС из базового образа).

Защита системы такого рода обеспечивается следующими действиями:

- установка «Аккорд-Win32»/«Аккорд-Win64» для виртуальных машин на Personal vDisk (в этом варианте для ПАК «Аккорд-В.» доступен каталог с ПАК «Аккорд»);
- осуществление посредством ПАК «Аккорд-В.» контроля целостности «Аккорд-Win32»/«Аккорд-Win64» для виртуальных машин;
- установка на контроль в «Аккорд-Win32»/«Аккорд-Win64» для виртуальных машин системного и других критичных файлов на диске C:\, а также всего содержимого .vhd-файла – проверка будет выполняться при логине пользователя.

В данном подходе необходимо учитывать следующие особенности по настройке:

- в эталонной ВМ для развертывания XenDesktop в ветке реестра *HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management* необходимо создать ключ *EnforceWriteProtection* со значением 0;
- в созданных на базе эталона ВМ установить на vDisk «Аккорд-Win32»/«Аккорд-Win64» для виртуальных машин, выполнить его настройку и активацию.

3.8. Настройка разграничения доступа на совмещенном АРМ АБИ/АИБ

В том случае если АРМ, на который устанавливается СПО «Аккорд-В.», является совмещенным, то есть на нем работают и Администратор БИ, и Администратор ВИ, необходимо разграничить доступ этих администраторов к утилитам управления «Аккорд-В.» и утилитам управления VMware.

С помощью ПО ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64» это можно сделать следующим образом:

1) создание пользователей в Active Directory: Администратора БИ, Администратора ВИ и специальной учетной записи для запуска LogService (при применении режима сервиса «SSPI»);

2) на АРМ АБИ/АИБ: установка ПО ШИПКА на АРМ АБИ (вариант установки «Обычная», дать согласие с установкой драйверов от неизвестного источника);

3) на АРМ АБИ/АИБ: установка ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64» (в конце установки – настройка идентификаторов, основной – ТМ-идентификатор (АМДЗ), дополнительный – ШИПКА);

4) на АРМ АБИ/АИБ: дать учетной записи, от имени которой работает сервис регистрации событий (например, специальной учетной записи LogService) права на папку с установленным ПО Accord-V (на запись в файл EventDatabase.db, а также на чтение и создание файлов в папке);

5) на АРМ АБИ/АИБ: в утилите разграничения правил доступа (РПД) задать идентификатор и пароль для Главного администратора, создать группы администраторов БИ и ИВ, создать пользователей (из AD, указав адрес AD, указать имя домена), задать для них идентификаторы и пароли;

6) в утилите РПД группе АБИ запретить доступ к папке с vClient (выбрать папку -> сброс -> Сохранить), а группе АИБ – на папку «Аккорд-В.»;

7) в настройке комплекса «Аккорд» активировать защиту, заранее указав протоколы виртуального канала (Параметры -> Terminal Server) (если используется ПО терминальной версии «Аккорд-Win64 К»);

Подробную информацию об использовании ПО ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64» и ШИПКА см. в соответствующей документации на указанные продукты.

4. Создание резервных копий

На заключительном этапе настройки следует выполнить процедуру создания резервных копий:

1) баз данных (БД) с ESXi (с помощью утилиты Installer-V. – рисунок 45);

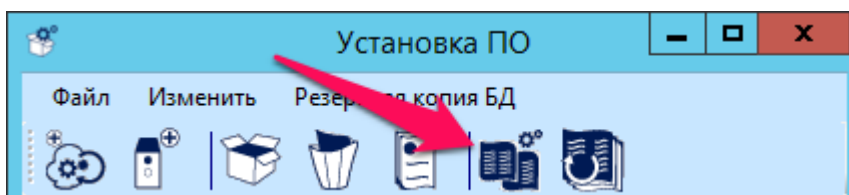


Рисунок 45 – Создание резервной копии БД

2) следующих элементов из каталога Accord-V (C:\Program Files (x86)\Accord-V):

- сертификаты: каталоги ./certs и sakey.pem;
- файл лицензии license-v.lic;
- ManagedDatabase.db (БД настроек утилиты «Accord-V.»);
- EventDatabase.db (БД событий, зарегистрированных сервисом регистрации событий);
- файлы конфигурации Config.xml и LogConfig.xml;
- фильтры утилиты просмотра событий.

5. Включение режима ESXi Lockdown Mode

Далее следует включить режим ESXi Lockdown Mode.

Для этого на vCenter следует выбрать хост -> configuration -> security profile -> lockdown mode -> enabled.

Режим ESXi Lockdown Mode не позволит:

- установить/удалить агентов «Аккорд-В.»;
- регенерировать сертификаты;
- сохранить/загрузить БД агентов «Аккорд-В.».

ВНИМАНИЕ! Все данные ESXi хранятся в ОЗУ. Если выполнять перезагрузку не стандартными способами, а путем отключения/включения питания, то возможна потеря данных в БД агентов «Аккорд-В.» (это также распространяется и на сами настройки ESXi). Поэтому после полноценной настройки рекомендуется перезагрузить все ESXi-серверы.

На этом настройку «Аккорд-В.» можно считать завершенной!

Теперь «Аккорд-В.» готов к работе. Но мы настоятельно рекомендуем, прежде чем начинать использование той или иной функции «Аккорд-В.», внимательно ознакомиться с полным комплектом эксплуатационной документации!

6. Порядок действий при обновлении гипервизора с установленным СПО «Аккорд-В.»

Если планируется **установка дополнений для гипервизора** или **переход на новую версию** (например, с ESXi версии 5.0 на ESXi версии 5.1/5.5), необходимо выполнить следующие действия:

1. Предварительно при помощи утилиты «Installer-V.» создать резервную копию БД агентов;
2. Удалить агентов «Аккорд-В.» с ESXi;
3. Выполнить процедуру обновления ESXi;
4. Повторно установить агент «Аккорд-В.» с управляющей машины (АРМ АБИ);
5. Выполнить процедуру восстановления БД из сделанной ранее резервной копии.

Также необходимо помнить, что обновление на новую версию будет обнаружено «Аккордом-АМДЗ» (ИНАФ) при перезагрузке (переход на новую версию всегда требует перезагрузки CBT), запуск CBT будет приостановлен, и потребуется выполнение процедуры пересчета контрольных сумм.

7. Интеграция СПО «Аккорд-В.» с IBM Security QRadar

Настройка взаимодействия «Аккорд-В.» с IBM Security QRadar выполняется следующим образом.

Настройка syslog на ESXi-сервере:

- 1.** Открыть исходящие порты syslog:

В vClient выбрать настраиваемый хост, затем перейти на вкладку Configuration -> Security Profile -> Firewall -> Properties и установить галочку для syslog (рисунок 46).

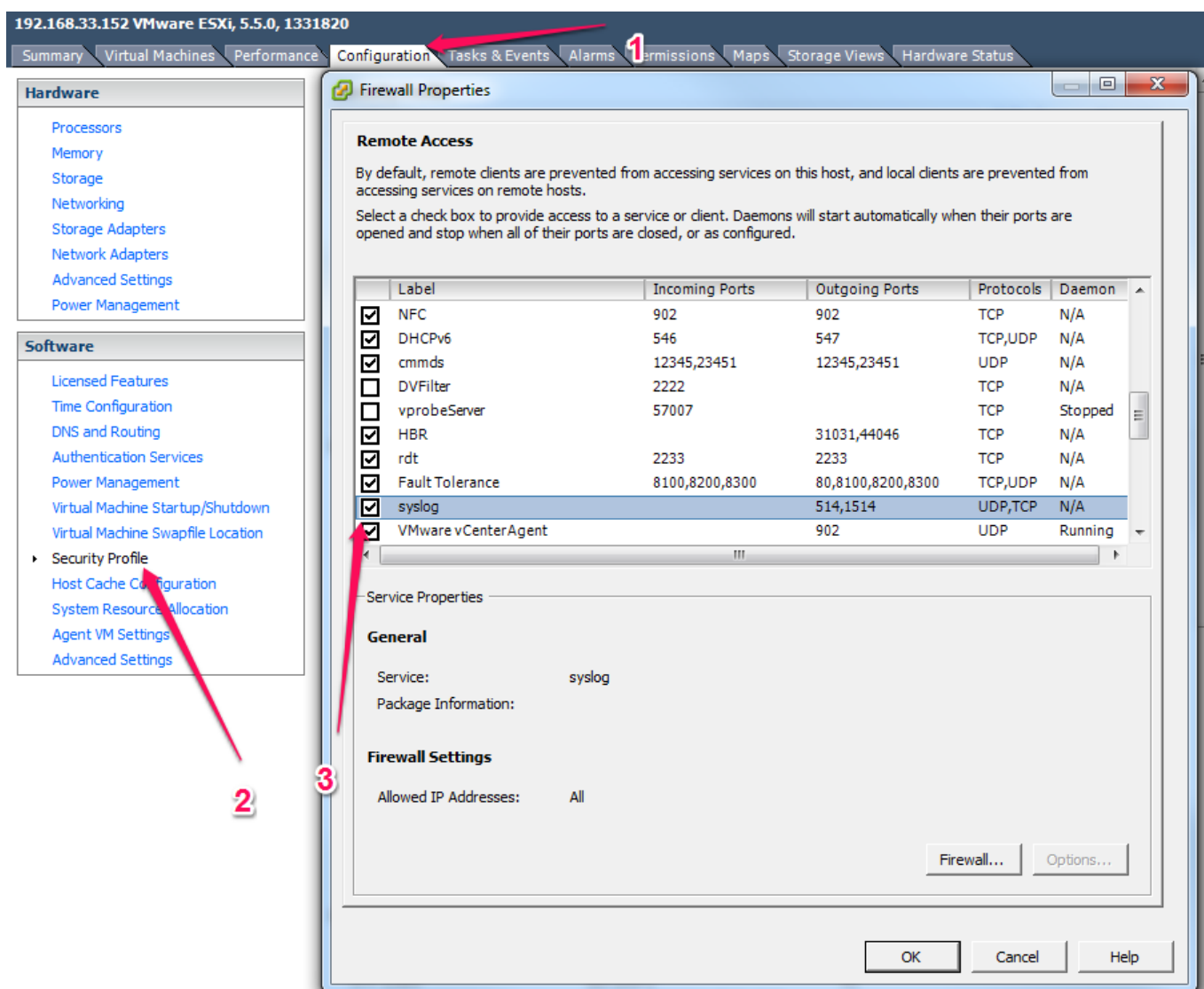


Рисунок 46 - Открытие исходящих портов syslog

2. Указать порт для передачи настроек. Данную процедуру можно выполнить одним из следующих способов:

1) настройка *через vClient* (рисунок 47): выбрать настраиваемый хост, затем перейти на вкладку Configuration, на панели Software выбрать Advanced Settings, открыть раздел Syslog -> global, указать для Syslog.global.LogHost сервер Qradar и порт для передачи (в нашем случае tcp://192.168.53.55:514; 514 – порт по умолчанию, передача возможна как по протоколу TCP, так и по UDP).

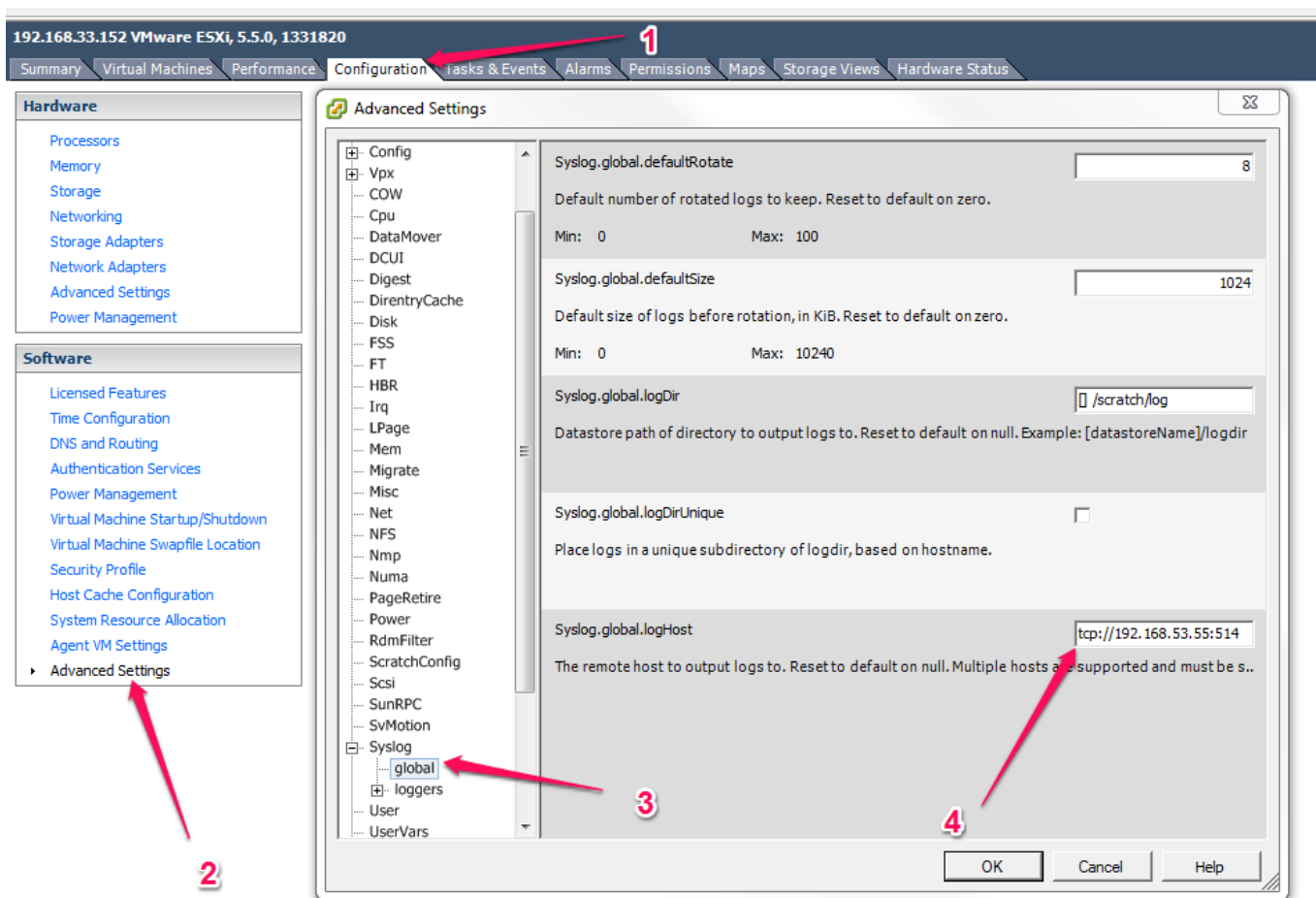


Рисунок 47 - Указание порта для передачи настроек через vClient

2) *настройка через shell/esxi* (рисунок 48):

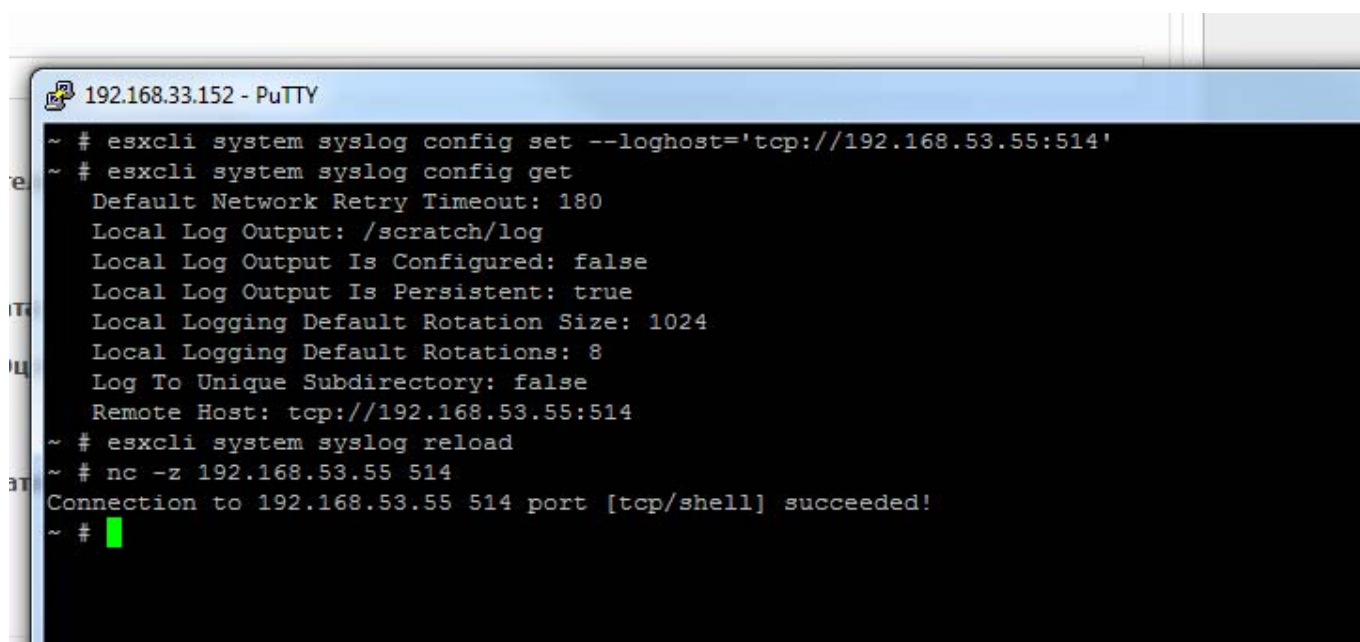
`esxcli system syslog config get` – отобразить текущие настройки;

`esxcli system syslog config set --loghost= 'tcp://192.168.53.55:514'` – указать также сервер Qradar;

`esxcli system syslog reload` – перезагрузить сервис syslog после изменения настроек;

`nc -z 192.168.53.55 514` – проверить, что подключение на заданный порт возможно;

Последние две команды полезны для проверки и в случае настройки через vClient!



```
192.168.33.152 - PuTTY
~ # esxcli system syslog config set --loghost='tcp://192.168.53.55:514'
~ # esxcli system syslog config get
Default Network Retry Timeout: 180
Local Log Output: /scratch/log
Local Log Output Is Configured: false
Local Log Output Is Persistent: true
Local Logging Default Rotation Size: 1024
Local Logging Default Rotations: 8
Log To Unique Subdirectory: false
Remote Host: tcp://192.168.53.55:514
~ # esxcli system syslog reload
~ # nc -z 192.168.53.55 514
Connection to 192.168.53.55 514 port [tcp/shell] succeeded!
~ #
```

Рисунок 48 - Указание порта для передачи настроек через shell/esxi

Настройки в Qradar:

1. Выполнить процедуру авторизации, в главном окне программы IBM QRadar Security Intelligence Platform перейти на вкладку Admin -> Log Sources (рисунок 49).

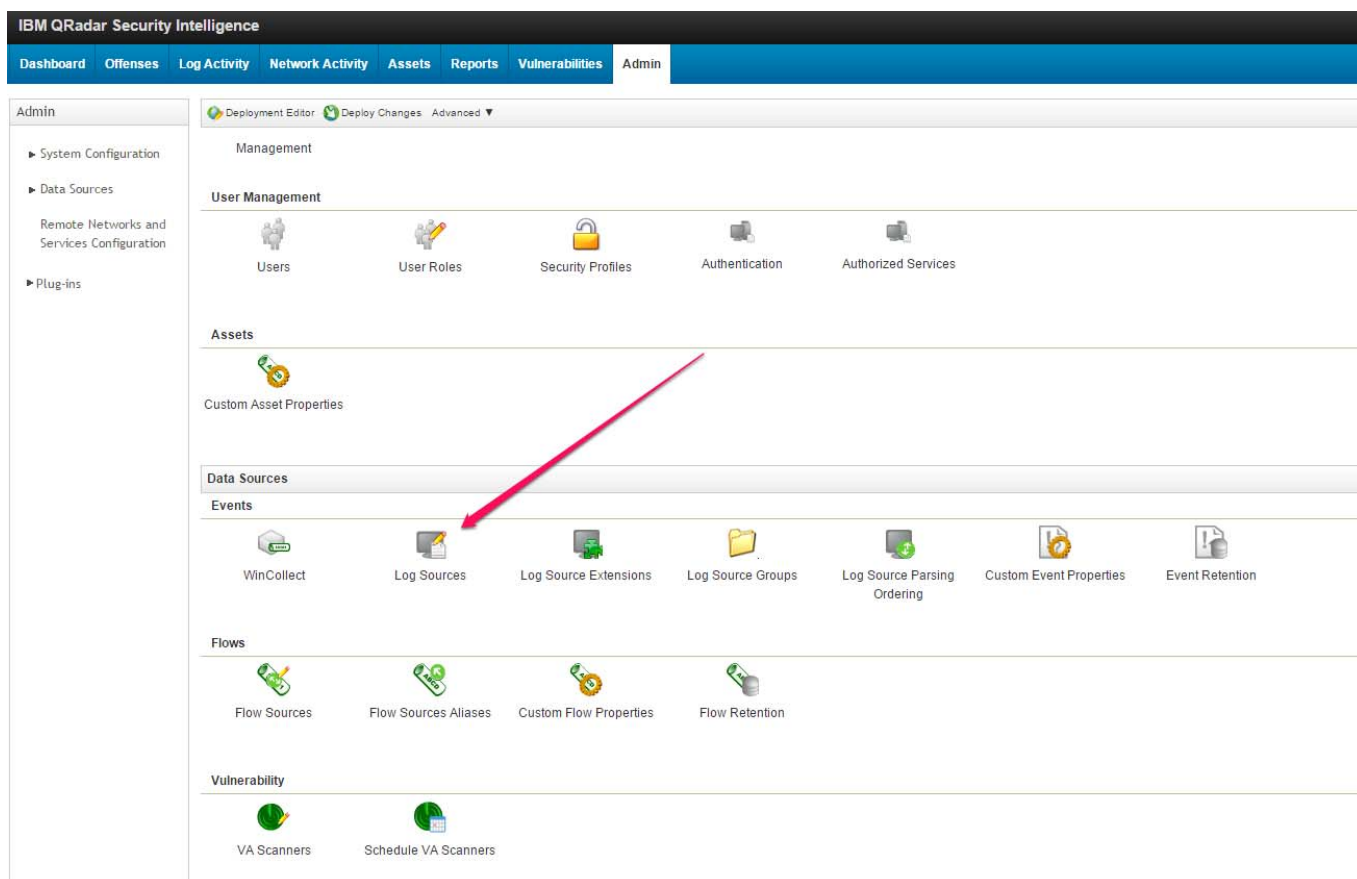


Рисунок 49 - Вкладка «Admin» главного окна программы IBM QRadar Security Intelligence Platform

2. Если автоматическое обнаружение включено, и все настройки выполнены правильно, источник уже будет отображен в «Log Sources» (рисунок 50).

Search For: Group All Log Source Groups Go Add Edit Enable/Disable Delete Bulk Actions Extensions Parsing Order Assign												
You have 1 of an allowable 750 active Log Sources as defined by your license												
Name	Desc	Status	Protocol	Group	Log Source Type	Enabled	Log Source Identifier	Target Event Collector	Credibility	Autodiscovered	Last Event Time	Creation Date
LinuxServer @ 192.168.33.152	LinuxServer device	Success	Syslog		Linux OS	True	192.168.33.152	eventcoll...	5	True	Nov 11, ...	Nov 11, ...

Рисунок 50 - Log Sources

В противном случае следует нажать <Add> и в появившемся далее окне указать параметры, аналогичные представленным на рисунке 51.

Add a log source

Log Source Name

esxi

Log Source Description

flex server

Log Source Type

Linux OS

Protocol Configuration

Syslog

Log Source Identifier

192.168.33.152

Enabled

☒

Credibility

5

Target Event Collector

eventcollector0 :: QRadarDemo

Coalescing Events

☒

Incoming Payload Encoding

UTF-8

Store Event Payload

☒

Please select any groups you would like this log source to be a member of:

Save

Cancel

Рисунок 51 - Окно добавления источника («Add a log source»)

3. Проверить, что события собираются успешно, можно в закладке «LogActivity» (рисунок 52).

IBM QRadar Security Intelligence

admin Help Messages 9 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Vulnerabilities Admin

System Time: 9:21 AM

Return to Event List

Offense

Map Event

False Positive

Extract Property

Previous

Next

Print

Event Information

Event Name	Linux login messages Message								
Low Level Category	Stored								
Event Description	Linux login messages Stored Event								
Magnitude	(5)		Relevance	6		Severity	3	Credibility	5
Username	N/A								
Start Time	Nov 11, 2015, 8:23:28 AM			Storage Time	Nov 11, 2015, 8:23:28 AM		Log Source Time	Nov 11, 2015, 8:23:28 AM	

Source and Destination Information

Source IP	192.168.33.152	Destination IP	192.168.33.152
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
IPv6 Source	0:0:0:0:0:0:0:0	IPv6 Destination	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf hex base64

Wrap Text

<166>2015-11-11T07:05:36Z flex.okbsapr.ru AccourdGuard: VirtualMachine ABI 2K12 can not be powered. Integrity was broken.

Рисунок 52 - Вкладка «Log Activity» главного окна программы IBM QRadar Security Intelligence Platform

Для этого следует выполнить процедуру добавления фильтров (рисунок 53, пример!):

- 1) Source or Destination IP | Equals | 192.168.33.152
- 2) Payload Contains | is | AccourdGuard:

3) отображенные события доступны для детального отображения по двойному щелчку; для более быстрого изучения имеется возможность выбрать режим отображения (display) *Raw Events*, в котором сразу будет виден текст сообщений.

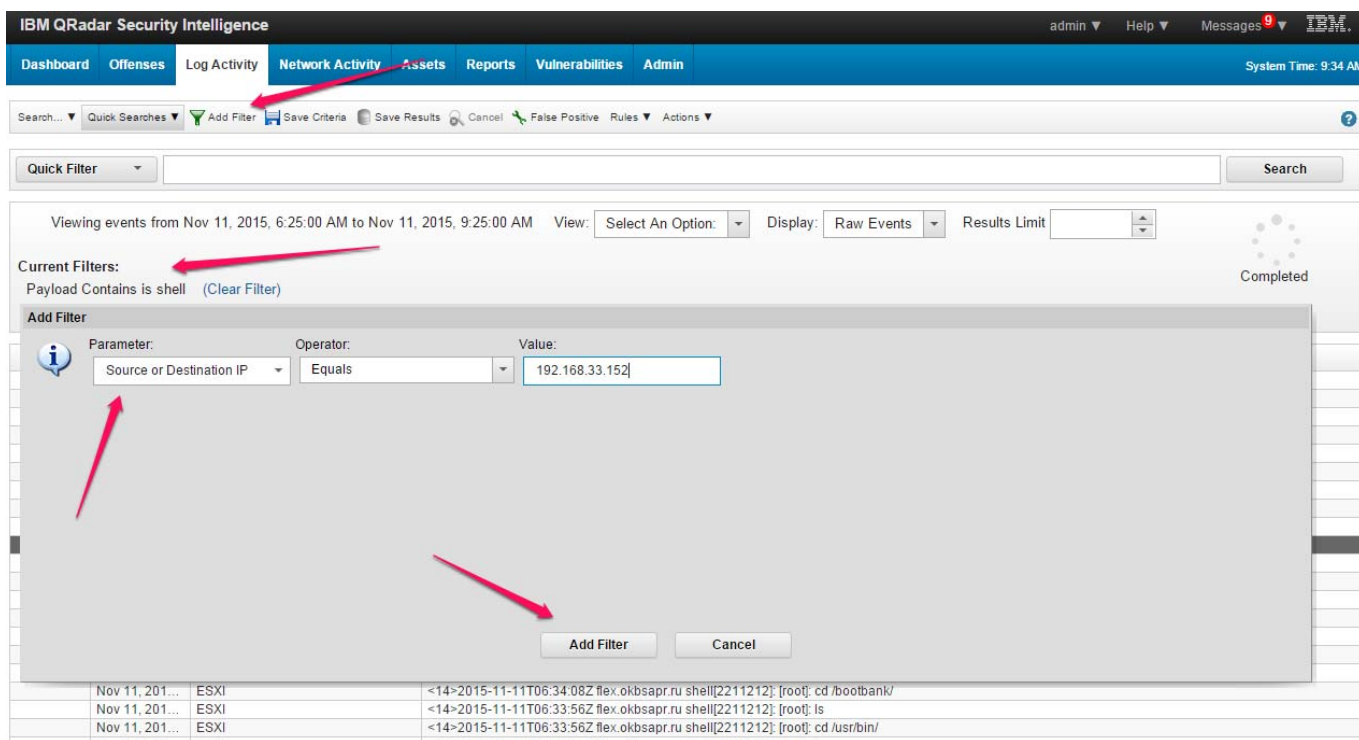


Рисунок 53 - Добавление фильтров

8. Удаление ПО «Аккорд-В.»

ВНИМАНИЕ! Действия, связанные с установкой или удалением агентов на ESXi, следует выполнять только с помощью утилиты «Installer-V.».

Следует учитывать, что статус установки агентов обновляется в окне утилиты «Installer-V.» только по факту установки или удаления агентов с помощью данной утилиты. То есть если агенты были удалены способом, отличным от рекомендованного, статус их установки в утилите не изменится.

В случае возникновения потребности в удалении ПО «Аккорд-В.» необходимо выполнить следующие процедуры в указанном порядке:

- 1) удаление агентов «Аккорд-В.» на ESXi с помощью утилиты Installer-V.;
- 2) удаление сервиса регистрации событий (logserviceinstall.exe -> Удалить Сервис);
- 3) удаление ПО управления «Аккорд-В.» с АРМ АБИ с помощью стандартного механизма удаления программ Windows: выбрать Пуск/Панель управления/Программы и компоненты (или «Установка и удаление программ» в Windows 2003)/«Accord-V.» и нажать кнопку <Удалить> (рисунок 54).

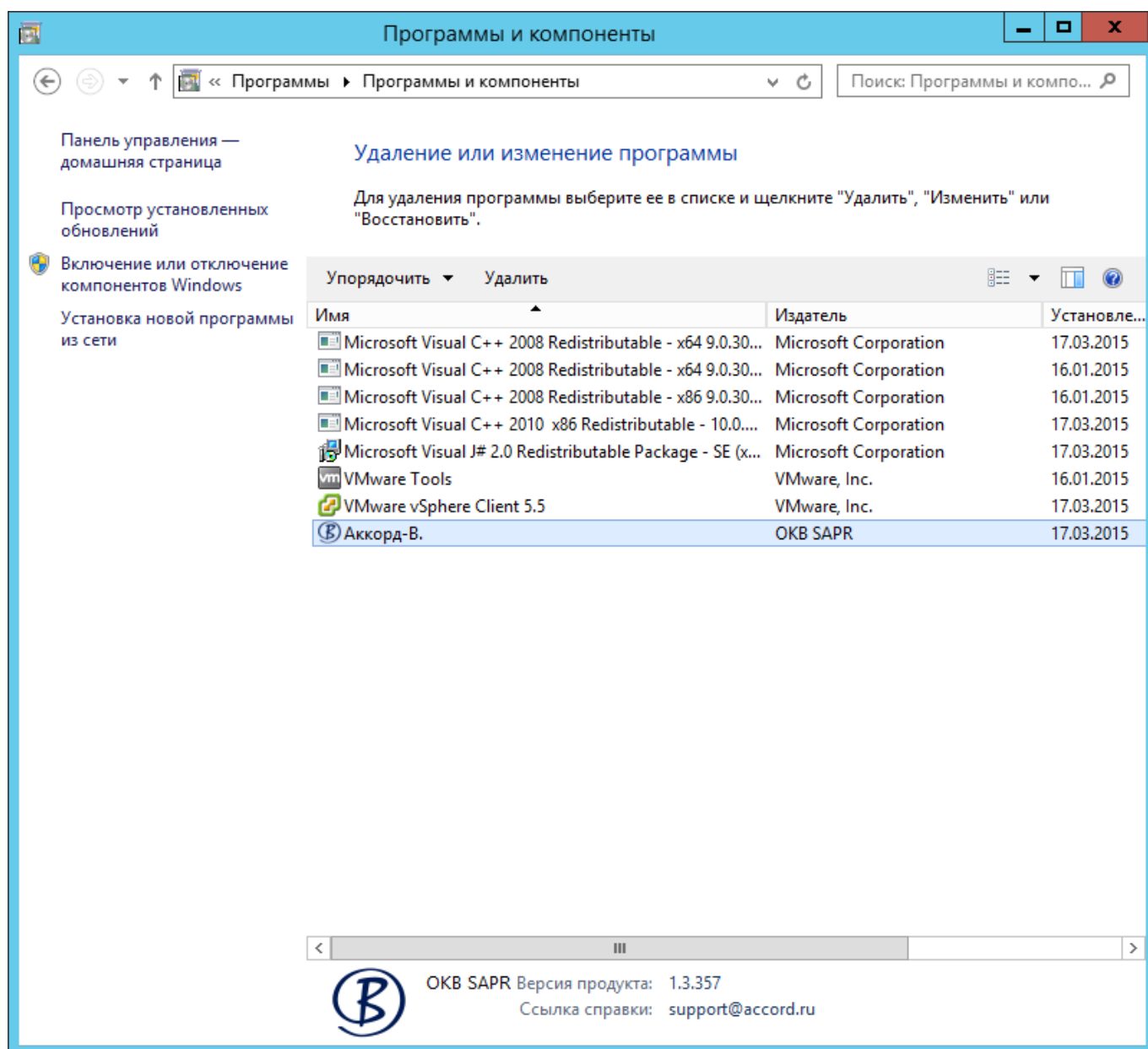


Рисунок 54 - Удаление ПО «Аккорд-В.»

ВНИМАНИЕ! Для полного завершения процесса удаления ПО «Аккорд-В.» необходимо удалить вручную папку C:/Program Files (x86)/OKB SAPR/Accord-V и перезагрузить сервер.

9. Лицензирование

Для работы с СПО «Аккорд-В.» требуется лицензия. Она выдается производителем и поставляется на компакт-диске в составе комплекта поставки продукта или иным способом (файл license-v.lic).

Для формирования Поставщиком файла лицензии необходимы следующие параметры (они должны быть известны перед приобретением лицензии):

1)Срок действия лицензии (устанавливается в соответствии с потребностью Заказчика).

2)Уникальная идентификационная информация средства доверенной загрузки (СЗИ НСД «Аккорд-АМДЗ» или СЗИ НСД «Инаф»), установленного на автоматизированном рабочем месте администратора информационной безопасности инфраструктуры виртуализации. Определить данный параметр можно одним из следующих способов:

а) запустить утилиту «Accord-V.» из комплекта поставки.

Уникальная идентификационная информация средства доверенной загрузки содержится в поле «Серийный номер платы» отображаемого на экране информационного окна (рисунок 55). Данный параметр следует передать Поставщику для создания файла лицензии. В целях предотвращения возникновения ошибок при перепечатаывании идентификационной информации можно установить курсор в указанное поле и выполнить процедуру копирования с использованием стандартного сочетания клавиш (<Ctrl>+<C> и <Ctrl>+<V>).

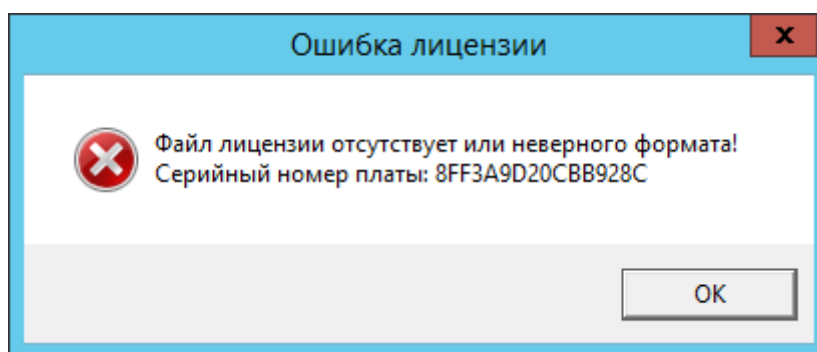


Рисунок 55 – Ошибка лицензии

б) запустить отдельно поставляемую утилиту Key-V-Info.exe. Уникальная идентификационная информация средства доверенной загрузки содержится в появившемся окне «Ключ лицензии». Данный параметр следует передать Поставщику для создания файла лицензии. В целях предотвращения возникновения ошибок при перепечатаывании идентификационной информации можно установить курсор в указанное поле и выполнить процедуру копирования с использованием стандартного сочетания клавиш (<Ctrl>+<C> и <Ctrl>+<V>).

3) Наименование продукта:

- «Accord-V.» – соответствует установке «Аккорд-В.» в качестве отдельного продукта;
- «Segment-V.» – соответствует установке «Сегмент-В.» в качестве отдельного продукта;
- «Accord-V. Enterprise» – соответствует совместному использованию «Аккорд-В.» и «Сегмент-В.».

4) Максимальное количество прокси-серверов (данный параметр учитывается только для «Сегмент-В.»; устанавливается в соответствии с потребностью Заказчика). Добавление в систему прокси-серверов в количестве, превышающем предусмотренное лицензией, невозможно.

5) Максимальное количество CPU в ESXi-серверах инфраструктуры виртуализации (устанавливается в соответствии с потребностью Заказчика). Подключение к инфраструктуре виртуализации, в которой суммарное число процессоров ESXi-серверов превышает заданное в лицензии, невозможно.

6) Максимальное количество виртуальных машин в инфраструктуре виртуализации (данный параметр учитывается только для «Аккорд-В.»; устанавливается в соответствии с потребностью Заказчика). Подключение к инфраструктуре виртуализации, в которой количество виртуальных машин превышает заданное в лицензии, невозможно.

Полученную от Поставщика лицензию (файл license-v.lic) необходимо скопировать в корень папки с установленным ПО управления:

C:\Program Files (x86)\OKB SAPR\Accord-V

Примечание: Лицензии на «Аккорд-В.» и «Сегмент-В.» аналогичны и отличаются наименованием продукта.

Проверка лицензии осуществляется только для утилиты **«Accord-V.» («Segment-V.»)**.

Если проверка не была пройдена (отличается уникальная идентификационная информация средства доверенной загрузки, истек срок действия лицензии, неверна подпись лицензии, превышено допустимое лицензией количество прокси-серверов, ВМ, процессоров ESXi-серверов и т.п.), утилита «Accord-V.» не будет функционировать, но агенты продолжат свою работу.

Продолжение работы станет возможным только после приведения параметров системы в соответствие с лицензией или после приобретения новой лицензии.

Статус лицензии, уникальная идентификационная информация средства доверенной загрузки и дата истечения срока действия лицензии отображаются на вкладке «Помощь» утилиты «Accord-V.» («Segment-V.») (рисунок 56).

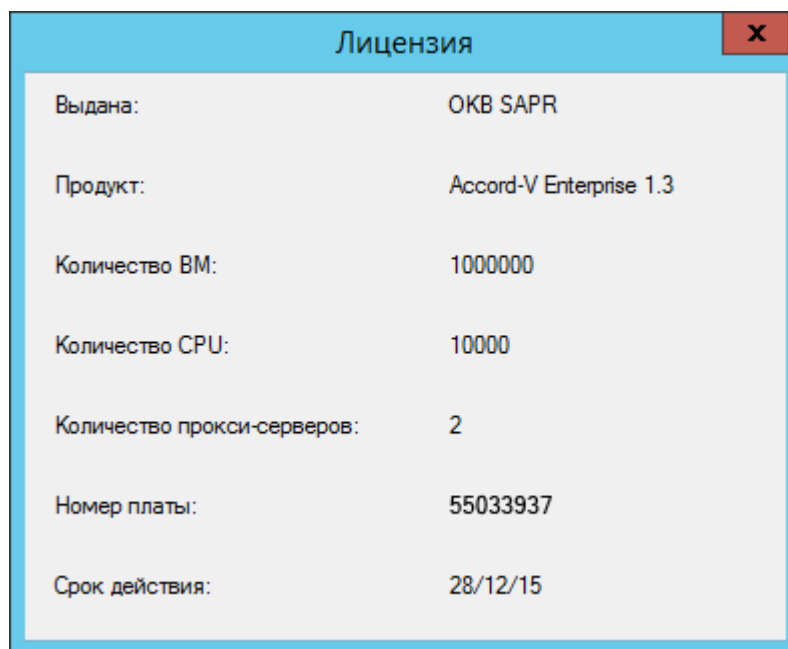


Рисунок 56 - Информация о лицензии

10. Сервисные команды

Сброс базы данных утилиты «Accord-V.»:

C:\Program Files\OKB SAPR\Accord-V\repair.exe -db

Сброс базы данных агента «Аккорд-В.» на ESXi:

/etc/accord-v/accordguard -n

Сброс базы данных сервиса регистрации событий:

C:\Program Files\OKB SAPR\Accord-V\repair.exe -log

Запуск/остановка/перезагрузка сервисов агента «Аккорд-В.» на ESXi:

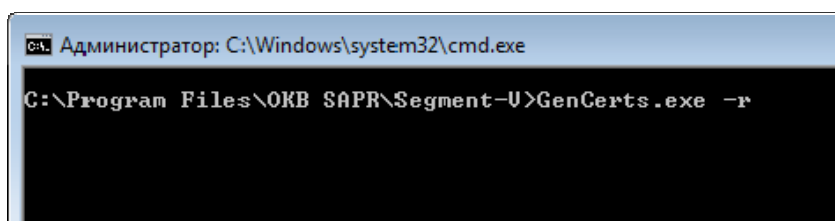
/etc/init.d/accordservice.sh {start|stop|restart}

/etc/init.d/logcollector.sh {start|stop|restart}

Перегенерирование сертификатов

Вызвать в папке с установленным ПО управления исполняемый файл GenCerts.exe:

- с параметром "-r" – для создания корневого сертификата;
- с параметром "-h" – для создания сертификата прокси-сервера.



11. Техническая поддержка

Все вопросы, связанные с поддержкой «Аккорд-В.», Вы можете отправлять по адресу help@okbsapr.ru либо обращаться по телефонам:

+7 (495) 994-49-96,

+7 (495) 994-49-97,

+7 (926) 235-89-17,

+7 (926) 762-17-72.