ОКБ АПР ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс «Аккорд-В.»
(версия 1.3)

Руководство администратора безопасности информации

11443195.4012.028 90

Листов 44

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством администратора безопасности программно-аппаратного комплекса СЗИ НСД «Аккорд-В.» v.1.3 (далее по тексту – ПАК «Аккорд-В.», либо «Аккорд-В.», либо комплекс), предназначенного для защиты инфраструктуры виртуализации на основе VMware vSphere 5.0, VMware vSphere 5.1, VMware vSphere 5.5, VMware vSphere 6.0, VMware vSphere 6.5.

Документ предназначен для администратора безопасности информации – должностного лица, обладающего знаниями и полномочиями, достаточными для того чтобы контролировать безопасность инфраструктуры виртуализации VMware vSphere.

В документе приведены рекомендации по организации защиты инфраструктуры виртуализации с использованием средств комплекса «Аккорд-В.».

Перед началом эксплуатации ПАК «Аккорд-В.» рекомендуется внимательно ознакомиться с содержанием полного комплекта эксплуатационной документации, а также нормативными и методическими документами, регулирующими обеспечение информационной безопасности, включая политику безопасности информации предприятия или организации, эксплуатирующей комплекс.

Процесс установки и первичной настройки комплекса описан в «Руководстве по установке». «Руководство администратора» содержит описание дополнительных настроек, которые будут полезны в процессе дальнейшего администрирования комплекса.

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

СОДЕРЖАНИЕ

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 ВИ (или АВИ) – администратор виртуальной инфраструктуры, привилегированный пользователь - должностное лицо, отвечающее за настройку и обслуживание виртуальной инфраструктуры.

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 комплекса

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа – «Аккорд-В.» предназначен для защиты инфраструктур виртуализации, построенных на базе платформ виртуализации:

- VMware vSphere 5.0;
- VMware vSphere 5.1;
- VMware vSphere 5.5;
- VMware vSphere 6.0;
- VMware vSphere 6.5.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД на основе:

- применения персональных идентификаторов пользователей;
- применения парольного механизма;
- блокировки загрузки операционной системы со съемных носителей информации;
- контроля целостности технических и программных средств и компонентов ПЭВМ (АС) (файлов общего, прикладного ПО и данных), выполняемого до ее запуска;
- контроля целостности программных компонентов ВМ (файлов общего, прикладного ПО и данных), выполняемого до ее запуска;
- обеспечения режима доверенной загрузки установленных в ПЭВМ (АС) и ВМ операционных систем, использующих любую из файловых систем: FAT 12, FAT 16, FAT 32, NTFS, HPFS, FreeBSD, Ext2FS, Sol86FS, QNXFS, MINIX, VMFS *(для ВМ: NTFS/EXT2/EXT3/EXT4)*.

1.2. Состав ПАК «Аккорд-В.»

ПАК «Аккорд-В.» представляет собой комплекс программных и аппаратных средств, который предназначен для защиты инфраструктуры виртуализации.

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

ПАК «Аккорд-В.» состоит из аппаратных и программных средств.

1.2.1. Аппаратные средства

В состав аппаратной части ПАК «Аккорд-В.» входит аппаратная часть «Аккорд-АМДЗ» (ТУ 4012-006-11443195-97, ТУ 4012-006-11443195-2005, ТУ 4012-038-11443195-2011)[1], предназначенная для защиты ESXi, vCenter (если он физический), АРМ АБИ/АВИ, а также, дополнительно, для защиты клиентских рабочих мест.

Контроллер «Аккорд-АМДЗ» устанавливается:

- на АРМ АБИ/АВИ;
- на vCenter (если он не является виртуальной машиной);
- на каждый ESXi-сервер;
- на клиентские рабочие места. Контроллер «Аккорд-АМДЗ» устанавливается на клиентские рабочие места, если требуется обеспечить доверенную загрузку установленной на них операционной системы. Контроллер «Аккорд-АМДЗ», устанавливаемый на клиентском рабочем месте, не поставляется в базовой комплектации ПАК СЗИ НСД «Аккорд-В.» и приобретается отдельно.

Модификация контроллера «Аккорд-АМДЗ» оговаривается при поставке комплекса.

1.2.2. Программные средства

Программные средства ПАК «Аккорд-В.» включают в себя:

1) модули СПО «Аккорд-В.»:

а) *ПО управления комплексом,* устанавливаемое на АРМ АБИ, включающее в себя 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);

2) модули разграничения доступа для ОС с vCenter (если он установлен на ОС Windows), гостевых ОС виртуальных машин, а также,

---

[1)] 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, для ОС АРМ АБИ/АВИ и клиентских рабочих мест (не являющихся виртуальными машинами):

а) *модуль «Аккорд-Win64 TSE»,* устанавливаемый в ОС с vCenter (если он установлен на ОС Windows), предназначенный для разграничения доступа к ресурсам ОС со стороны АБИ и АВИ;

б) *модуль «Аккорд-Win32 TSE» / «Аккорд-Win64 TSE» (СПО «Аккорд-ТС» и СПО «Аккорд-ТК»),* устанавливаемый в ОС ВМ семейства Windows, предназначенный для разграничения доступа пользователей к ресурсам ВМ и, в случае необходимости, обеспечивающий возможность удаленного подключения к ВМ с клиентских рабочих мест.

Дополнительно может использоваться ПО ПАК «ПИ ШИПКА» (не входит в комплект поставки ПАК «Аккорд-В.») – устанавливается в случае если в качестве персонального идентификатора при работе с СПО разграничения доступа используется ПИ ШИПКА. ПО ПАК «ПИ ШИПКА» используется для проведения операций инициализации и форматирования ПИ ШИПКА.

1.3. Технические условия применения комплекса

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

- наличие инфраструктуры виртуализации, построенной на базе одной из поддерживаемых платформ виртуализации, список которых приведен в подразделе 1.1;
- 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)[1].

2. Установка и настройка компонентов комплекса

Установка и первичная настройка компонентов ПАК «Аккорд-В.» проводится в соответствии с положениями «Руководства по установке» (11443195.4012.028-98), входящего в состав комплекта поставки комплекса.

[1)] Данные компоненты включены в комплект поставляемого ПО ПАК «Аккорд-В.»

3. Разделение должностных обязанностей в рамках роли администратора ПАК «Аккорд-В.»

При работе с ПАК «Аккорд-В.» является возможным разделение должностных обязанностей в рамках роли администратора ПАК «Аккорд-В.». Например, может использоваться следующий принцип разделения:

1) администрирование аппаратной части и модулей разграничения доступа, входящих в комплект поставки ПАК «Аккорд-В.» – подробнее см. раздел 4 настоящего руководства;

2) администрирование модулей СПО «Аккорд-В.» – подробнее см. «Руководство по установке» и раздел 5 настоящего руководства.

4. Администрирование аппаратной части и модулей разграничения доступа

Процедуры администрирования аппаратной части («Аккорд-АМДЗ») и модулей разграничения доступа «Аккорд-Win32 TSE» / «Аккорд-Win64 TSE» / «Аккорд-X» / «Аккорд-XL» описаны в соответствующих разделах документации, входящей в комплект поставки комплексов:

- «Аккорд–АМДЗ»: см. «Руководство по установке» (11443195.4012-038 98), «Руководство администратора» (11443195.4012-038 90);
- «Аккорд-Win32»: «Руководство по установке» (11443195.4012-036 98), «Руководство администратора» (11443195.4012-036 90);
- «Аккорд-Win64»: «Руководство по установке» (11443195.4012-037 98), «Руководство администратора» (11443195.4012-037 90);
- «Аккорд-X»: «Руководство администратора» (11443195.4012-026 90).

ВНИМАНИЕ! При работе с «Аккорд-АМДЗ» на ESX-серверах и ПО разграничения доступа на виртуальных машинах необходимо учитывать следующее принципиальное обстоятельство:

ПО разграничения доступа, устанавливаемое на ВМ, идентично ПО разграничения доступа, устанавливаемому на физические АРМ, за исключением того, что в процессе функционирования модуль в ВМ не синхронизируется с контроллером «Аккорд-АМДЗ».

5. Администрирование модулей СПО «Аккорд-В.»

5.1. Общие сведения

ВНИМАНИЕ! Информация, необходимая для установки и первоначальной настройки комплекса «Аккорд-В.», содержится в «Руководстве по установке». Настоящее руководство содержит описание дополнительных настроек ПО «Аккорд-В.», которые могут понадобиться в процессе дальнейшей эксплуатации.

Для администрирования модулей СПО «Аккорд-В.» используются следующие компоненты управления:

- «Accord-V.» – утилита управления комплексом «Аккорд-В.» (подробнее см. «Руководство по установке» и подраздел 5.2 настоящего руководства);
- «LogViewer-V.» – утилита просмотра зарегистрированных событий (подробнее см. «Руководство по установке» и подраздел 5.3 настоящего руководства);
- «Installer-V.» – утилита для установки агентов «Аккорд-В.» на ESXi (подробнее см. «Руководство по установке») и перегенерации сертификатов (подробнее см. подраздел 5.5.1 настоящего руководства).

5.2. Работа с утилитой управления комплексом «Accord-V.»

5.2.1. Начало работы с утилитой

Для начала работы с утилитой управления комплексом следует на АРМ АБИ запустить с правами администратора утилиту **«Accord-V.»** (Trusted Startup Module) и выполнить процедуру авторизации АБИ в системе (подробнее см. соответствующий подраздел «Руководства по установке» (11443195.4012.028 98)).

После авторизации на экран выводится главное окно утилиты управления комплексом (рисунок 1), содержащее на панели задач ряд кнопок, подробные сведения о которых отражены в таблице 1.

Таблица 1 - Описание элементов панели задач главного окна утилиты «Accord-V.»

Название кнопки	Назначение	Примечание
<Подключить>	подключение к агенту «Аккорд-В» на ESXi, с которым не было установлено соединение при включении «Accord-V.»	подробнее см. 5.2.2
<Миграция>	настройка ESXi серверов, на которые разрешено мигрировать данной ВМ (разрешено включаться)	подробнее см. п. «Настройка доверенной загрузки ВМ» «Руководства по установке» (11443195.4012.028 98)
<Поставить на контроль>	установка на контроль необходимых элементов ВМ	подробнее см. п. «Настройка доверенной загрузки ВМ» «Руководства по установке» (11443195.4012.028 98)
<Добавить группу>	создание новой группы	подробнее см. пп. «Работа с группами» в пункте «Настройка доверенной загрузки ВМ» «Руководства по установке» (11443195.4012.028 98)
<Удалить группу>	удаление группы	
<Добавить в группу>	добавление элементов (ВМ) в группу	
<Проверить>	проверка целостности необходимых элементов ВМ	подробнее см. 5.2.4
<Пересчитать>	пересчет КС необходимых элементов ВМ	подробнее см. 5.2.5

Название кнопки	Назначение	Примечание
<Настройка>	настройка политик безопасности хостов	подробнее см. 5.2.6

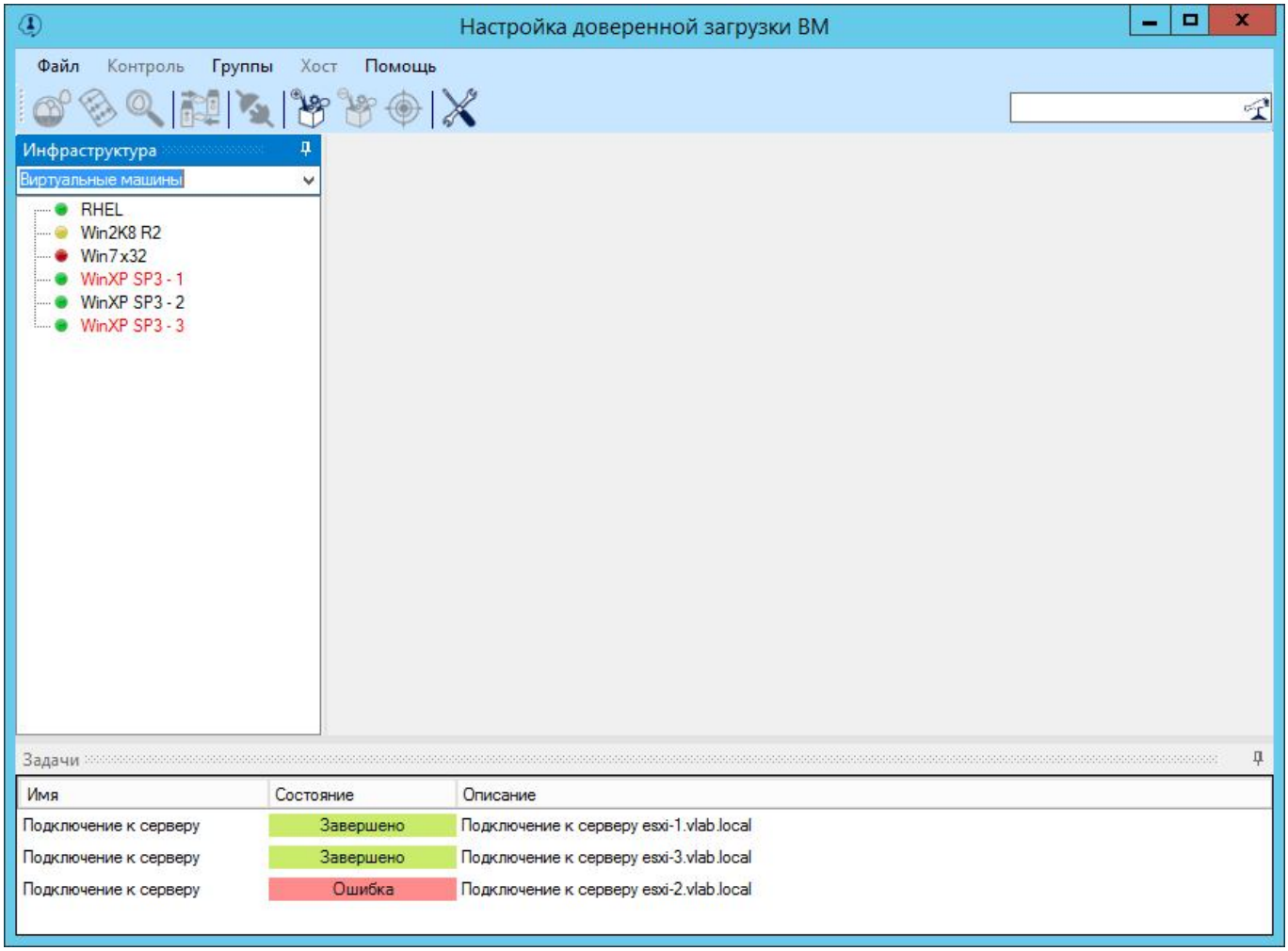


Рисунок 1 - Главное окно утилиты управления комплексом

По умолчанию в главном окне утилиты управления комплексом открывается вкладка инфраструктуры **«Виртуальные машины»**, содержащая список виртуальных машин (рисунок 1). Ее содержимое обновляется автоматически.

Для ВМ возможны следующие состояния:

1) зеленый маркер – ВМ выключена;
2) красный маркер – ВМ включена (операции с ней запрещены);
3) желтый маркер – ВМ в состоянии «Suspend»;
4) имя ВМ отмечено серым – ВМ удалена или конвертирована в шаблон. В случае если ВМ удалена или переведена в шаблон, она помечается серым цветом как неактивная. При следующем включении «Accord-V.» данная ВМ уже не будет отображаться;

5) имя ВМ отмечено красным – недостаточно информации о ВМ (например, ВМ находится в одном из статусов orphaned, inaccessable, 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».

На вкладке инфраструктуры **«Хосты»** главного окна утилиты управления отображается (рисунок 2):

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

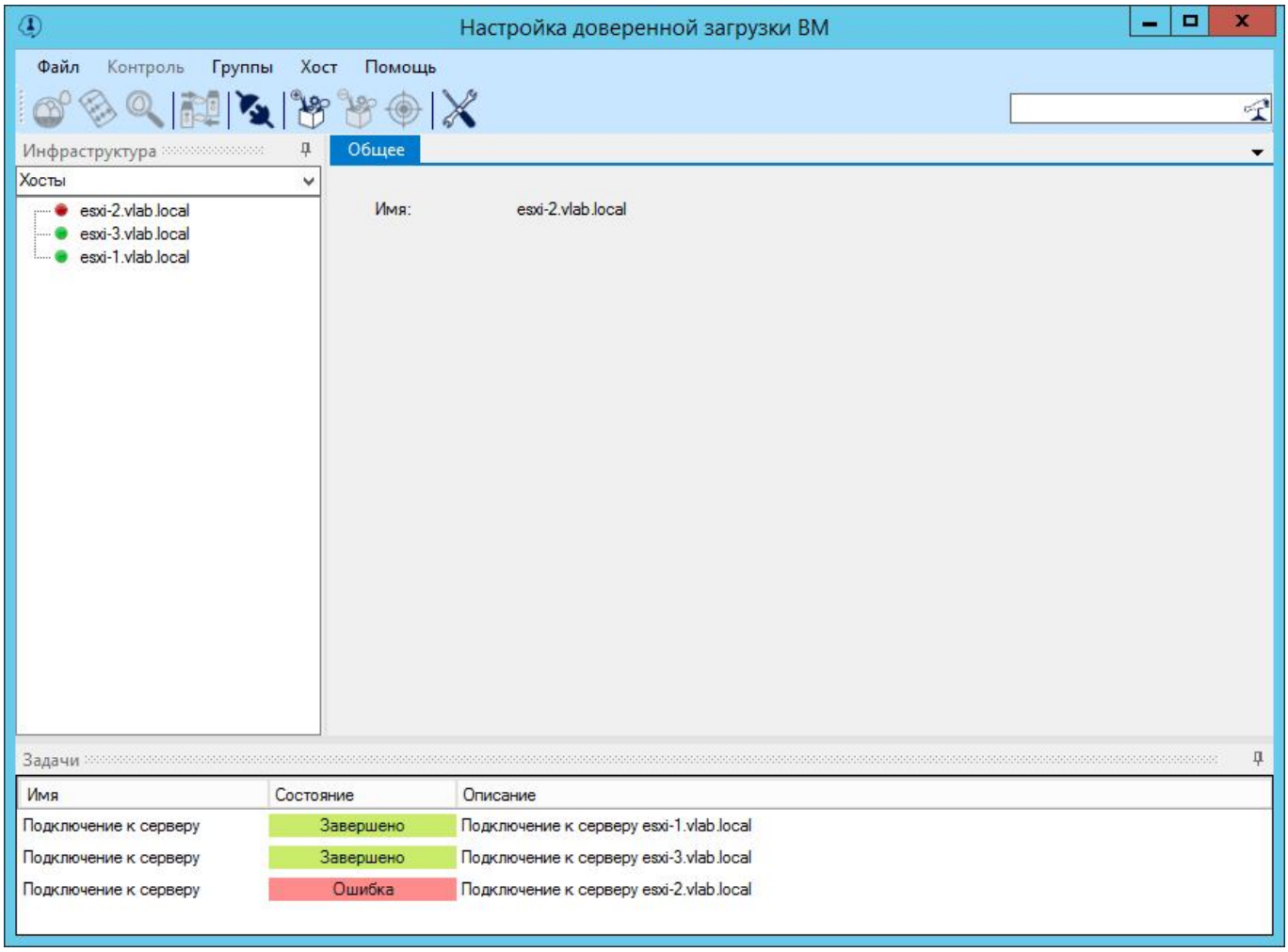


Рисунок 2 - Главное окно утилиты управления комплексом. Инфраструктура хостов

Область задач главного окна утилиты управления комплексом при включении утилиты содержит задачи на подключение к агентам «Аккорд-В.» на ESXi серверах.

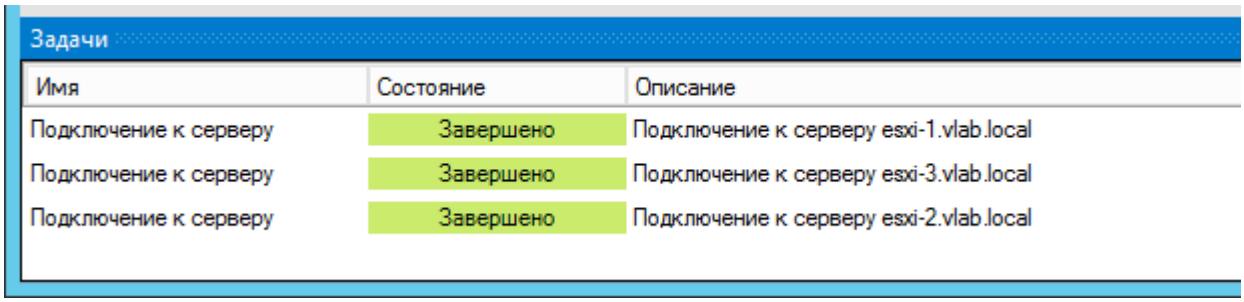


Рисунок 3 – Задачи на подключение к агентам

При этом состояния подключений могут быть выделены различными цветами:

- зеленый – соединение установлено;
- желтый – соединение установлено, но в настройках выбран небезопасный режим работы с ВМ;
- красный – соединение не удалось установить.

5.2.2. Подключение к агенту «Аккорд-В» на ESXi вручную

Если при включении утилиты «Accord-V.» с каким-либо агентом «Аккорд-В» на ESXi не было установлено соединение (состояние подключения выделено красным цветом), следует выяснить причину отсутствия соединения и нажать кнопку <Подключить> (рисунок 4).

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!

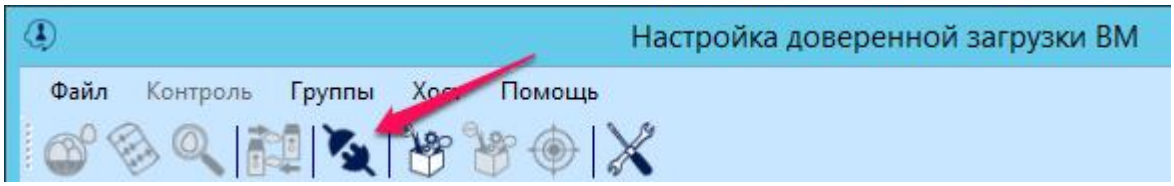


Рисунок 4 - Кнопка <Подключить>

5.2.3. Настройка доверенной загрузки и параметров миграции ВМ

Процесс настройки доверенной загрузки ВМ, в том числе настройка параметров миграции, описан в «Руководстве по установке» (11443195.4012.028-98).

5.2.4. Проверка целостности необходимых элементов

ВНИМАНИЕ! Время, затрачиваемое на проверку целостности, зависит от производительности сервера и размера установленных на контроль файлов.

Целостность установленных на контроль компонентов проверяется каждый раз при старте ВМ.

В ПАК «Аккорд-В.» имеется возможность выполнения проверки целостности установленных на контроль компонентов ВМ по мере возникновения необходимости. Для этого в главном окне утилиты управления следует выбрать нужную ВМ и нажать кнопку <Проверить> (рисунок 5).

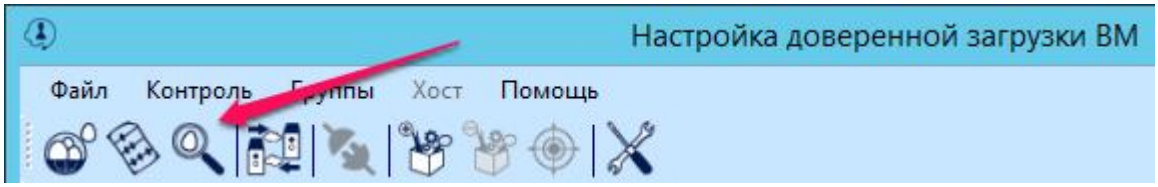


Рисунок 5 - Кнопка <Проверить>

В появившемся далее окне проверки целостности следует выбрать нужные компоненты и нажать кнопку <Проверить> (рисунок 6).

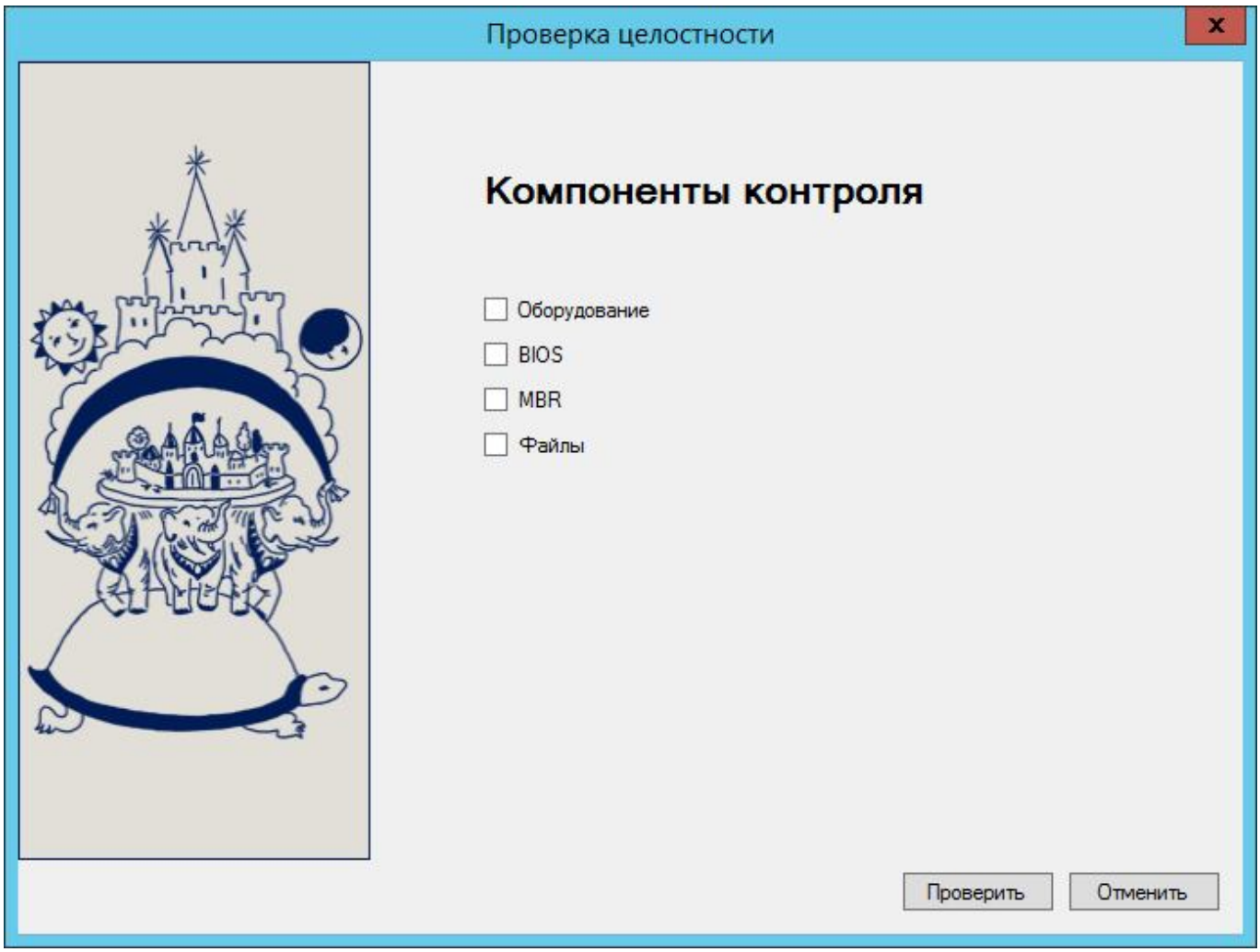


Рисунок 6 - Выбор компонентов для проверки целостности

В левой области появившегося далее окна (рисунок 7) следует выбрать для проверки необходимые файлы гостевой ОС (в том числе при помощи клавиш <Shift> и <Ctrl>) и нажать кнопку <+> для добавления в список проверяемых (правая часть окна).

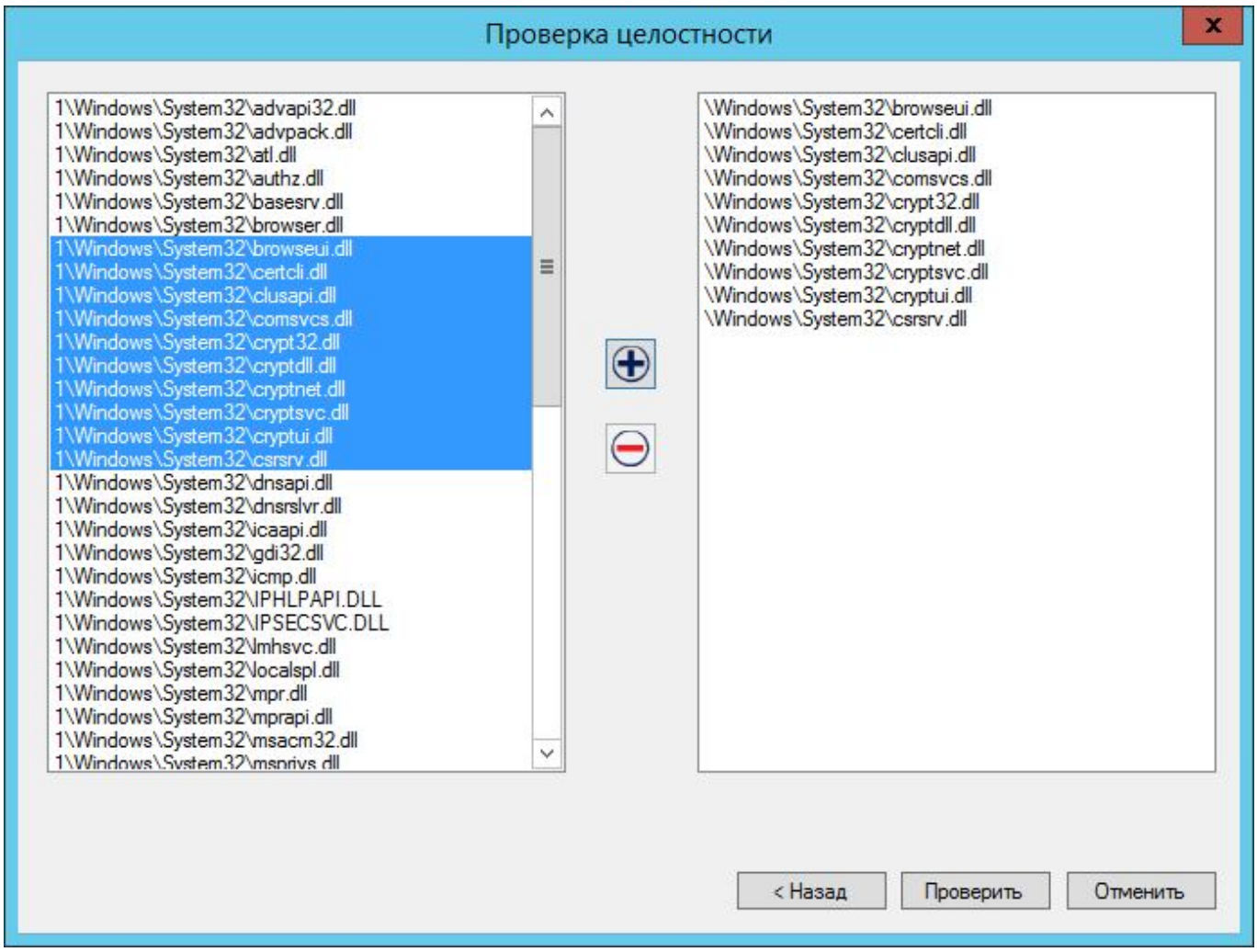


Рисунок 7 - Выбор файлов гостевой ОС для проверки

Далее следует нажать кнопку <Проверить> и дождаться окончания процедуры (рисунок 8).

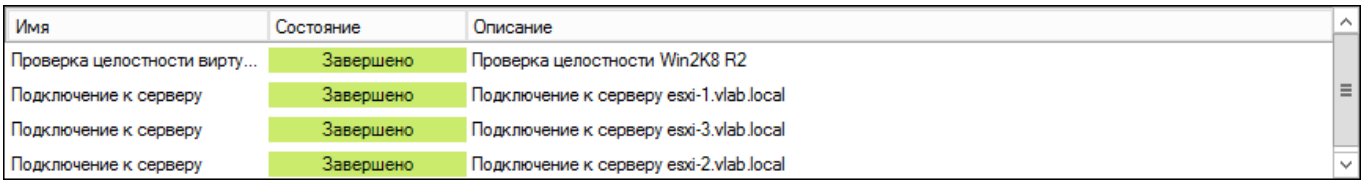


Рисунок 8 - Состояние проверки целостности ВМ в области задач

В случае нарушения целостности какого-либо компонента выбранной ВМ состояние проверки в области задач (рисунок 8) изменяется на «Предупреждение». Список измененных компонентов отображается в сообщениях журнала (утилита «LogViewer-V.») (статус «завершено», если проверка пройдена успешно, статус «ошибка», если сама проверка по какой-либо причине не завершилась успешно).

После выяснения причин изменения файлов необходимо пересчитать КС.

5.2.5. Пересчет КС необходимых элементов

Для пересчета КС необходимых элементов следует в главном окне утилиты управления выбрать нужную ВМ и нажать кнопку <Пересчитать> (рисунок 9).

Рисунок 9 - Кнопка <Пересчитать>

В появившемся далее окне пересчета контрольных сумм следует выбрать нужные компоненты и нажать кнопку <Пересчитать> (рисунок 10).

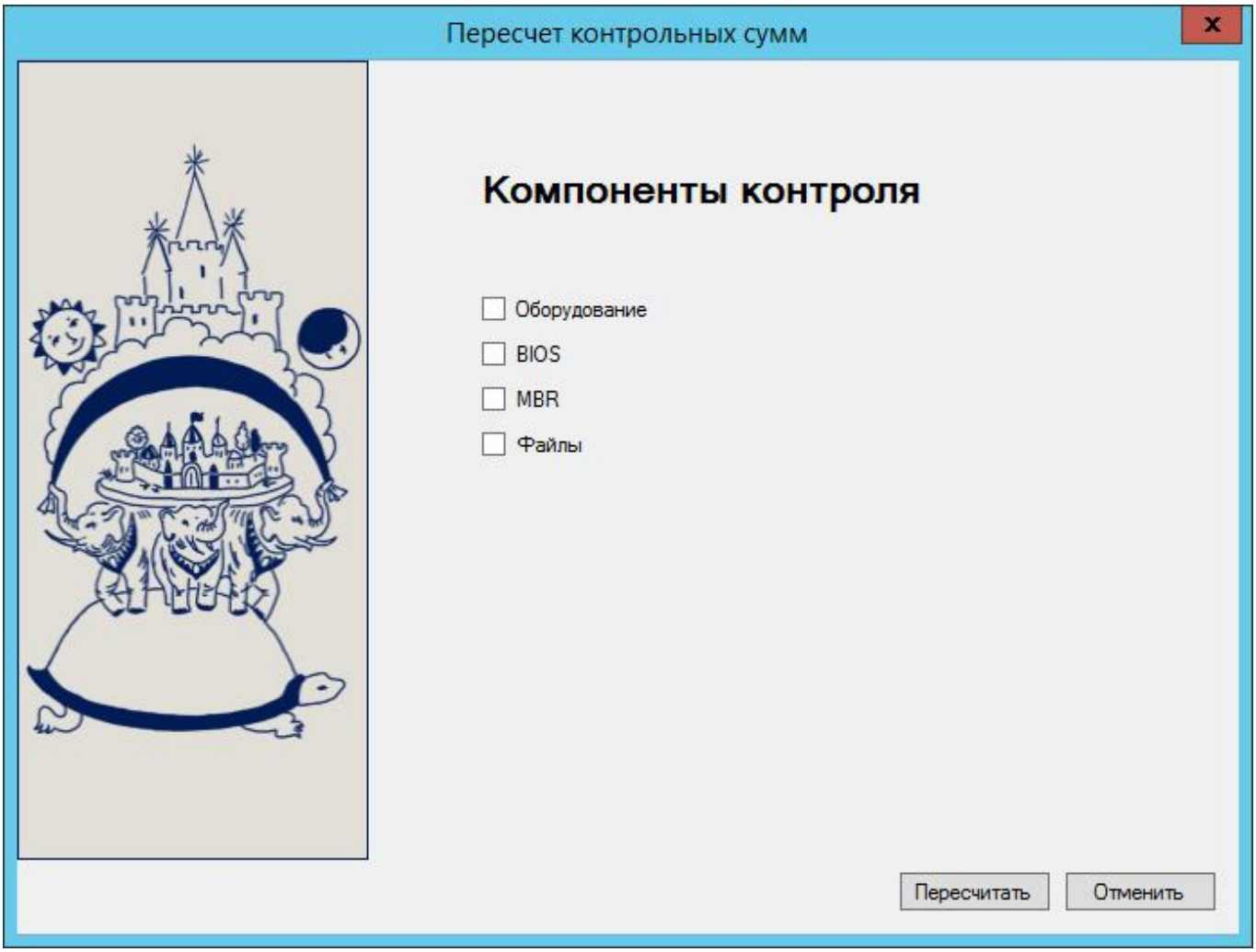


Рисунок 10 - Выбор компонентов для пересчета КС

В левой области появившегося далее окна (рисунок 11) следует выбрать для проверки необходимые файлы гостевой ОС (в том числе при помощи клавиш <Shift> и <Ctrl>) и нажать кнопку <+> для добавления в список проверяемых (правая часть окна).

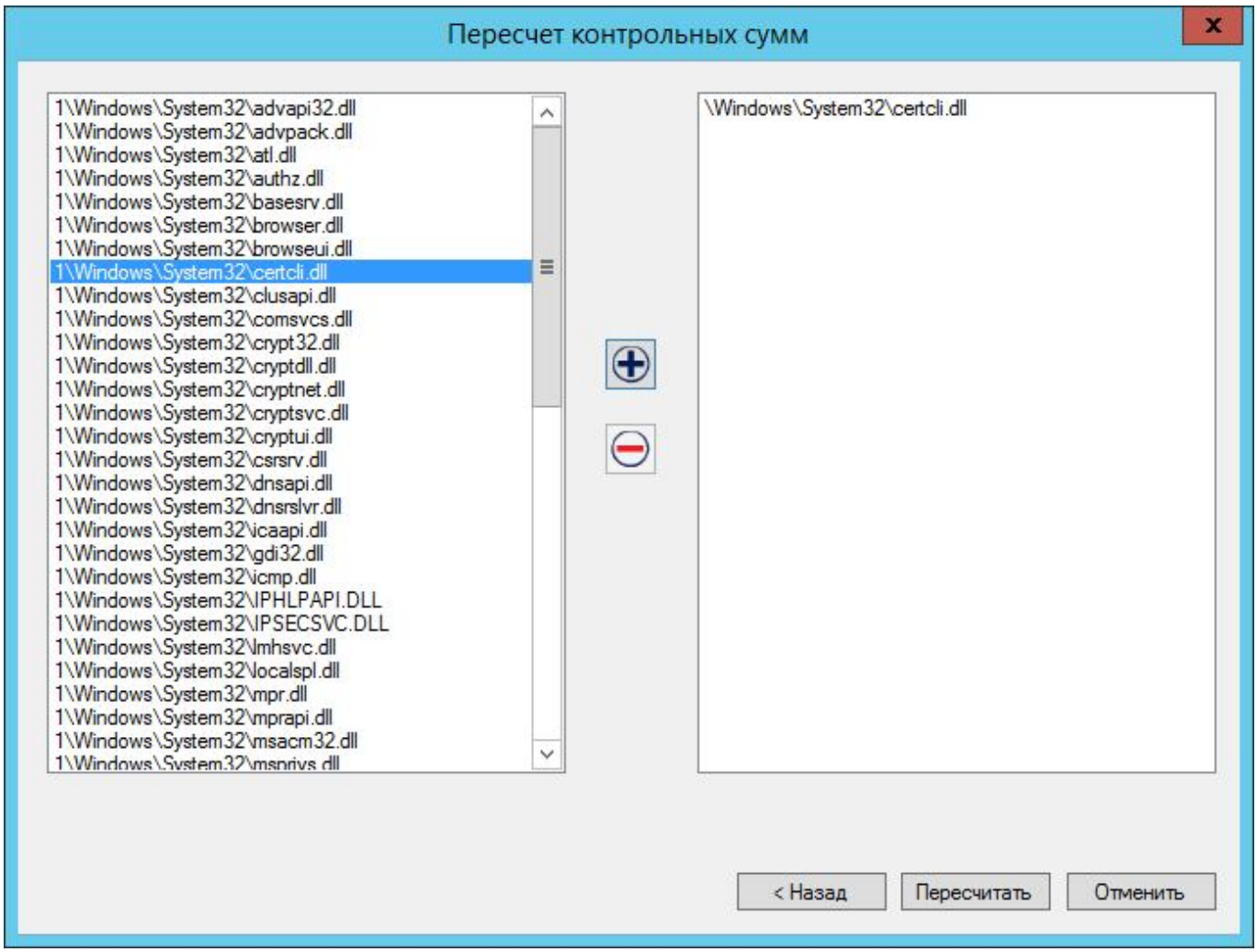


Рисунок 11 - Выбор файлов гостевой ОС для пересчета КС

Далее следует нажать кнопку <Пересчитать> и дождаться окончания процедуры (рисунок 12).

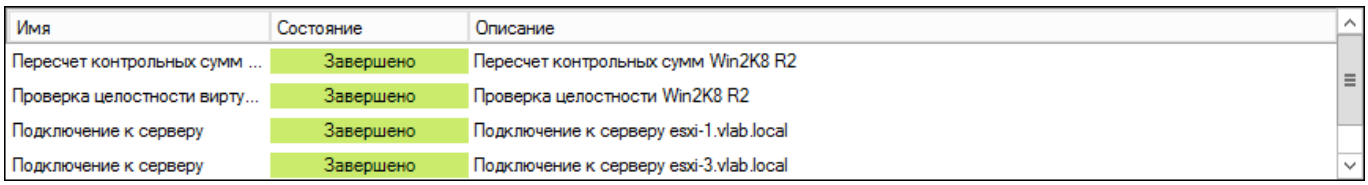


Рисунок 12 - Состояние пересчета КС в области задач

5.2.6. Настройка политик безопасности хостов

Для настройки политик безопасности хостов следует в главном окне утилиты управления комплексом нажать кнопку <Настройка> (рисунок 13).

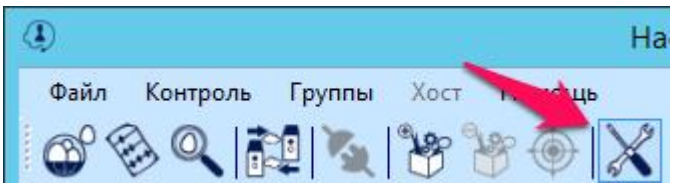


Рисунок 13 - Кнопка <Настройка>

В появившемся далее окне можно выбрать в списке нужный хост и настроить для него:

– *политики включения ненастроенных ВМ* (рисунок 14). После установки ПО включение всех ВМ заблокировано – данная политика установлена в «Accord-V.» по умолчанию. Все ВМ в этот момент считаются **ненастроенными**, т.к. для них в «Аккорд-В.» нет никаких настроек (они отсутствуют в базе данных). После выполнения в «Accord-V.» какой-либо настройки для ВМ (настройка миграции и/или настройка элементов контроля), ВМ всегда будет считаться **настроенной**;

ВНИМАНИЕ! После того как все ВМ настроены, в инфраструктуре могут появляться новые ВМ, которые также попадают в категорию «ненастроенных». Иногда необходимо разрешать этим новым ненастроенным ВМ включаться.

Например, в случае развертывания VDI ВМ (например, XenDesktop) возможны ситуации с созданием промежуточной ВМ (которая затем автоматически удаляется). В таком случае, если поведение для незарегистрированных ВМ будет оставлено как блокирование, операции развертывания будут завершаться ошибкой. В этом случае следует временно устанавливать режим включения ненастроенных ВМ.

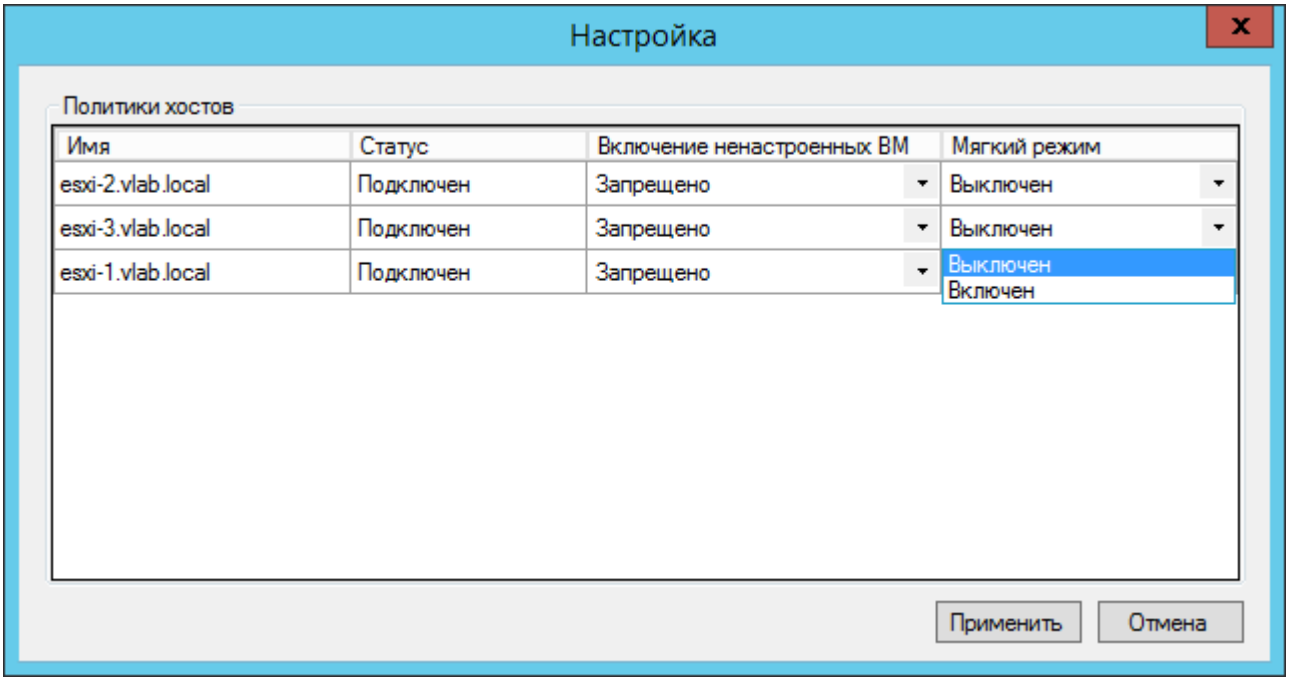


Рисунок 14 - Настройка мягкого режима работы с хостами

– *мягкий режим* (рисунок 15). Установка мягкого режима может потребоваться при отладке настраиваемой системы, когда необходимо

понаблюдать за поведением ПО «Аккорд-В.», но при этом не вносить проблемы в текущую инфраструктуру: все установленные проверки выполняются, но вне зависимости от результата все **настроенные** ВМ включаются.

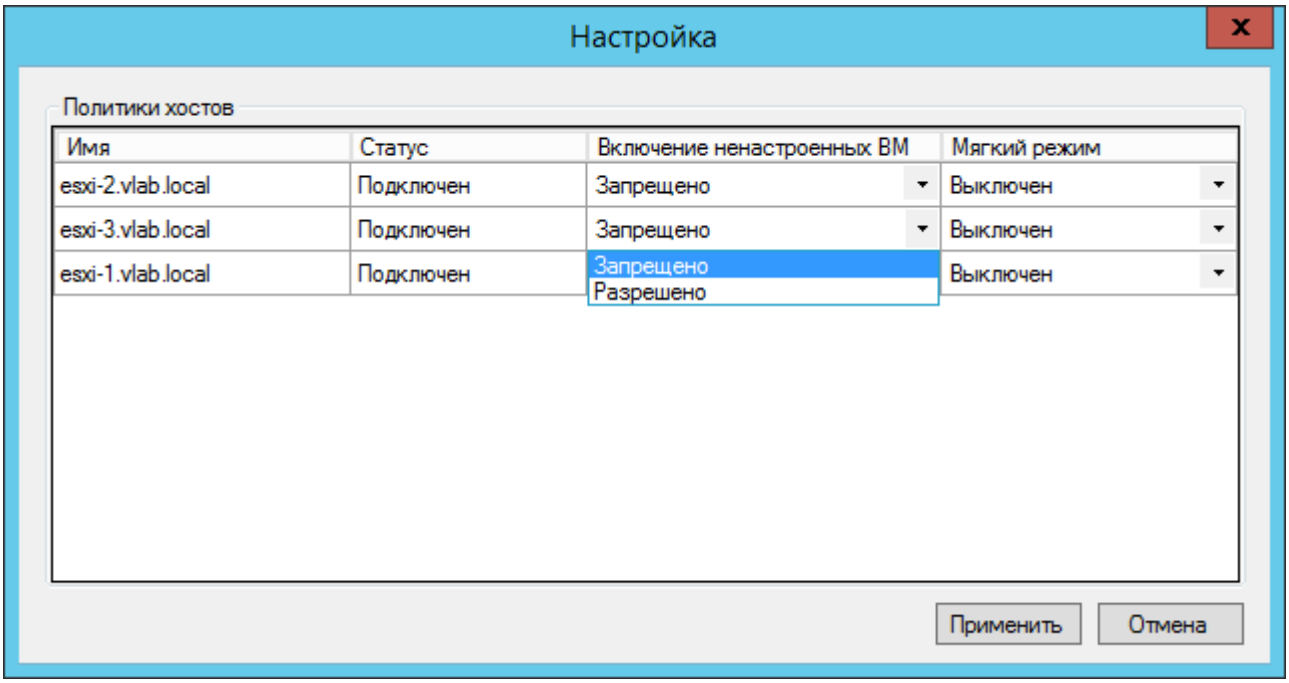


Рисунок 15 - Настройка политики включения ненастроенных ВМ

Включение любого из указанных режимов (включение ненастроенных ВМ или мягкий режим) влияет на сообщения в журнале: они будут иметь статус «Warning»,т.к. такое состояние считается небезопасным. Также в «Accord-V.» при подключении к хостам в этом случае появляются предупреждающие сообщения о небезопасных настройках.

5.3. Работа с сервисом регистрации событий

5.4. Общие сведения

Если в инфраструктуре виртуализации предусмотрено наличие vCenter, сбор событий выполняется с vCenter и агентов «Аккорд-В.» на ESXi. Если vCenter отсутствует, события собираются только с агентов «Аккорд-В.» на ESXi.

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.

ВНИМАНИЕ! Файл конфигурации **Config.xml**, находящийся в корне папки с установленным сервисом регистрации событий, содержит список хостов и vCenter, с которых будут собираться события, и считывается только при запуске сервиса!

Если количество хостов и vCenter увеличилось или изменились их ip-адреса или имена, необходимо обновить данный конфигурационный файл (вручную или скопировав повторно с АРМ АБИ) и перезапустить сервис!

5.4.1. Получение событий

Для того чтобы начать работу с журналом регистрации событий, необходимо запустить с правами администратора ярлык **«LogViewer-V.»** на АРМ с установленным сервисом регистрации событий.

На экран выводится главное окно утилиты просмотра журнала регистрации событий (рисунок 16).

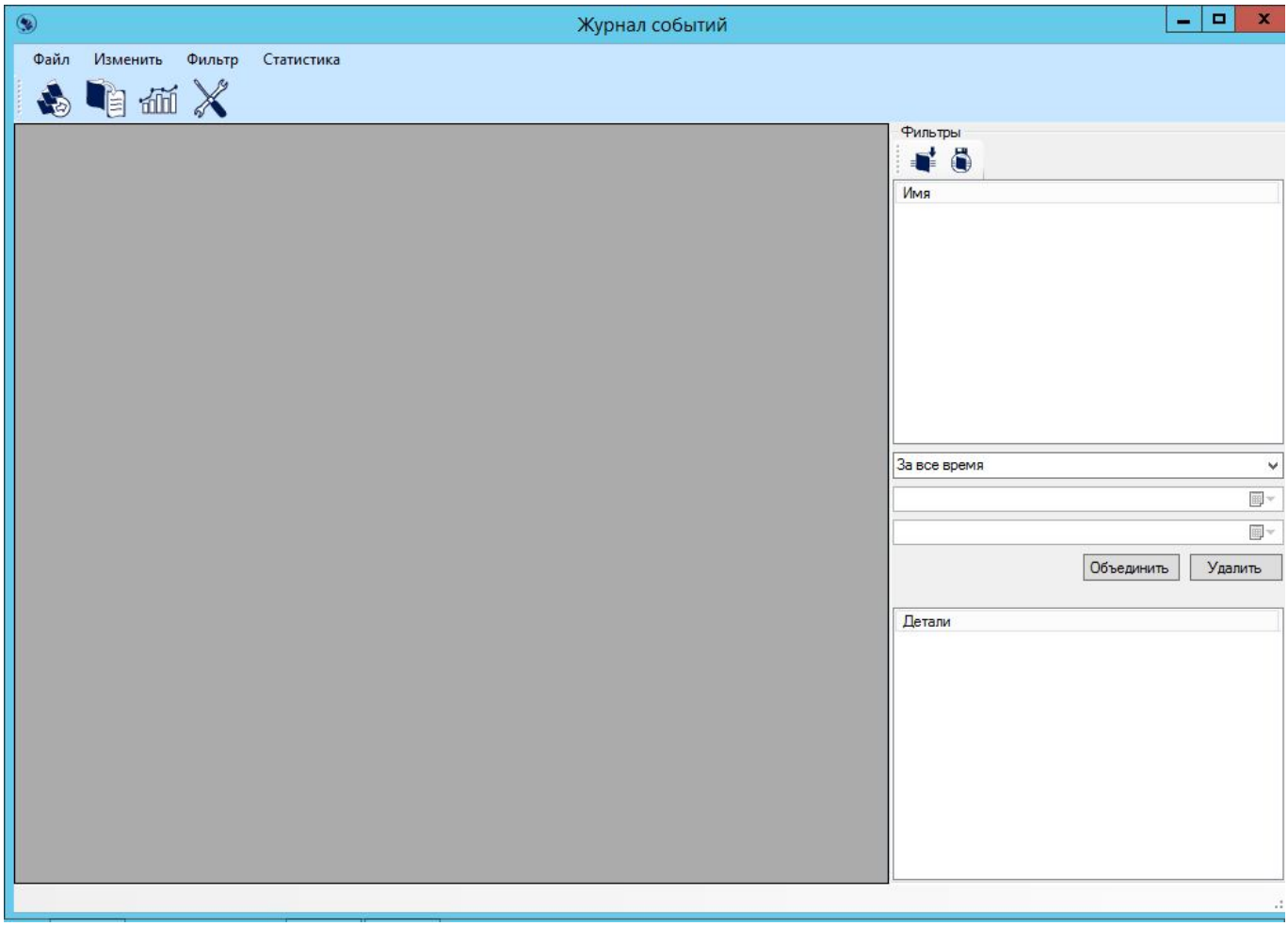


Рисунок 16 - Главное окно утилиты просмотра журнала регистрации событий

Для получения событий в главном окне журнала регистрации событий следует нажать кнопку <Получить события> (либо выбрать пункт меню «Файл»/ «Получить события» или нажать кнопку F5).

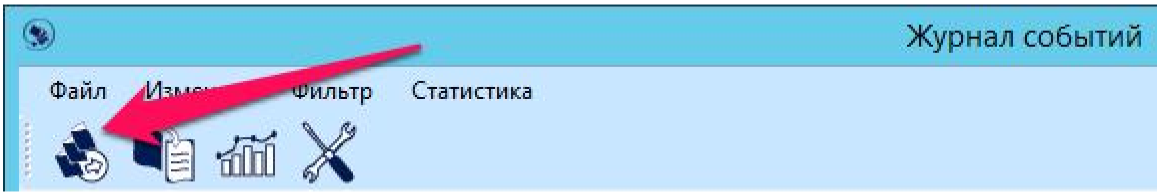


Рисунок 17 – Кнопка <Получить события>

На экран выводится список всех выполненных событий (рисунок 18).

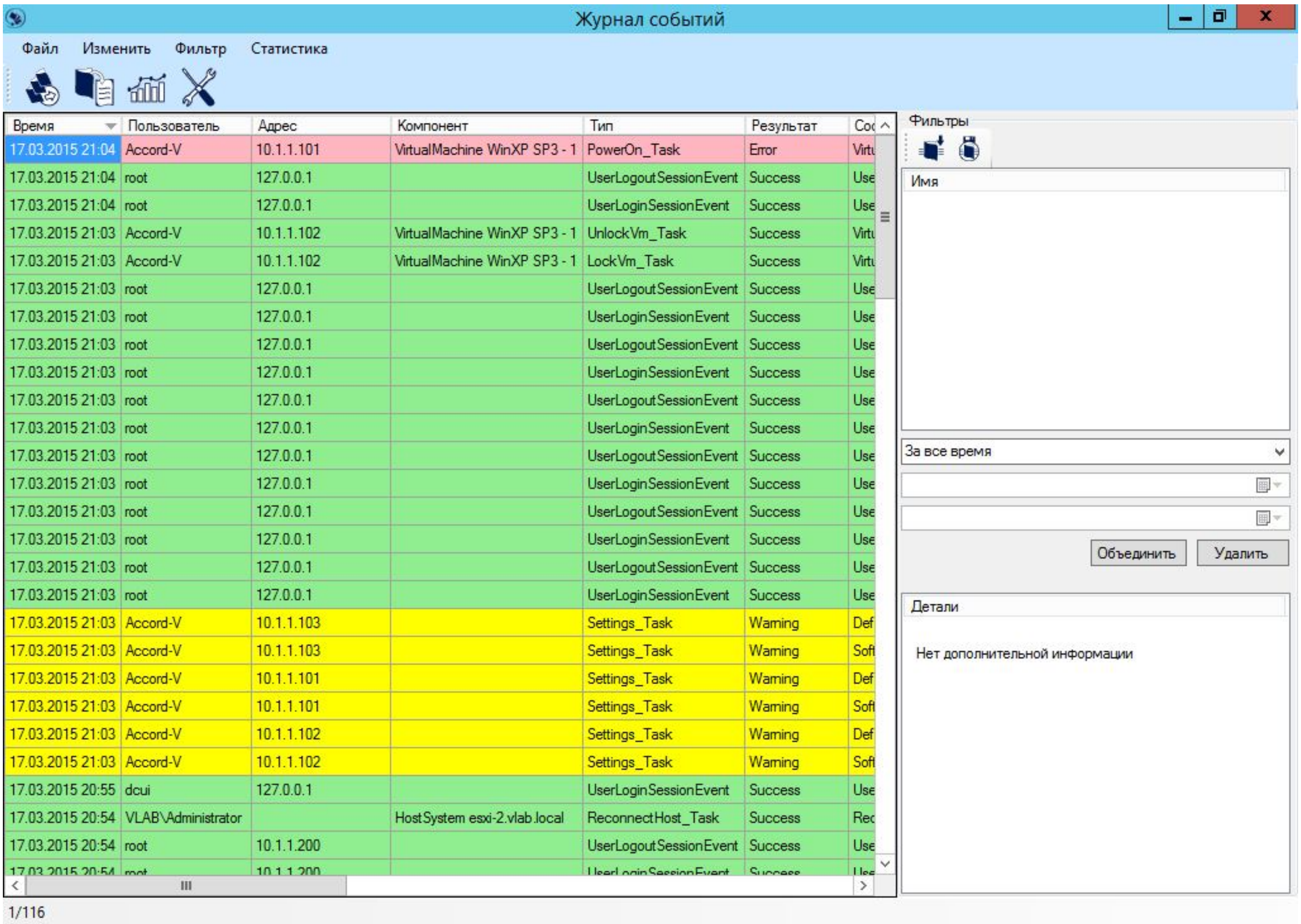
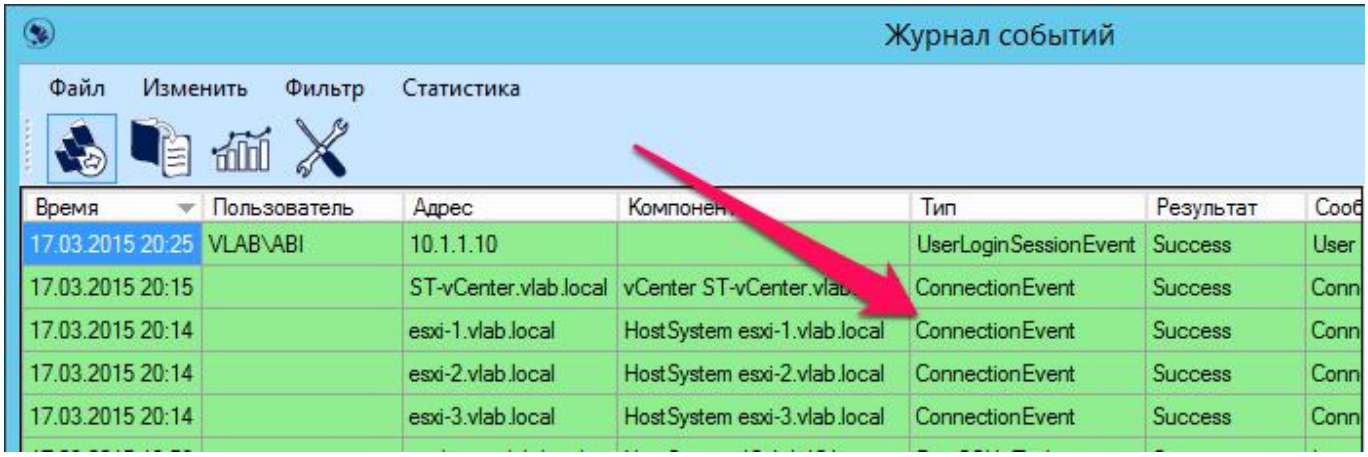


Рисунок 18 – События в главном окне журнала

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. «Руководство по установке» (11443195.4012.028 98)).

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

Для некоторых событий (например, для изменившегося оборудования) доступно расширенное описание по двойному клику мыши (рисунок 19).

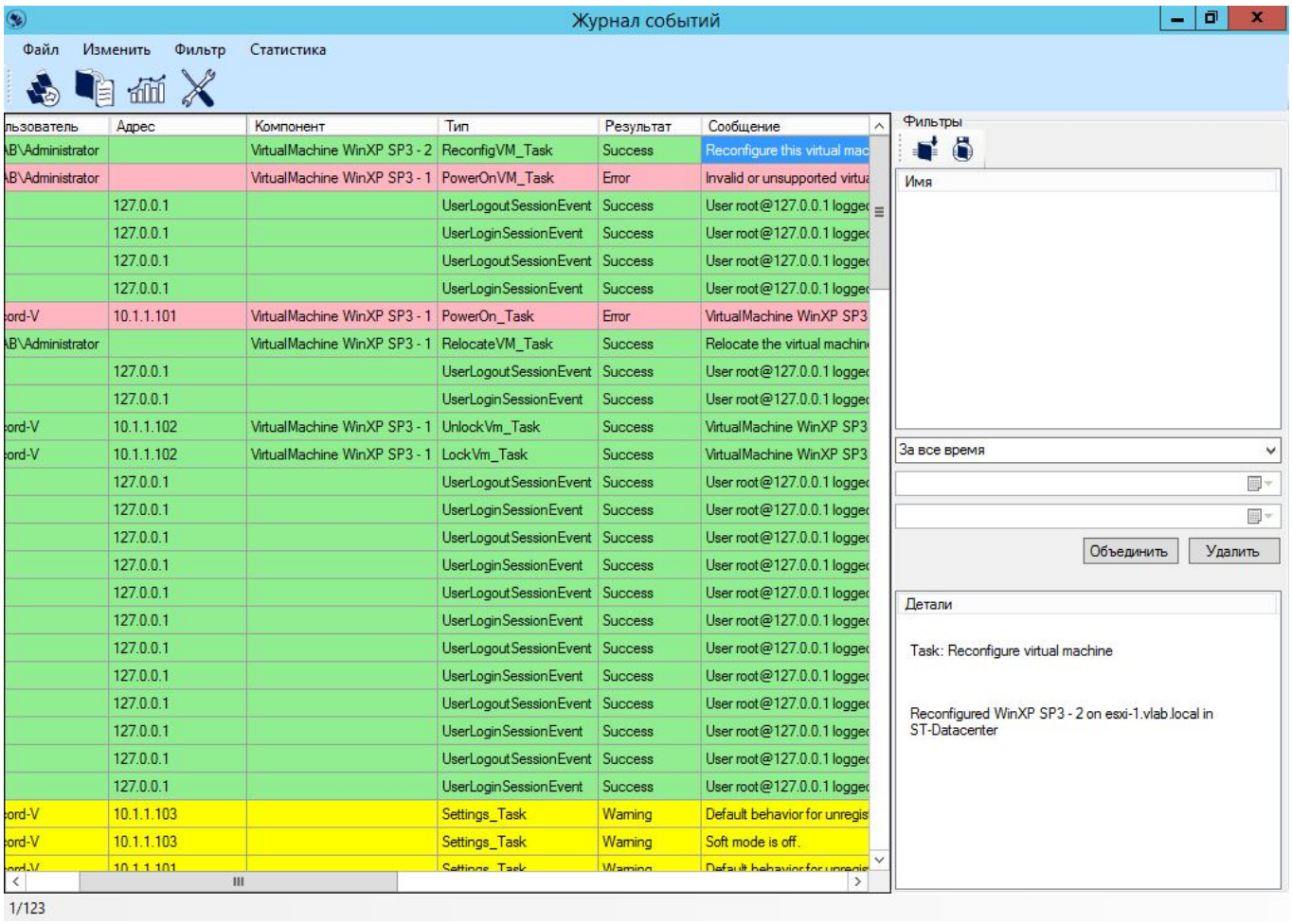


Рисунок 19 – Главное окно журнала регистрации событий

В этом случае следствием двойного щелчка мышью по выбранной строке является вывод на экран окна с подробным описанием события (рисунок 20).

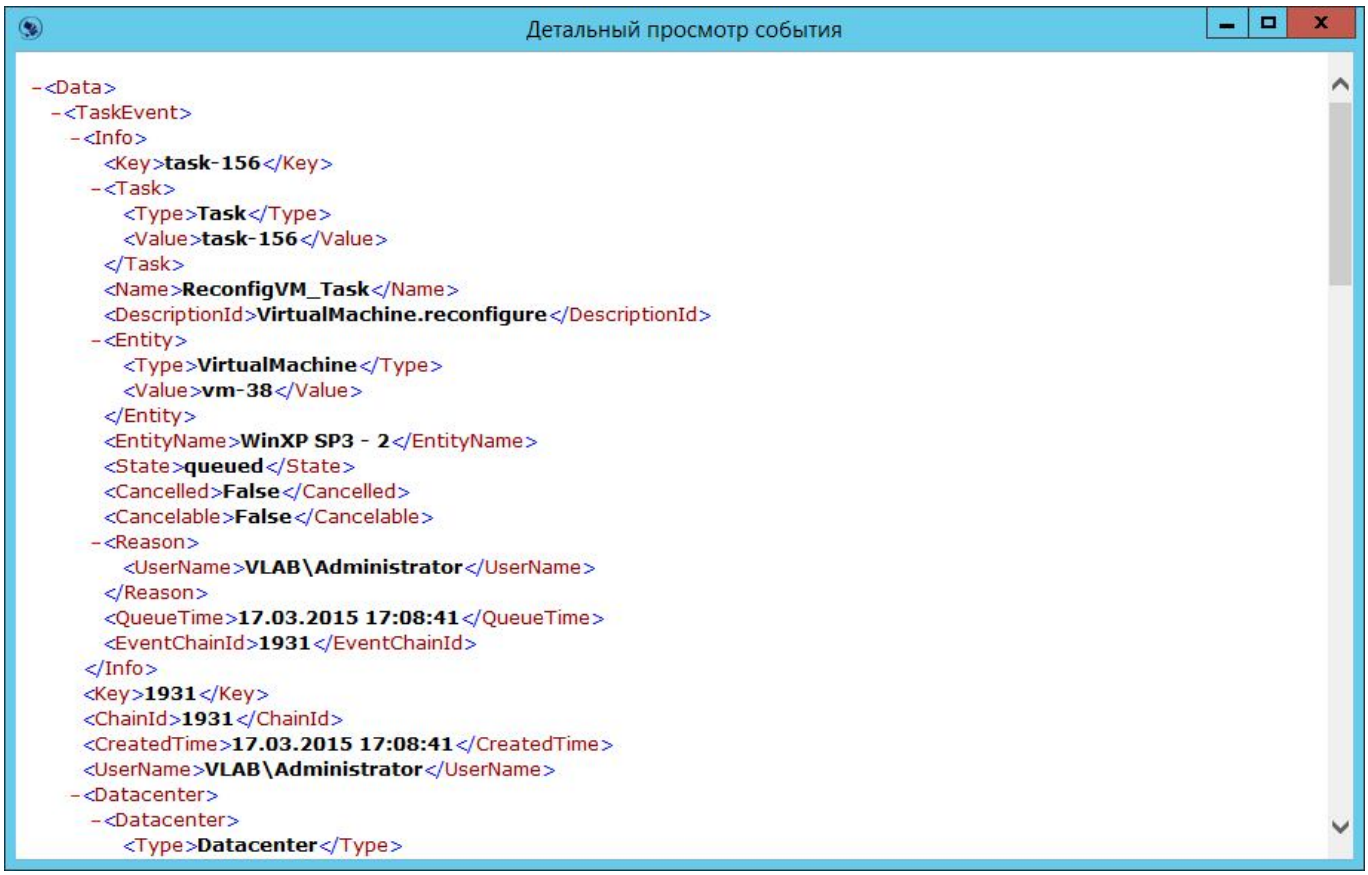


Рисунок 20 – Окно с расширенным описанием события

5.4.2. Работа с фильтрами

5.4.2.1. Общие сведения

Для удобства, в процессе работы с журналом регистрации событий имеется возможность применения различных фильтров для выборки необходимых событий. Это возможно путем перетаскивания мышкой значений из таблицы в поле «Фильтры». Для применения установленных параметров фильтрации необходимо нажать кнопку <F5> или <Получить события>.

В целом логика работы фильтров соответствует законам математической логики Де Моргана.

По умолчанию к фильтрам применяется логическое «И» (например: «инициатор root и IP = 192.168.53.53»).

В случае использования кнопки <Объединить> (рисунок 21) к фильтрам применяется логическое «ИЛИ».

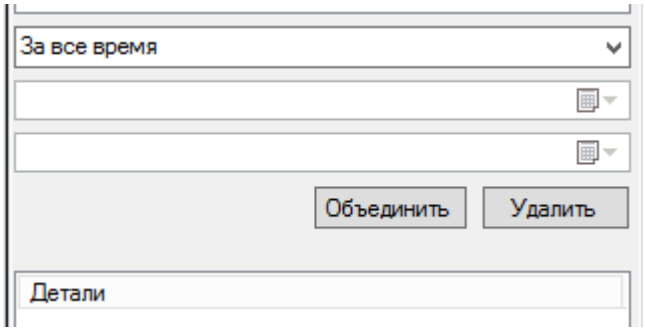


Рисунок 21 - Кнопки <Объединить> и <Удалить>

Для удаления какого-либо фильтра используется кнопка <Удалить> (рисунок 21).

При нажатии правой клавишей мыши на фильтр появляется возможность его инвертировать(рисунок 22).

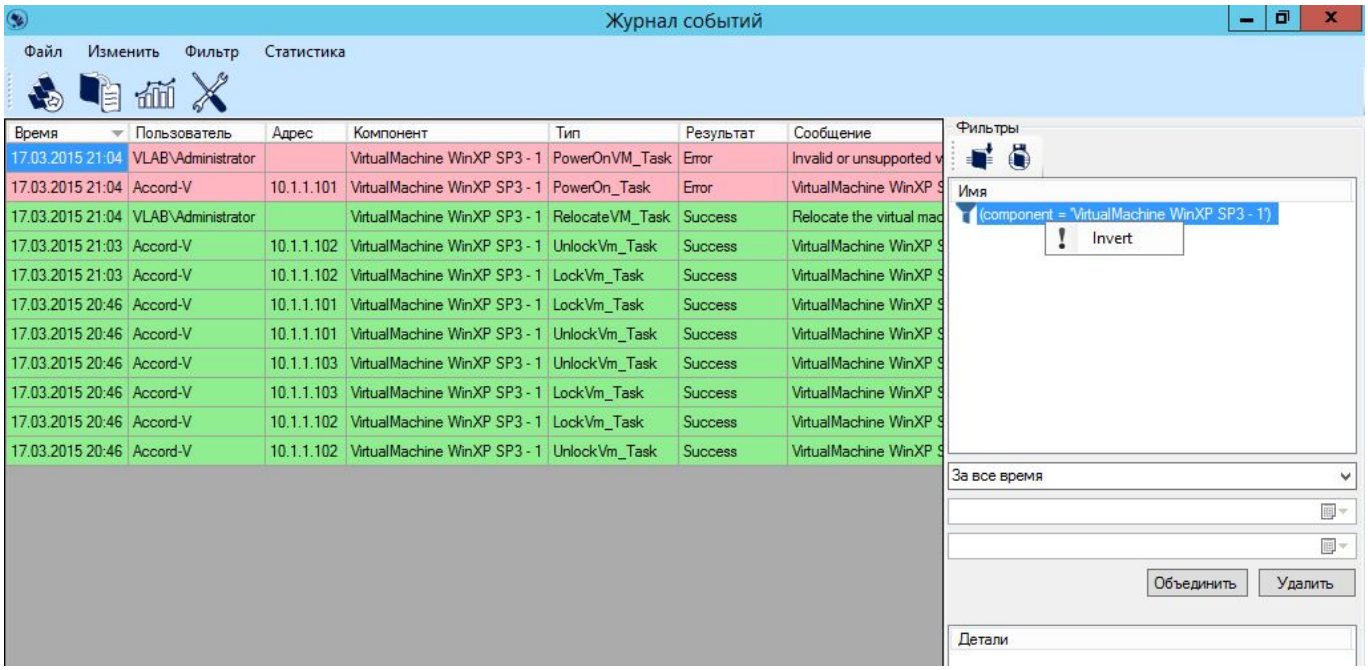


Рисунок 22 – Инвертирование фильтра

Имеется возможность фильтрации событий по времени (рисунок 23).

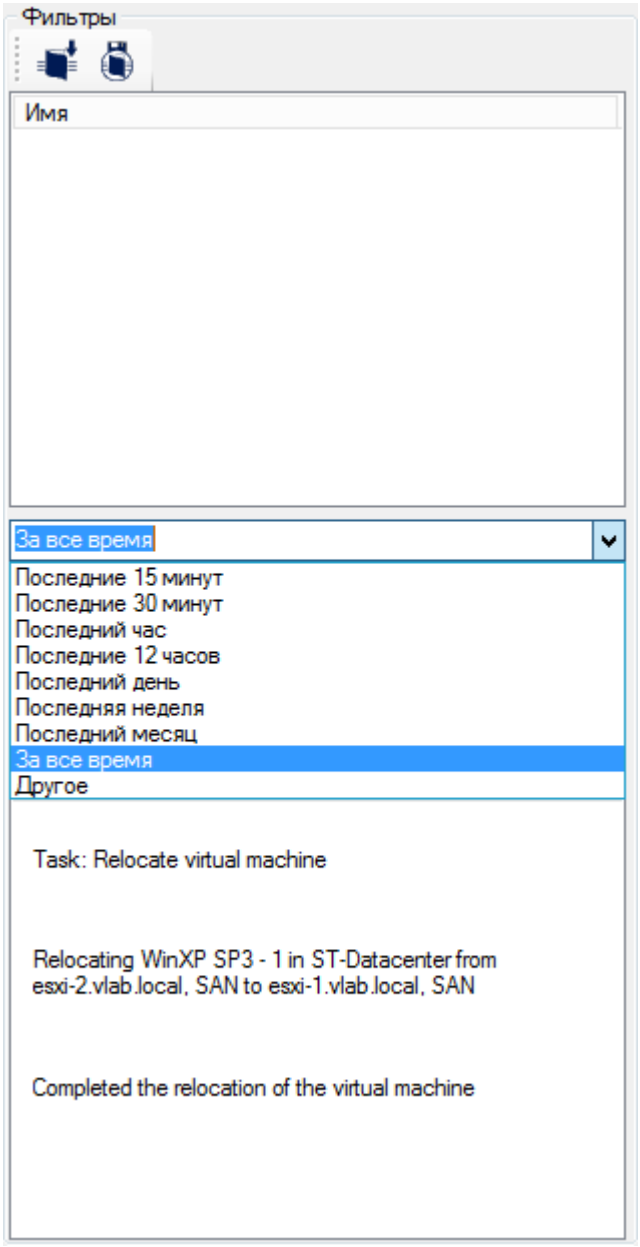


Рисунок 23 - Фильтрация событий по времени

5.4.2.2. Сохранение фильтра в файл

При необходимости фильтр можно сохранить в файл посредством нажатия кнопки <Сохранить фильтр> справа в окне журнала.

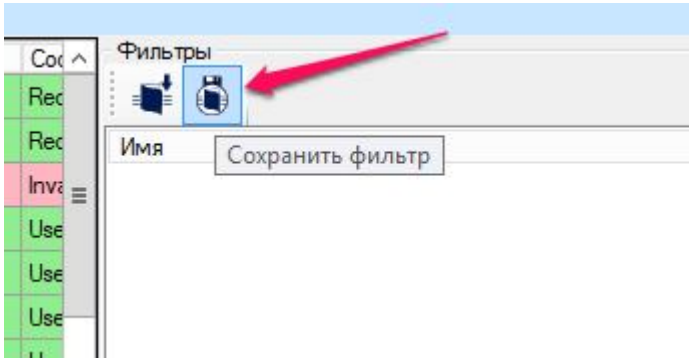


Рисунок 24 - Кнопка <Сохранить фильтр>

В появившемся далее окне следует выбрать нужный каталог для сохранения, задав при этом имя файлу, в который будет сохранен фильтр, и нажать кнопку <Save> (рисунок 25).

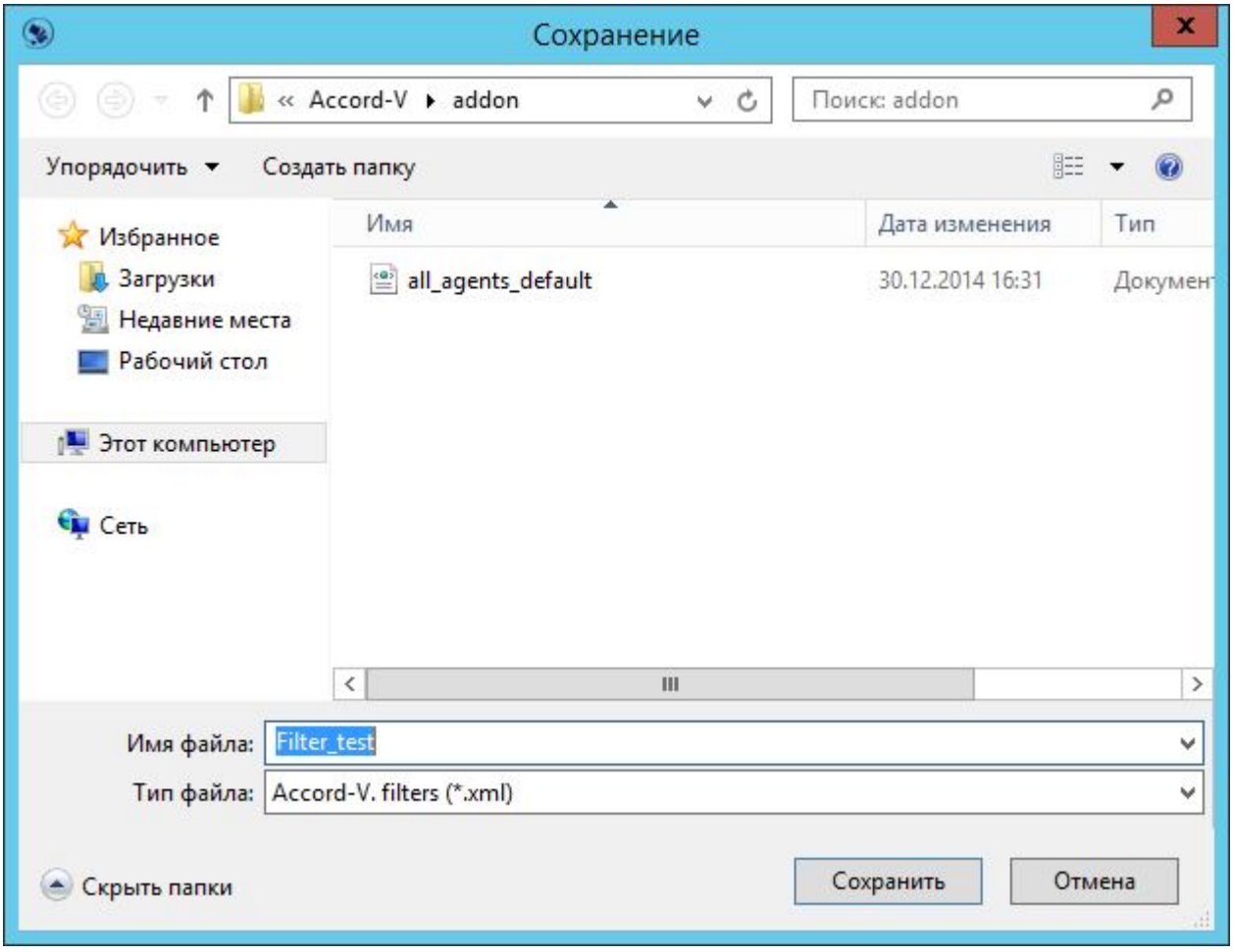


Рисунок 25 – Сохранение фильтра

В случае успешного выполнения описанной последовательности действий на экран выводится соответствующее сообщение (рисунок 26).

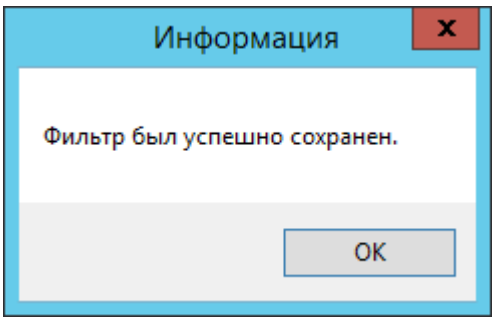


Рисунок 26 – Сообщение об успешном сохранении фильтра

5.4.2.3. Загрузка ранее сохраненного фильтра

Для того чтобы загрузить ранее сохраненный фильтр, следует нажать кнопку <Загрузить фильтр> и в появившемся окне выбрать нужный файл (рисунок 28).

ВНИМАНИЕ! При экспорте фильтров фильтр времени не экспортируется.

Рисунок 27 - Кнопка <Загрузить фильтр>

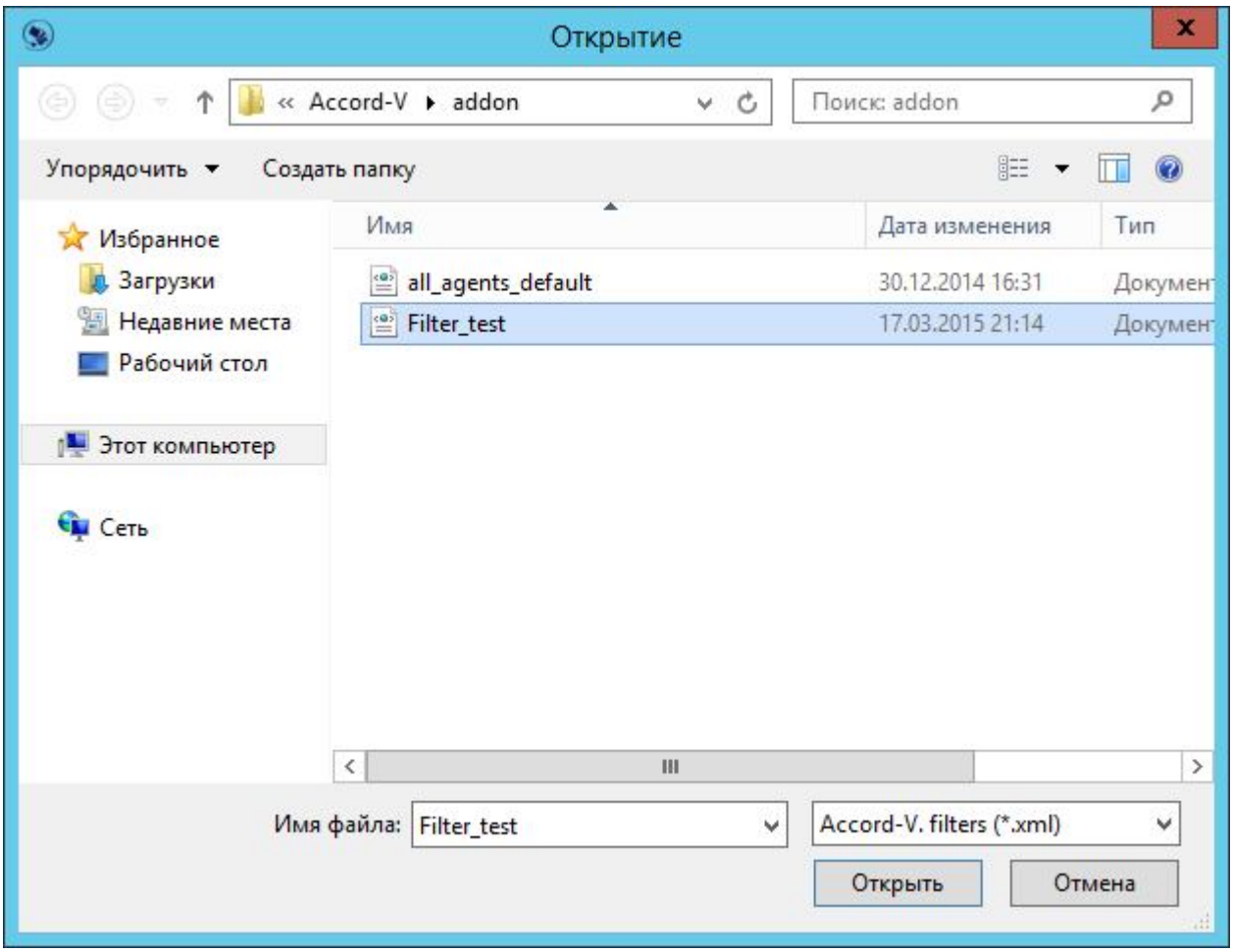


Рисунок 28 – Загрузка ранее сохраненного фильтра

В случае успешного выполнения описанной последовательности действий на экран выводится соответствующее сообщение (рисунок 29).

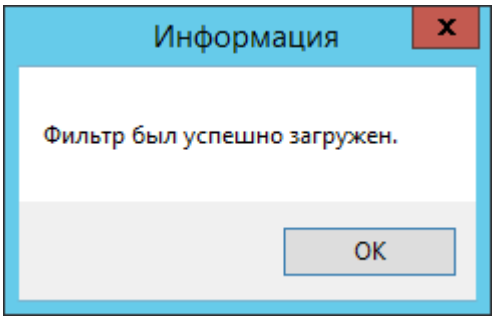


Рисунок 29 – Сообщение об успешной загрузке фильтра

5.4.3. Экспорт журнала

Список полученных событий можно экспортировать (формат CSV) посредством нажатия кнопки <Экспортировать события в файл> (рисунок 30).

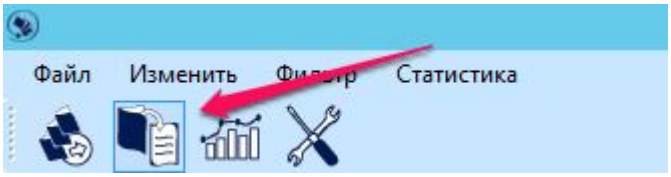


Рисунок 30 – Кнопка <Экспортировать события в файл>

В появившемся далее окне следует выбрать нужный каталог, задать название файлу, в который будут сохранены события, и нажать кнопку <Save> (рисунок 31).

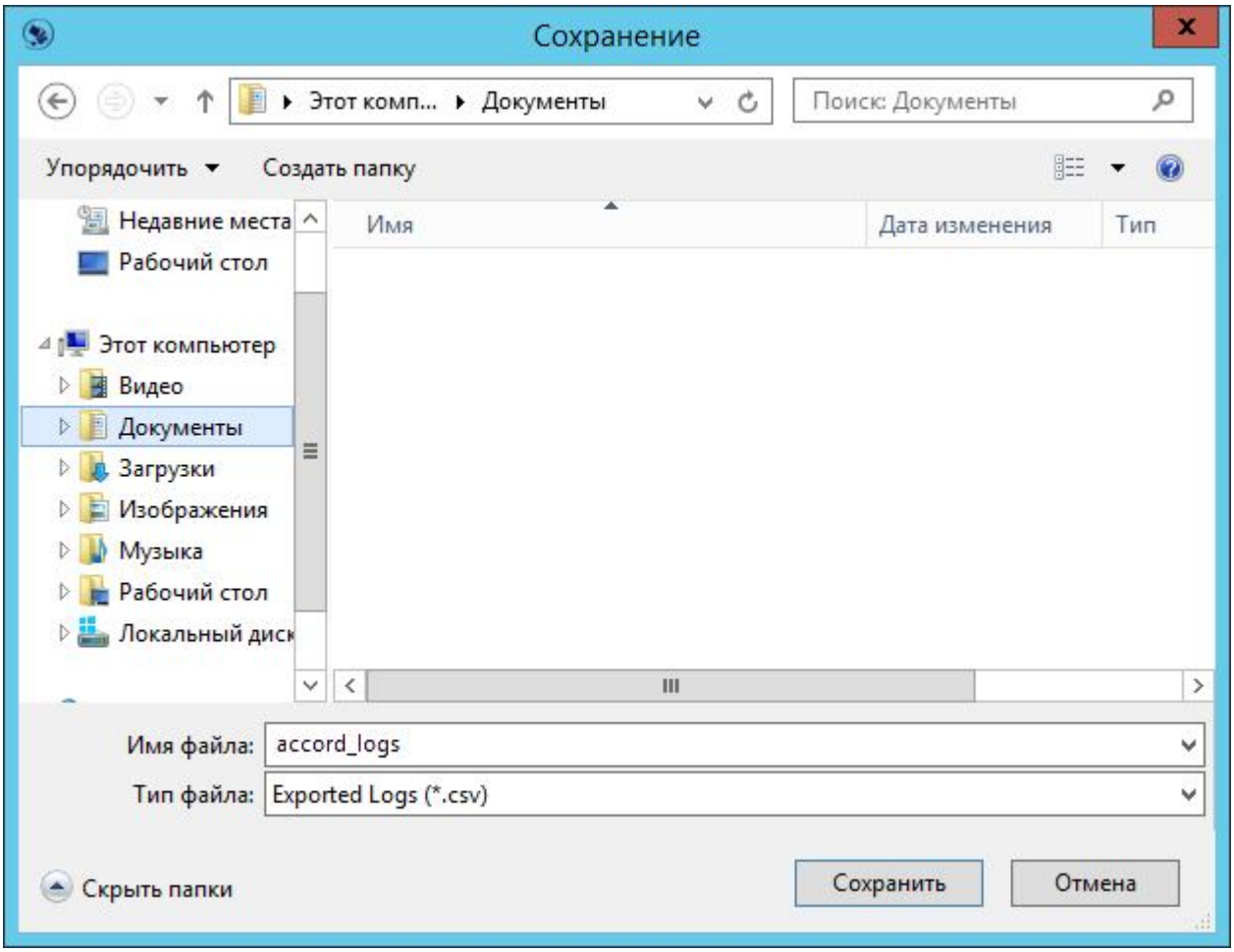


Рисунок 31 – Выбор каталога и задания имени файла для экспорта журнала

В случае успешного выполнения описанной последовательности действий на экран выводится соответствующее сообщение (рисунок 32).

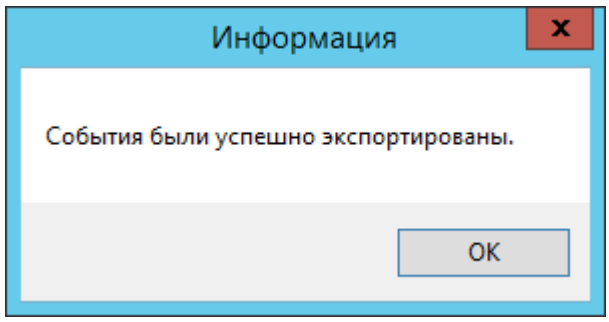


Рисунок 32 – Сообщение об успешном выполнении процедуры экспорта журнала

5.4.4. Просмотр статистики по полученным событиям

В утилите просмотра журнала регистрации событий предусмотрена возможность ведения статистики по полученным событиям.

Для этого следует в главном окне программы нажать кнопку <Анализ> (рисунок 33).

Рисунок 33 - Кнопка <Анализ>

В появившемся окне выводится статистика по количеству, типам и результатам полученных событий (рисунок 34).

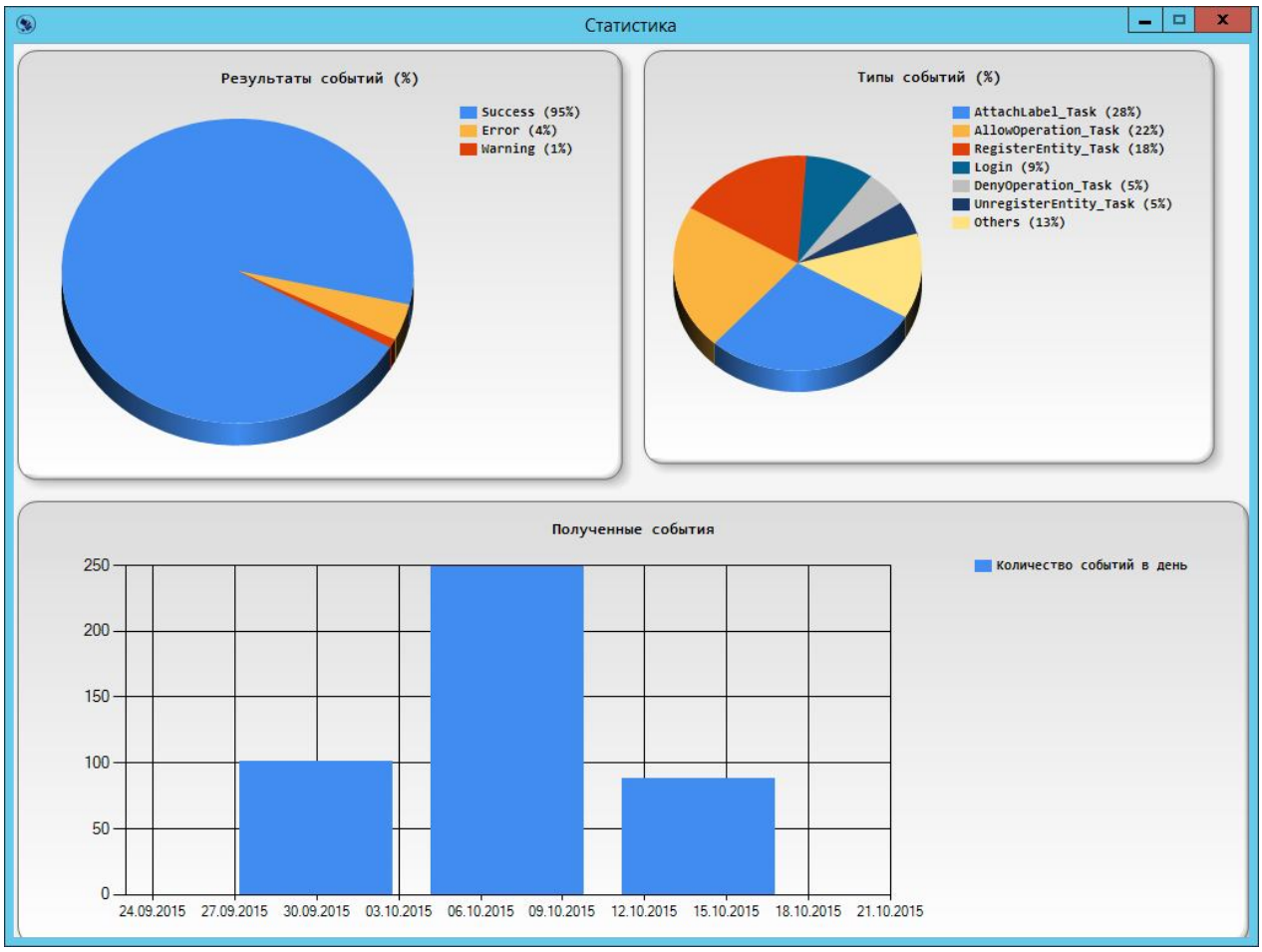


Рисунок 34 - Просмотр статистики

5.4.5. Настройки

Посредством нажатия кнопки <Настройки> (рисунок 35) имеется возможность настроить (рисунок 36):

- параметры цветовой схемы, используемой в утилите просмотра регистрируемых событий;
- IP-адрес и порт сервиса регистрации событий (данные параметры настраиваются администратором при первом сеансе работы – подробнее см. «Руководство по установке» (11443195.4012.028 98));
- максимальное количество событий, отображаемых в интерфейсе.

Рисунок 35 – Кнопка <Настройки>

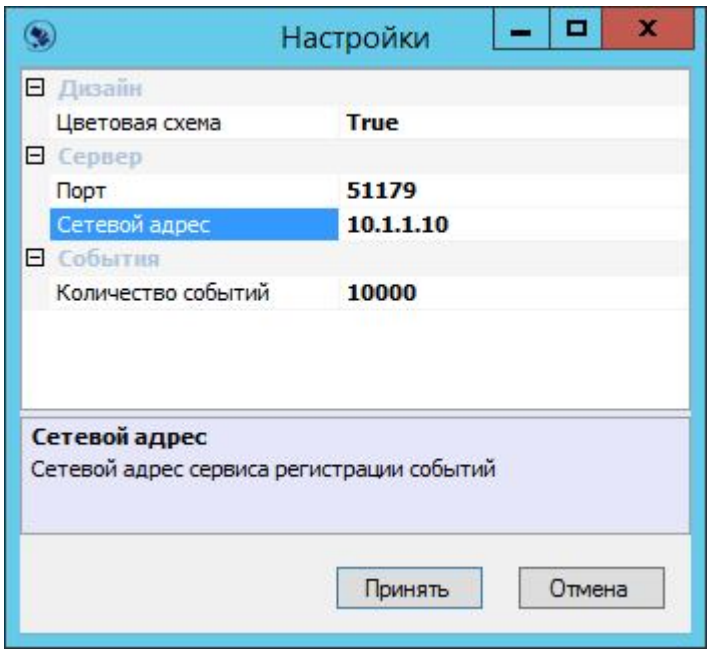


Рисунок 36 – Настройка IP-адреса сервиса регистрации событий

ВНИМАНИЕ! Ограничение в настройках на количество событий применяется к отображаемых количеству событий с учетом применения фильтра (т.е. по умолчанию 10 000 событий, попадающих под критерий заданного фильтра).

5.5. Работа с утилитой «Installer-V.»

5.5.1. Перегенерация сертификатов

Службы «Аккорд-В.» передают между собой информацию по протоколу SSL с использованием российской криптографии. В начале каждого соединения между ПО управления комплексом и всеми агентами «Аккорд-В.» на ESXi-серверах происходит двусторонняя идентификация и аутентификация, поэтому до начала взаимодействия соответствующие сертификаты и ключи, распределяются между всеми участниками информационного обмена.

В процессе установки агентов «Аккорд-В.» на ESXi распространение сертификатов на ESXi-серверы производится автоматически.

По умолчанию срок действия сертификатов составляет 365 дней (параметр default_days в файле openssl.cfg).

В случае необходимости, можно выполнить процедуру перегенерации сертификатов при помощи утилиты **«Installer-V.»**, в главном окне программы выбрав из списка нужный хост и нажав кнопку <Сгенерировать сертификаты>.

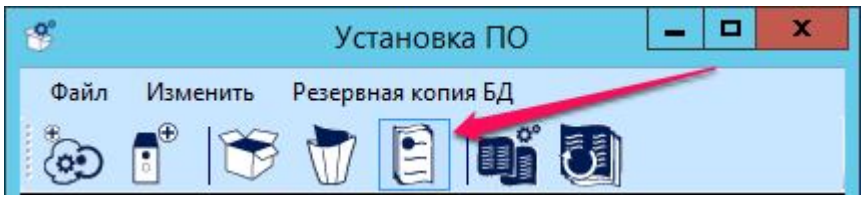


Рисунок 37 - Кнопка <Сертификаты>

В появившемся далее окне следует ввести имя учетной записи на выбранных ESXi (root) и ее пароль для соответствующего хоста (рисунок 38).

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 перегенерацию сертификатов на каждом ESXi отдельно, последовательно выделяя в списке нужный хост и нажимая кнопку <Сертификаты>.

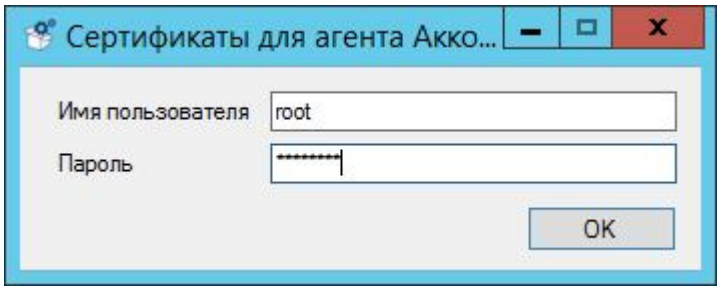


Рисунок 38 - Окно ввода параметров учетной записи root на ESXi

По нажатии кнопки <OK> в окне ввода пароля учетной записи root выполняется процедура перегенерации сертификатов на ESXi, в результате которой на экран выводится соответствующее сообщение (рисунок 39).

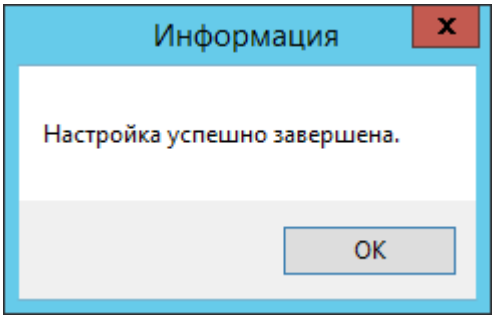


Рисунок 39 - Сообщение об успешном выполнении процедуры перегенерации сертификатов

ВНИМАНИЕ! Во время установки или удаления агента на ESXi работает SSH-сервис. Если перед установкой или удалением агента SSH-сервис на ESXi был отключён, по завершении этих действий может появиться окно ошибки, связанной с потерей соединения с сервером (рисунок 40). 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.

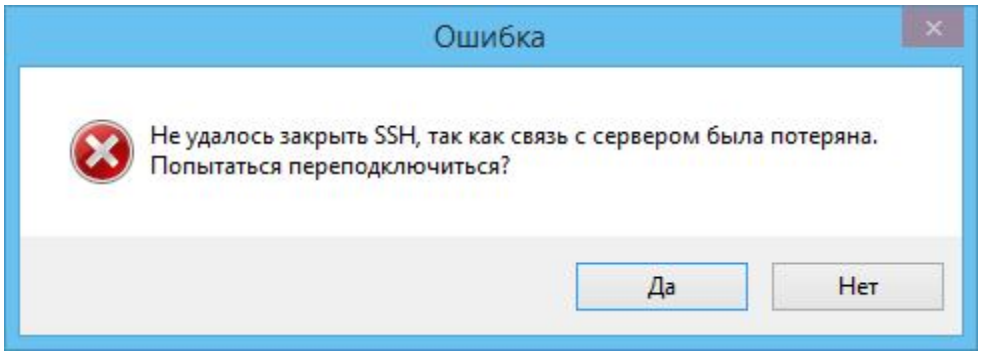


Рисунок 40 - Ошибка, связанная с потерей соединения с сервером

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!

5.5.2. Восстановление БД

Для восстановления резервной копии БД с ESXi следует запустить утилиту «Installer-V.» и нажать кнопку <Восстановить БД из резервной копии> (рисунок 41).

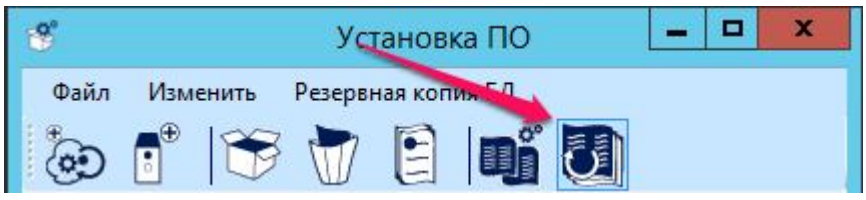


Рисунок 41 - Кнопка <Восстановить БД из резервной копии>

В появившемся далее окне следует указать путь к резервной копии БД и нажать кнопку <OK> (рисунок 42).

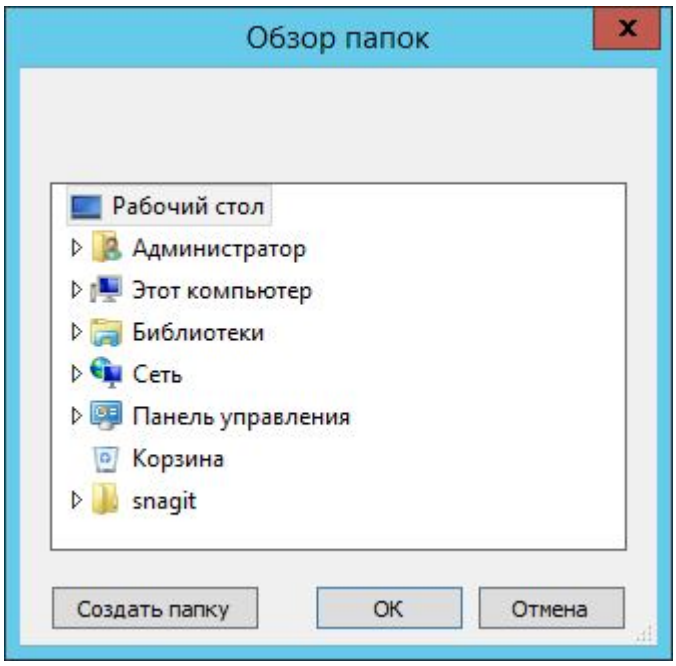


Рисунок 42 - Выбор каталога с резервной копией БД

6. Работа на клиентских рабочих местах

Работа на клиентских рабочих местах производится пользователем ПАК «Аккорд-В.» в соответствии с «Руководством пользователя» (11443195.4012.028-34).

ВНИМАНИЕ! Для выполнения процедур идентификации и аутентификации в виртуальной машине, которая находится в защищаемой инфраструктуре виртуализации, пользователю необходимо предъявлять персональный идентификатор; поэтому администратор безопасности информации должен настроить возможность проброса идентификатора пользователя с клиентского рабочего места в виртуальную машину.

7. Возможные затруднения в работе с ПАК «Аккорд-В.» и методы их устранения

7.1. Блокировка ВМ

7.1.1. Что приводит к блокировке ВМ

К блокировке ВМ могут приводить следующие действия:

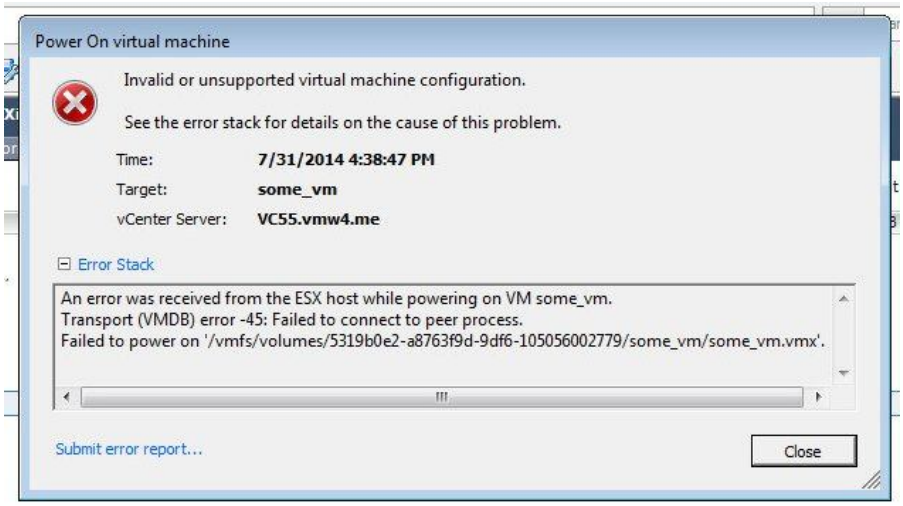
- изменение оборудования ВМ, в том числе подключение оборудования без выключения или перезагрузки (например, подключение usb-контроллера);

– изменение контролируемых файлов внутри ОС и MBR.

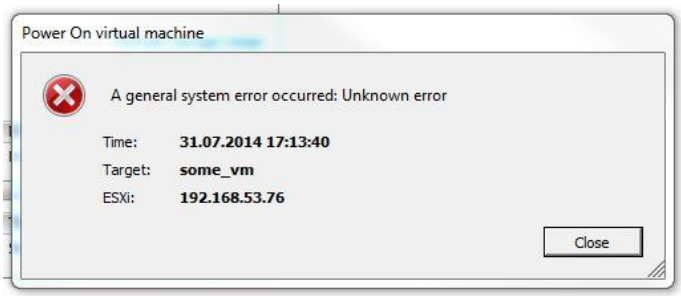
7.1.2. Поведение в случае блокировки ВМ

Если ВМ в vClient не включается и на экран выводятся следующие сообщения:

Для vSphere 6.5



Для vSphere 5.5 и 6.0



Для vSphere 5.0 и 5.1

то для выяснения причины необходимо открыть LogViewer для просмотра событий с агентов «Аккорд-В.» на ESXi (в этом случае удобнее отфильтровать события по компоненту Accord-V).

Для некоторых событий, отображенных в журнале, доступно расширенное описание по двойному клику (например, имеется возможность отследить, какое именное оборудование ВМ изменилось – событие «vmx verification failed»).

7.2. Что делать, если утилита «Accord-V.» не отвечает на команды

ВНИМАНИЕ! В случае если утилита «Accord-V.» не отвечает на выполнение какого-либо действия, оно завершается автоматически через 120 секунд. **Не прекращайте работу утилиты принудительно!**

В случае если по каким-либо причинам работа утилиты все же была завершена принудительно, следует:

- проверить список процессов (taskmgr) и завершить принудительно процесс AccordManager;
- повторно открыть утилиту «Accord-V.» и уточнить, с какими хостами не установилось соединение;
- зайти через shell/ssh на данные хосты по очереди;
- набрать команду «ps | grep acc» и проверить список отобразившихся процессов;
- если в списке присутствует процесс «accordguard», следует завершить его по указанному в начале PID процесса (например, «kill -9 234123»);
- вне зависимости от предыдущего пункта необходимо перезапустить accordservice (команда «/etc/init.d/accordservice.sh restart»). В случае если для запуска сервиса окажется недостаточно таймаута по умолчанию (10 секунд) и сервис не запустится, следует запустить его командой «/etc/init.d/accordservice.sh start»;
- после успешного старта сервиса следует выбрать данный хост в «Accord-V.» и нажать кнопку <Подключить>.

7.3. Сбор событий в случае некорректного поведения ПО «Аккорд-В.»

Причины неполадок в работе сервиса регистрации событий выводятся в стандартную утилиту системы Start -> Administrative tools -> Event Viewer.

В случае возникновения проблем при работе с утилитой «Accord-V.»:

- необходимо описать по пунктам действия, приведшие к данному результату (были ли подключены хосты в «Accord-V.», ОС ВМ, количество снапшотов, количество vmdk, также полезен скриншот папки с содержимым ВМ или скриншот из storage views -> show all Virtual Machine Files);
- если на экран выводится сообщение типа «exception», необходимо приложить его полную выдержку в конце сообщения, а также crash dump из папки с ПО;
- при зависании события установки на контроль следует также собрать события и на ESXi (файлы accordservice.log ; accordguard.log в директории /var/log/accordguard);
- список процессов выведенных после команды «ps | grep acc» (в shell/ssh у ESXi).

7.4. Создание/Обнуление БД

В случае экстраординарных ситуаций, повлекших за собой рассинхронизацию или нарушение целостности БД, необходимо выполнить следующие команды:

`repair.exe -db` (в папке C:\Program Files\OKB SAPR\Accord-V);

`./accordguard -n` (на ESXi в папке /etc/accord-V).

Для сервиса регистрации событий:

`repair.exe -log` (в папке C:\Program Files\OKB SAPR\Accord-V).

8. Техническая поддержка и информация о комплексе

Все вопросы, связанные с поддержкой ПАК «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.

Дополнительную информацию, а также список часто задаваемых вопросов Вы можете найти на сайте www.accord-v.ru.

Мы будем рады узнать Ваши пожелания и предложения по поводу этой документации. Вы можете отправить их по адресу help@okbsapr.ru.

Приложение 3. Перечень регистрируемых событий от VMware и от агентов «Аккорд-В.»

Тип	Результат	Сообщение	Описание	Примечание
Результат попытки включения ВМ (миграция между хранилищами и хостами так же попадает под ситуацию включения)				
PowerOn_Task	Error	VirtualMachine [имя ВМ] can not be powered. Integrity was broken.	ВМ не может быть включена, т.к. ее целостность нарушена или она заблокирована	
PowerOn_Task	Warning	VirtualMachine [имя ВМ] isn't registered on this host. Default behavior: Allow power on.	ВМ отсутствует в БД агента. Поведение по умолчанию: разрешить включение	ВМ еще не устанавливалась на контроль
PowerOn_Task	Error	VirtualMachine [имя ВМ] isn't registered on this host. Default behavior: Deny power on.	ВМ отсутствует в БД агента. Поведение по умолчанию: запрет включения	ВМ еще не устанавливалась на контроль
PowerOn_Task	Error	VirtualMachine [имя ВМ] isn't allowed to run on this host.	ВМ не разрешен запуск на данном хосте	Необходимо разрешить миграцию на хост в «Accord-V.»
PowerOn_Task	Success	VirtualMachine [имя ВМ] powered on.	ВМ разрешено включение	
PowerOn_Task	Error	AMDZ or ENOUGH device was not found	На ESXi отсутствует АМДЗ/ИНАФ. Включение ВМ невозможно.	Сертифицируемая версия не работает без аппаратной части на ESXi. Для тестирования возможно запросить версию без аппаратной привязки.
Проверка ВМ при включении/миграции включенной ВМ (между хранилищами и хостами)/проверка через «Accord-V.»			Если проверка прошла успешно, никаких событий не будет зарегистрировано	Для BIOS невозможна ситуация, когда КЦ нарушен. При каждом включении агент подставляет зафиксированную версию BIOS (установленную на контроль)
Verification_Task	Error	VirtualMachine [имя ВМ] snapshot chain was changed.	ВМ заблокирована, т.к. для нее был сделан снапшот (или был осуществлен переход к уже существующему снапшоту)	Если последовательность снапшотов будет восстановлена (новые будут удалены или будет выполнен возврат к текущему зафиксированному снапшоту), то ВМ снова можно будет включить. При попытке отката к снапшоту, где ВМ во включенном состоянии, будет выведена ошибка и ВМ перейдет в состояние suspend

Тип	Результат	Сообщение	Описание	Примечание
Verification_Task	Error	VirtualMachine [имя ВМ] vmx verification has been failed. + diff	Оборудование ВМ изменено	Двойной клик на сообщение покажет дополнительную информацию об изменениях
Verification_Task	Error	VirtualMachine [имя ВМ] has been locked.	ВМ заблокирована	
Verification_Task	Error	VirtualMcahine [имя ВМ] mbr integrity was failed.	Целостность MBR нарушена	На одном из vmdk принадлежащем ВМ MBR изменился (при установке MBR ВМ на контроль он вычисляется для всех vmdk)
Verification_Task	Error	VirtualMachine [имя ВМ] file [имя файла] verification has been failed.	Целостность файла [путь\имя] нарушена	
Verification_Task	Error	Storage vMotion blocked.	Storage vMotion заблокирован	Блокируется всегда. Единственный вариант перемещения ВМ на другое хранилище без выключения - включить мягкий режим на хосте. Позже, когда ВМ будет выключена, для нее необходимо будет повторно настроить миграцию (убрать хосты с миграции и снова разрешить) и поставить снова на контроль на новом хранилище
PAM: события И/А на ESXi при помощи shell/ssh				События DCUI не регистрируются
PamShell_Task	Success	Login succeeded.	Пользователь успешно вошел в систему	
PamShell_Task	Error	Login failed. Wrong user or password.	Вход в систему запрещен. Неправильный пользователь или пароль	
PamSSH_Task	Success	Login succeeded.	Пользователь успешно вошел в систему	

Тип	Результат	Сообщение	Описание	Примечание
PamSSH_Task	Error	Login failed. Wrong user or password.	Вход в систему запрещен. Неправильный пользователь или пароль	
Установка/потеря соединения с агентами ESXi/vCenter				везде ip или везде имя
ConnectionEvent	Error	Connection with [ip/имя] was lost	Соединение с [ip/имя] было потеряно	
ConnectionEvent	Success	Connection with [ip/имя] was established	Соединение с [ip/имя] установлено	
Поведение по умолчанию				
Settings_Task	Warning	Default behavior for unregistered VM set to "Deny Power On VM"	Поведение по умолчанию для данного хоста установлено в "запрет включения ВМ"	Если ВМ отсутствует в БД агента "Аккорд-В." на ESXi, то ее включение будет запрещено
Settings_Task	Warning	Default behavior for unregistered VM set to "Allow Power On VM"	Поведение по умолчанию для данного хоста установлено в "разрешение включения ВМ"	Если ВМ отсутствует в БД агента "Аккорд-В." на ESXi, то ее включение будет разрешено. Небезопасная конфигурация!
Settings_Task	Warning	Soft mode is off.	Мягкий режим выключен	Настройка по умолчанию. Если КС ВМ изменились, то она не включится
Settings_Task	Warning	Soft mode is on. All registered virtual machines are allowed to start.	Мягкий режим включен	Вне зависимости от результата проверки целостности ВМ будет включена. Небезопасная конфигурация!
Установка на контроль /снятие с контроля / пересчет КС				При пересчете КС, отобразятся сначала remove действия, затем set (только для пересчитываемых элементов). Если повторно устанавливаем на контроль, то отображаются ВСЕ действия: сначала действия remove для всех элементов, затем set только для установленных

Тип	Результат	Сообщение	Описание	Примечание
LockVm_Task	Success	VirtualMachine [имя ВМ]has been locked.	ВМ заблокирована	Если ВМ заблокирована, то ей запрещено включение. При разрешении миграции для ВМ в событиях отобразятся действия unlock/lock (подряд, порядок может отличаться). Результат ВМ разблокирована!
UnlockVm_Task	Success	VirtualMachine [имя ВМ] has been unlocked.	ВМ раблокирована	
SetVmxControl_Task	Success	VirtualMachine [имя ВМ] vmx has been set to control.	Оборудование ВМ установлено на контроль	
RemoveVmxControl_Task	Success	VirtualMachine [имя ВМ] vmx has been removed from control.	Оборудование ВМ снято с контроля	
SetBiosControl_Task	Success	VirtualMachine [имя ВМ] BIOS has been set to control.	BIOS ВМ установлен на контроль	ВМ с EFI вместо BIOS также может быть установлена на контроль
RemoveBiosControl_Task	Success	VirtualMachine [имя ВМ] BIOS has been removed from control.	BIOS ВМ снят с контроля	
SetMbrControl_Task	Success	VirtualMachine [имя ВМ] mbr has been set to control.	MBR ВМ установлен на контроль	При установке MBR ВМ на контроль он вычисляется для всех vmd
RemoveMbrControl_Task	Success	VirtualMachine [имя ВМ] mbr has been removed from control.	MBR ВМ снят с контроля	
SetFileControl_Task	Success	VirtualMachine [имя ВМ] files has been set to control.	Файлы гостевой ОС ВМ были установлены на контроль	Список файлов, установленных на контроль, можно посмотреть только в утилите «Accord-V.»
RemoveFileControl_Task	Success	VirtualMachine [имя ВМ] files has been removed from control.	Файлы гостевой ОС ВМ были сняты с контроля	