ОСОБОЕ КОНСТРУКТОРСКОЕ БЮР
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАН

Программно-аппаратный комплекс средств защиты от несанкционированного доступа «ГиперАккорд»

Руководство администратора безопасности информации

11443195.4012.057 90

Листов 22

Москва
2016

АННОТАЦИЯ

Настоящий документ является руководством администратора безопасности программно-аппаратного комплекса средств защиты информации от несанкционированного доступа (ПАК СЗИ НСД) «ГиперАккорд» (далее по тексту – ПАК «ГиперАккорд», либо «ГиперАккорд»), предназначенного для защиты инфраструктур виртуализации, построенных на базе платформ виртуализации Hyper-V версии 2 и версии 3.

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

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

Перед началом эксплуатации ПАК «ГиперАккорд» 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.

Применение ПАК «ГиперАккорд» 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.

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 – персональный идентификатор пользователя.

Использовать идентификатор – приложить персональный идентификатор пользователя к контактному устройству съемника информации, или подключить к USB-порту на плате контроллера.

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

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

Пояснения – 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 Состав ПАК «ГиперАккорд»

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

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

ПАК «ГиперАккорд» включает в себя:

1) ПАК СЗИ НСД «Аккорд-Win64» (ТУ 4012-037-11443195-10), устанавливаемый в ОС сервера HV, в составе:
   - СЗИ НСД «Аккорд-АМДЗ»;
   - специальное программное обеспечение «Аккорд-Win64».
2) СПО «ГиперАккорд», устанавливаемое в ОС сервера HV;
3) СПО «Аккорд-Win32 TSE», устанавливаемое в ОС ВМ (32-битные);
4) СПО «Аккорд-Win64 TSE», устанавливаемое в ОС ВМ (64-битные).
5) СПО «Аккорд-ТК», устанавливаемое на клиентские рабочие места.

ПАК «Аккорд-Win64 TSE», устанавливаемый в ОС сервера HV, реализует доверенную загрузку сервера HV, используется для разграничения доступа к ресурсам сервера HV со стороны АБИ и АВИ.

СПО «ГиперАккорд», устанавливаемое в ОС сервера HV, является основным компонентом управления ПАК «ГиперАккорд», контролирует включение ВМ и обеспечивает контроль целостности до ее запуска. Данное СПО предоставляет также пользовательский интерфейс, реализующий функции управления ПАК «ГиперАккорд».

СПО «Аккорд-Win32 TSE»/«Аккорд-Win64 TSE» (в зависимости от установленной в ВМ ОС), устанавливаемое на ВМ, используется для разграничения доступа пользователей к ресурсам ВМ и, в случае необходимости, обеспечивает возможность удаленного подключения к ВМ с клиентских рабочих мест.

СПО «Аккорд-ТК», устанавливаемое на клиентские рабочие места в случае наличия потребности подключения пользователей клиентских рабочих мест к ВМ с использованием технологии терминального доступа, обеспечивает удаленное защищенное подключение к ВМ.

СЗИ НСД «Аккорд-АМДЗ» устанавливается:

- на сервер HV;

- на клиентские рабочие места. Контроллер «Аккорд-АМДЗ» устанавливается на клиентские рабочие места, если пользователь одновременно обрабатывает информацию локально на клиентском рабочем месте и на виртуальной машине, запущенной на сервере HV. Если на клиентском рабочем месте не производится локальная обработка информации, то в установке контроллера нет необходимости. Контроллер «Аккорд-АМДЗ», устанавливаемый на клиентском рабочем месте, не является частью ПАК СЗИ НСД «ГиперАккорд».

Модификация контроллера оговаривается при поставке комплекса.

1.2 Назначение комплекса

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

- Hyper-V версии 2;
- Hyper-V версии 3.

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 (файлов общего, прикладного ПО и данных) ПЭВМ (АС);
- контроля целостности программных компонентов (файлов общего, прикладного ПО и данных) ВМ, 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.

1.3 Технические условия применения комплекса

Для установки комплекса «ГиперАккорд» требуется следующий минимальный состав технических и программных средств:

- наличие инфраструктуры виртуализации, построенной на базе одной из поддерживаемых платформ виртуализации, список которых приведен в подразделе 1.2;

- наличие свободного слота PCI/PCI-X/Express на материнской плате ПЭВМ (для сервера HV);
- объем свободного дискового пространства для размещения ПО на жестком диске около 50 Мбайт (на сервере HV).

1.4 Особенности работы ПО ПАК «ГиперАккорд» с виртуальными машинами

Работа ПО ПАК «ГиперАккорд» с виртуальными машинами имеет ряд особенностей:

- ПО ПАК «ГиперАккорд» не поддерживает работу с виртуальными машинами, переведенными в состояние «Suspend». Оперативная память в таком случае не защищена от модификации, поэтому защищаемые машины не должны переводиться в это состояние;
- файлы, зашифрованные встроенными средствами Windows, не рекомендуется ставить на контроль. Это не относится к файлам, зашифрованным сторонними СКЗИ – их целостность контролируется аналогично стандартным файлам;
- имя виртуальной машины не должно содержать символов кириллицы.

2 Работа с ПАК «ГиперАккорд»

2.1 Компоненты управления ПАК «ГиперАккорд»

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

1)администрирование СПО «ГиперАккорд» (подробнее см. раздел 2.3 настоящего руководства);

2)администрирование остальных компонентов, входящих в комплект поставки ПАК «ГиперАккорд»:

- ПАК СЗИ НСД «Аккорд-Win64» (подробнее см. комплект эксплуатационной документации на ПАК СЗИ НСД «Аккорд-Win64»), в том числе «Аккорд–АМДЗ» (подробнее см. «Руководство по установке» (11443195.4012.038 98), «Руководство администратора» (11443195.4012.038 90));
- «Аккорд-Win32 TSE»/«Аккорд-Win64 TSE», устанавливаемое в виртуальные машины (подробнее см.: «Руководство по установке» (11443195.4012.036 98), «Руководство администратора» (11443195.4012.036 90) – для «Аккорд-Win32 TSE»; «Руководство по установке» (11443195.4012.037 98), «Руководство администратора» (11443195.4012.037 90) – для «Аккорд-

Win32 TSE»;
«Руководство по установке» (11443195.4012.026 98).

Для администрирования СПО «ГиперАккорд» используется утилита администрирования «ГиперАккорд», установленная в ОС сервера HV.

2.2 Установка компонентов комплекса

Установка компонентов ПАК «ГиперАккорд» проводится в соответствии с положениями «Руководства по установке» (11443195.4012.057 98), входящего в состав комплекта поставки комплекса.

2.3 Администрирование ПАК «ГиперАккорд»

2.3.1 Общие сведения

Администрирование ПАК «ГиперАккорд» осуществляется в следующем порядке: АБИ запускает на сервере HV СПО, реализующее функции управления ПАК «ГиперАккорд», и в соответствии с подразделом 2.3 настоящего руководства производит настройку и администрирование системы защиты «ГиперАккорд».

ВНИМАНИЕ! Перед первым сеансом работы с пользовательским интерфейсом управления «ГиперАккорд» необходимо предварительно настроить инфраструктуру виртуализации: создать необходимые виртуальные машины, сделать необходимые снапшоты и т. д.

Если во время работы с пользовательским интерфейсом были внесены изменения в конфигурацию инфраструктуры виртуализации, необходимо перезагрузить модуль управления системой защиты.

2.3.2 Настройка списка виртуальных машин в СПО «ГиперАккорд»

Первым шагом в настройке «ГиперАккорд» является настройка в СПО «ГиперАккорд» списка размещенных на сервере HV виртуальных машин, целостность которых необходимо контролировать. Для этого в окне программы «ГиперАккорд» следует на вкладке «Виртуальные машины» нажать кнопку <Добавить виртуальную машину> (рисунок 1).

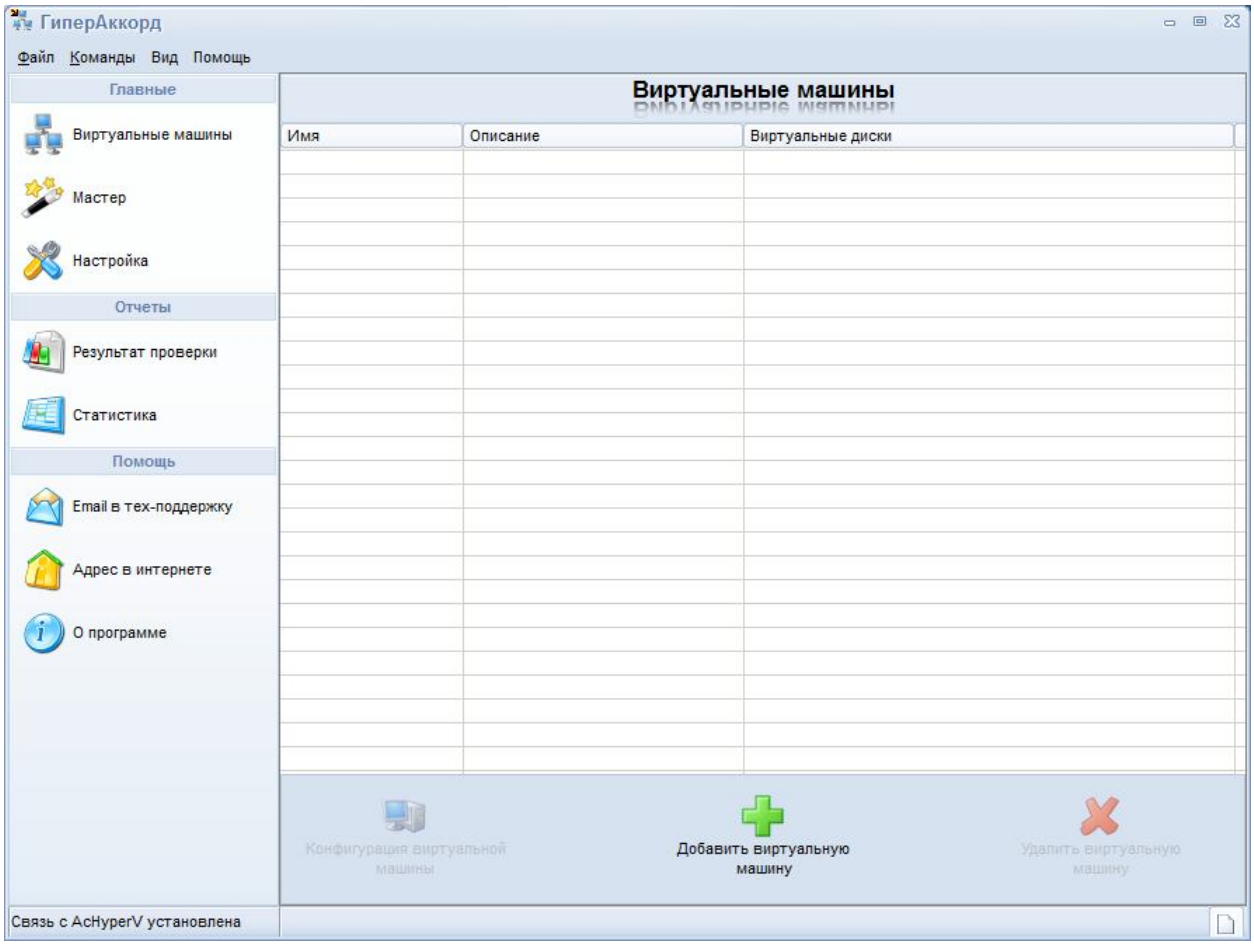

Рисунок 1 – Главное окно программы. Вкладка «Виртуальные машины»

В появившемся далеее окне следует выбрать файл с описанием виртуальной машины, целостность которой необходимо контролировать (рисунок 2).

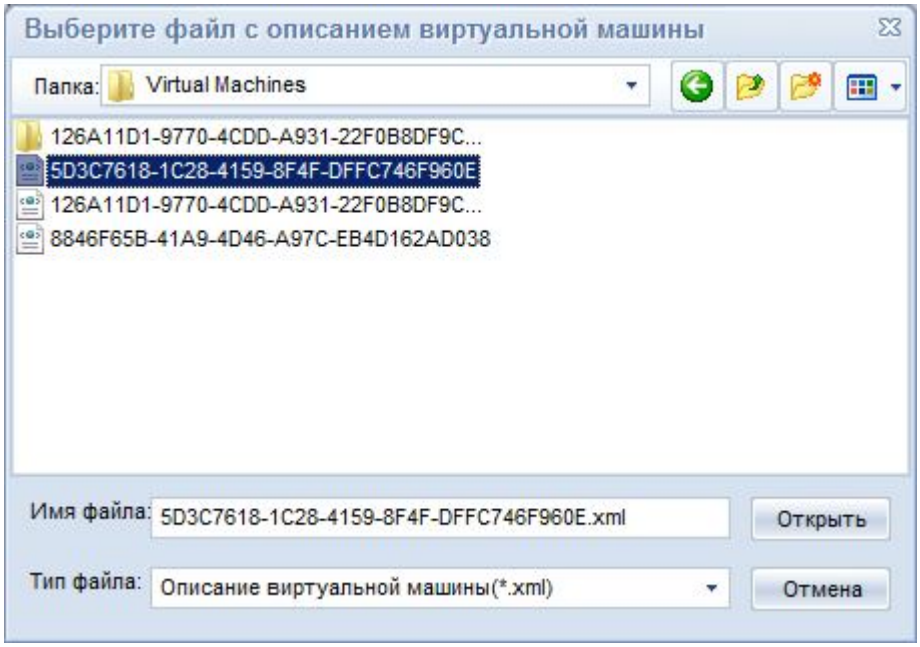

Рисунок 2 – Окно выбора файла с описанием ВМ

В появившемся далее окне следует в поле «Описание машины» ввести необходимую информацию, предназначенную для того, чтобы можно было легко отличить нужную ВМ от других (рисунок 3).

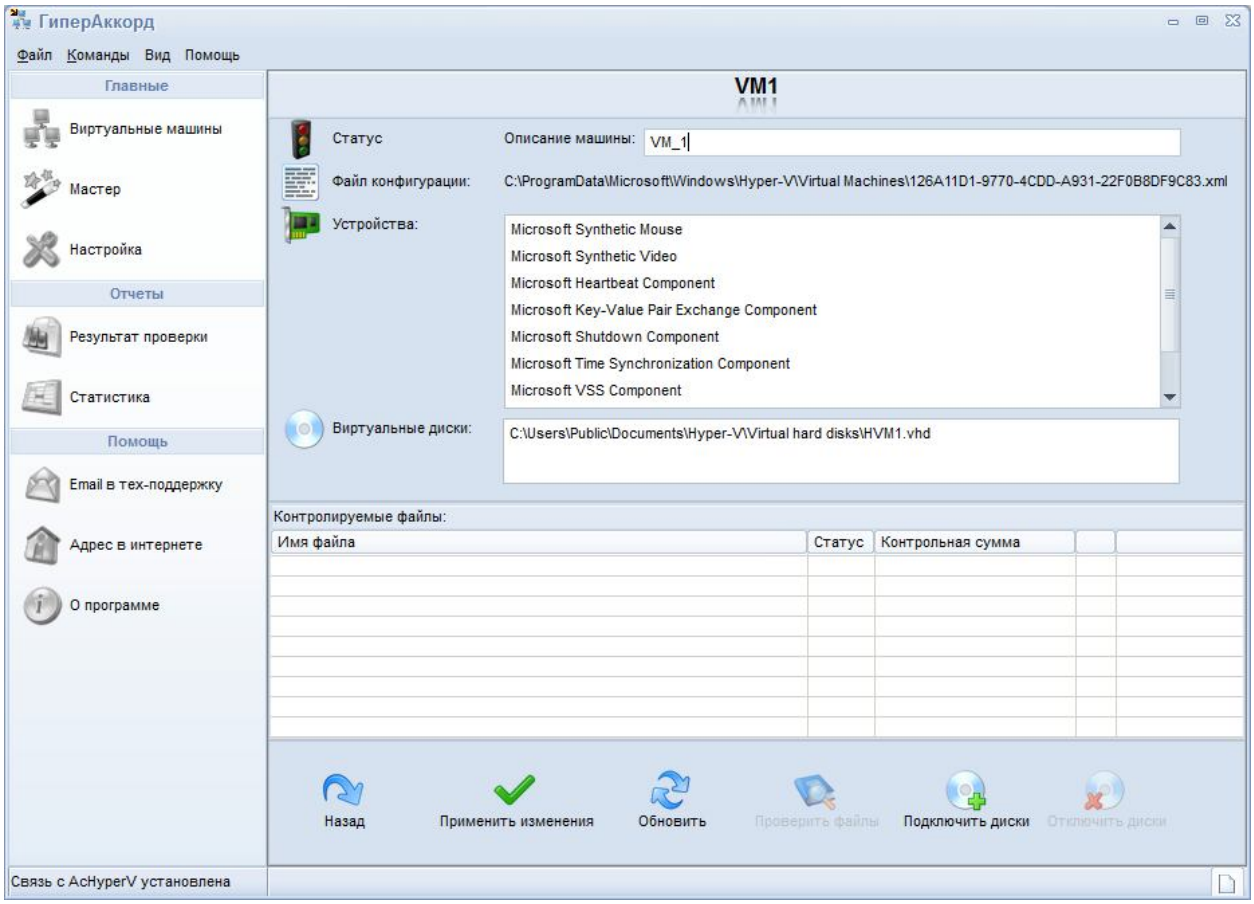

Рисунок 3 – Описание виртуальной машины

После успешного выполнения описанной последовательности действий необходимо сохранить изменения посредством нажатия кнопки <Применить изменения> (рисунок 3). При этом виртуальная машина появляется в списке ВМ на вкладке «Виртуальные машины» (рисунок 4).

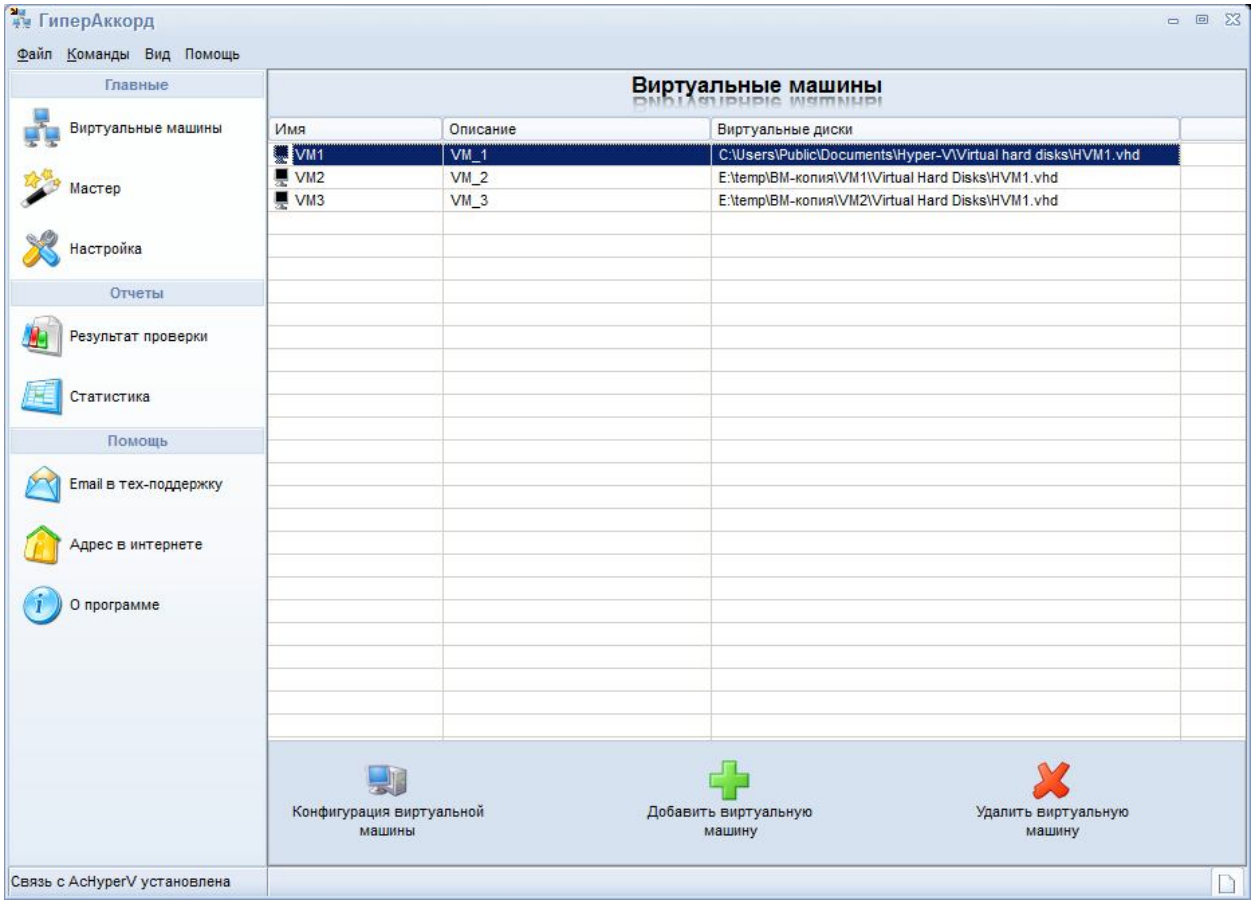

Рисунок 4 – Список ВМ на вкладке «Виртуальные машины»

После того как список нужных ВМ сформирован, следует перейти к процедуре настройки списков контроля целостности файлов ВМ (подробнее см. 2.3.3).

2.3.3 Настройка списков контроля целостности файлов виртуальной машины

Для того чтобы настроить списки контроля целостности файлов виртуальной машины, следует выбрать ее в общем списке ВМ и нажать кнопку <Конфигурация виртуальной машины> или дважды щелкнуть по ней левой кнопкой мыши (рисунок 4).

В появившемся далее окне (рисунок 3) следует нажать кнопку <Подключить диски> – на экран выводится окно с деревом каталогов, в котором по двойному щелчку левой кнопки мыши следует выбрать файлы ВМ, которые необходимо контролировать (рисунок 5).

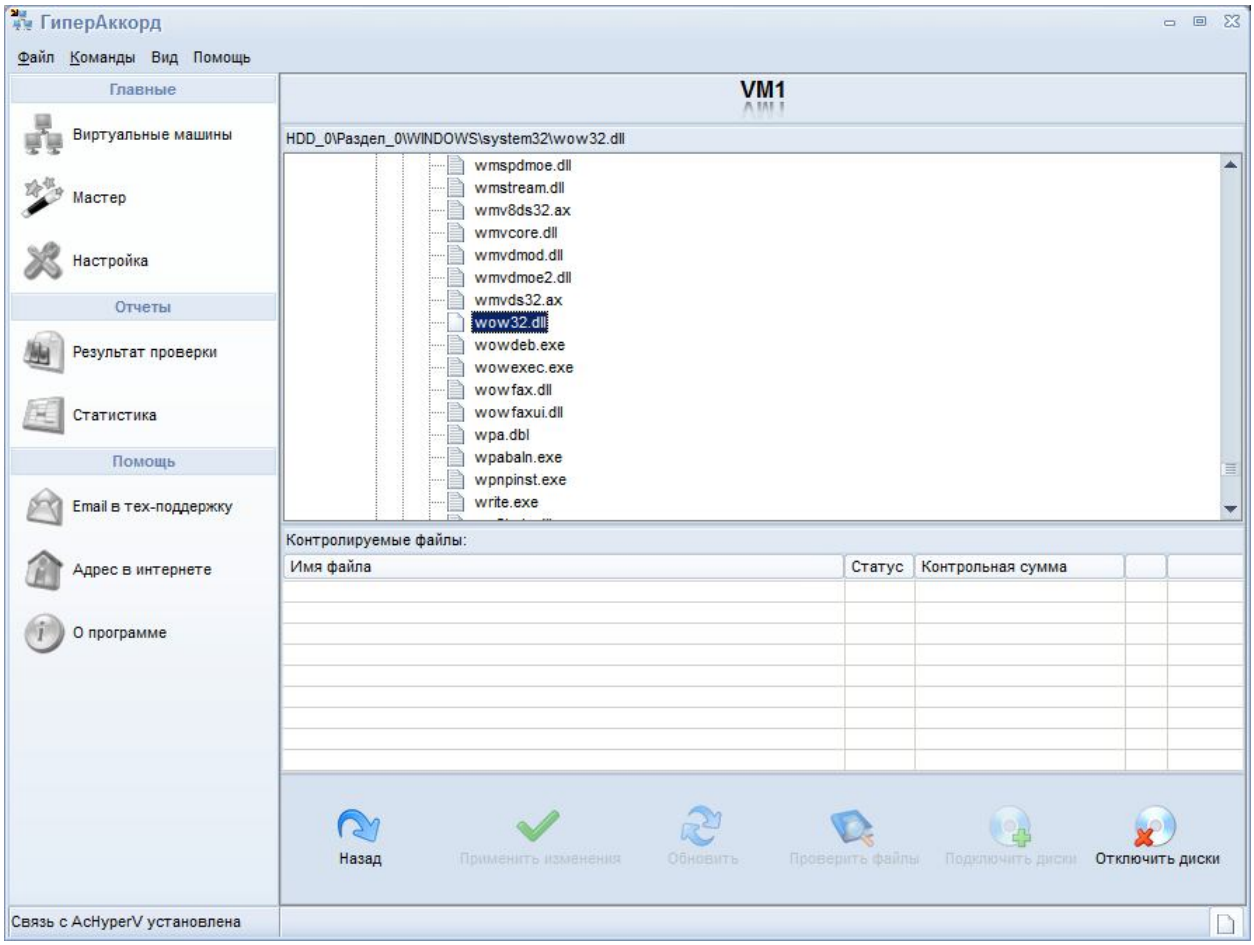

Рисунок 5 – Окно с деревом каталогов ВМ

При этом выбранные файлы появляются в списке контролируемых файлов (рисунок 6).

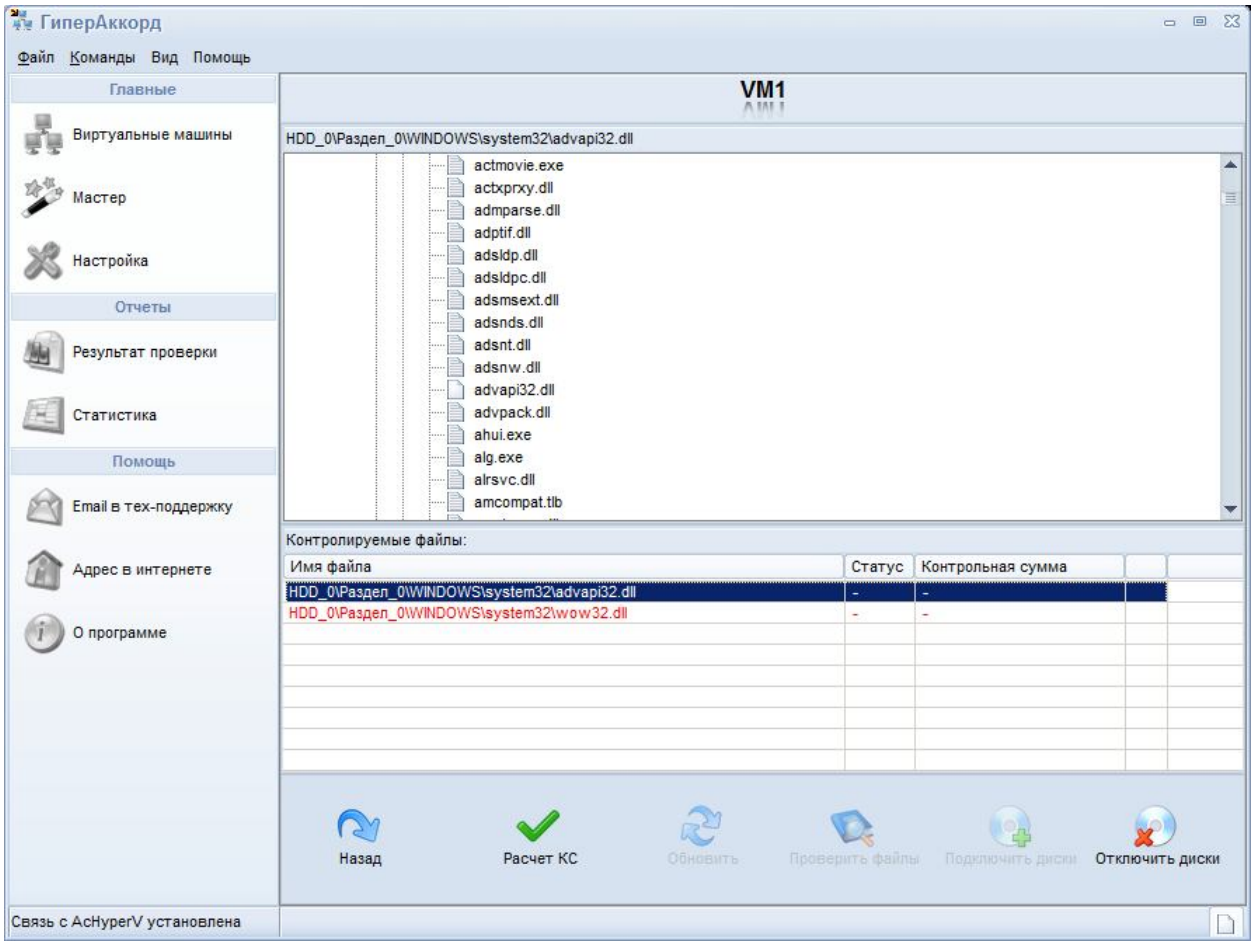

Рисунок 6 – Список контролируемых файлов

После того как список контролируемых файлов сформирован, следует рассчитать для них контрольные суммы, выделив в списке нужные файлы и нажав кнопку <Расчет КС> (рисунок 6) – в соответствующих ячейках таблицы появляются рассчитанные КС для файлов и результат их проверки (рисунок 7).

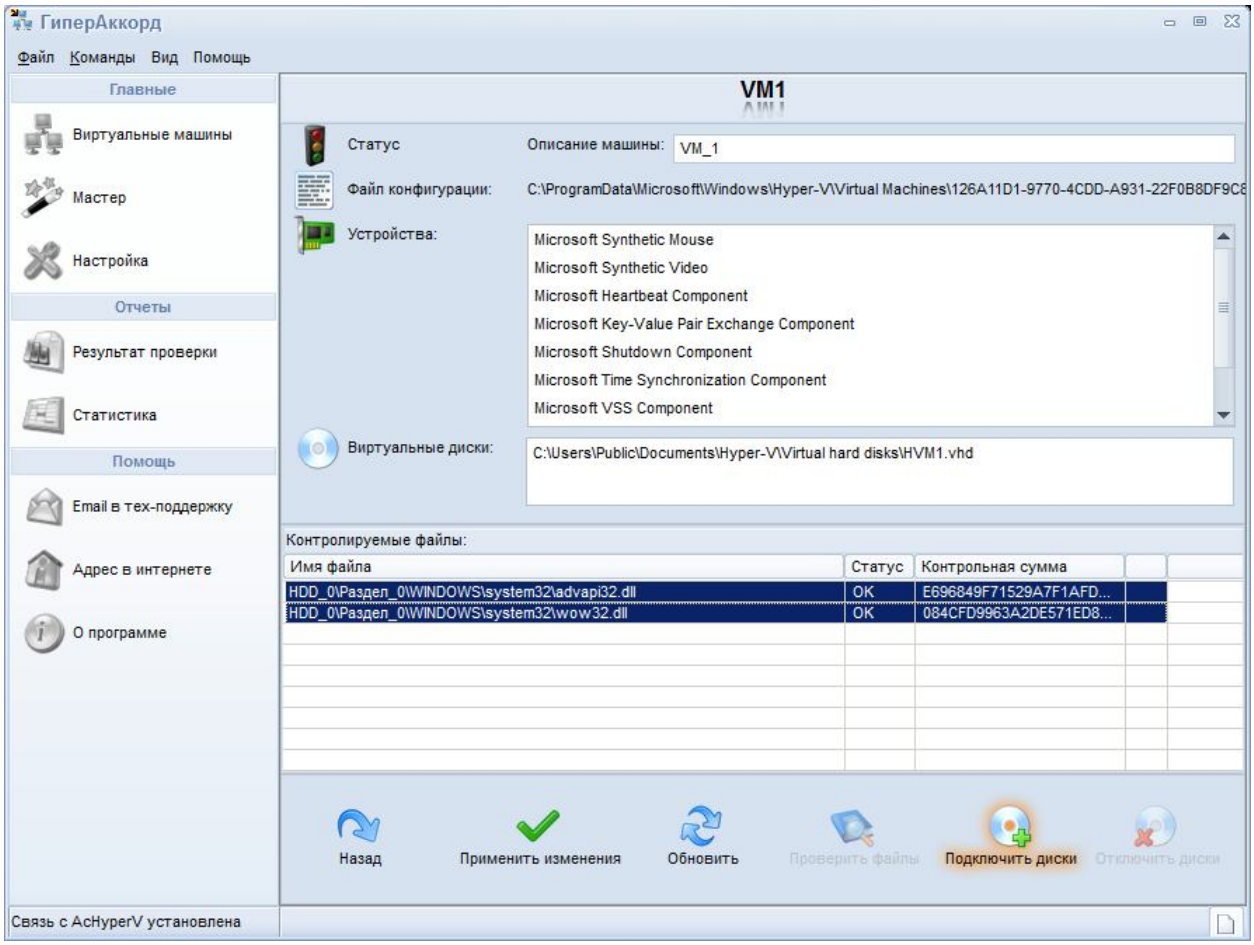

Рисунок 7 – Рассчитанные КС для файлов

После того как расчет контрольных сумм для всех необходимых файлов выполнен, следует нажать кнопку <Применить изменения>, для того чтобы изменения в списке вступили в силу (рисунок 7), – происходит автоматический возврат на вкладку «Виртуальные машины» главного окна программы (рисунок 4).

2.3.4 Проверка целостности файлов ВМ

Для выполнения процедуры проверки целостности файлов ВМ следует во вкладке «Виртуальные машины» главного окна программы выбрать нужную ВМ и нажать кнопку <Конфигурация виртуальной машины> (рисунок 4). В появившемся далее окне следует нажать кнопку <Проверить файлы> (рисунок 7).

В случае если целостность не нарушена, на экран выводится сообщение о том, что ошибок при проверке КС не обнаружено (рисунок 8).

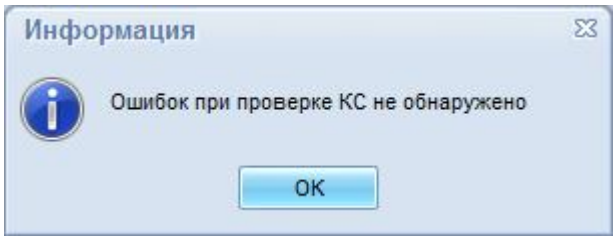

Рисунок 8 – Сообщение об отсутствии ошибок при проверке КС

При нарушении целостности виртуальная машина, поставленная на контроль, не запускается. Причина, по которой ВМ не стартовала (например, появление нового оборудования или нарушение целостности файлов ОС этой виртуальной машины), приводится в отчете о проверке виртуальных машин (см. рисунок 13 в п. 2.3.7.1).

При проверке целостности файлов каталоги с измененными файлами или сами файлы подсвечиваются красным цветом. Список измененных файлов отображается также в сообщениях из полученного журнала. После выяснения причин изменения файлов необходимо пересчитать КС.

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

2.3.5 Работа во вкладке «Мастер»

Мастер позволяет автоматически находить новые виртуальные машины и устанавливать на контроль рекомендуемый список файлов (рисунок 9).

При выборе в главном окне программы вкладки «Мастер», в каталоге, указанном в поле «Каталог с описанием виртуальных машин» автоматически происходит поиск ВМ. В случае если найдена ВМ, отсутствующая в базе (вкладка «Виртуальные машины» главного окна программы), такая машина добавляется в список «Новые виртуальные машины» (рисунок 9).

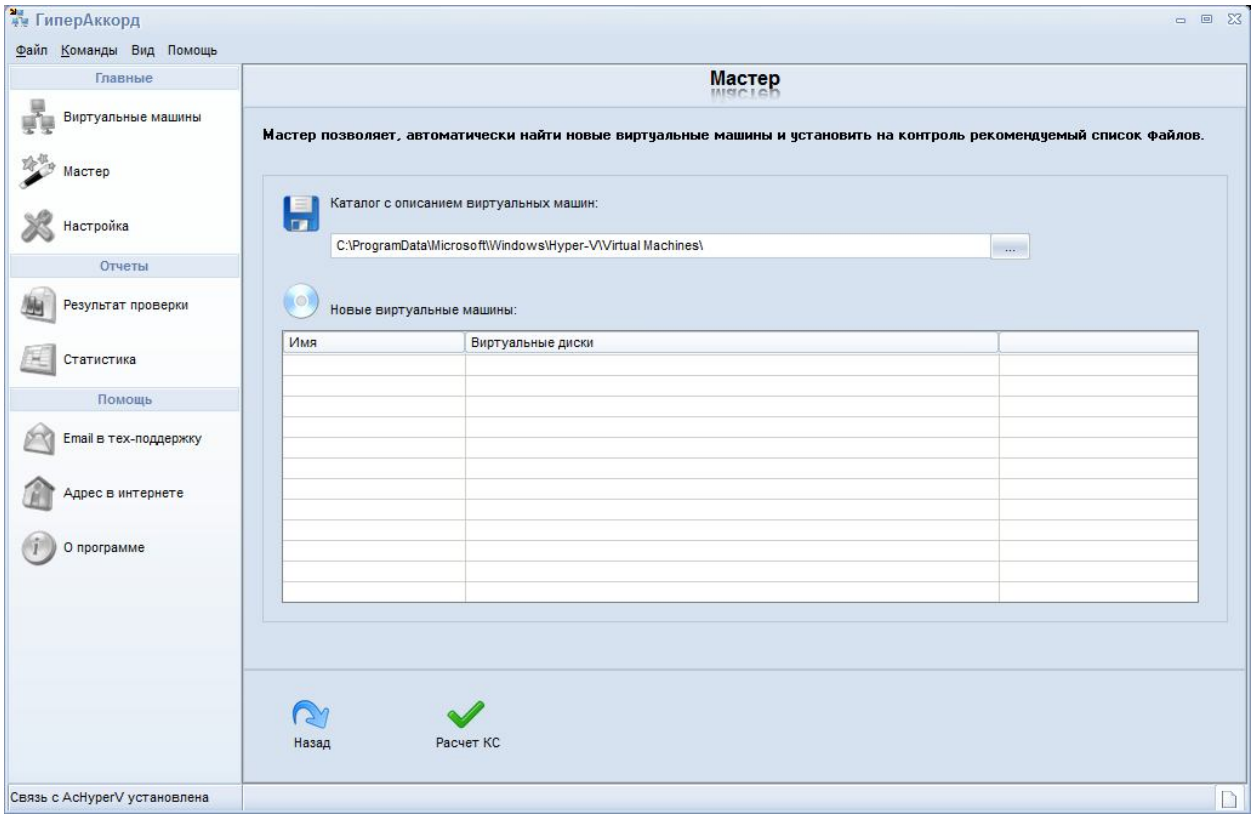

Рисунок 9 - Главное окно программы. Вкладка «Мастер»

Далее можно нажать кнопку «Расчет КС» – в базу автоматически добавятся выбранные ВМ и на контроль целостности установятся их файлы, указанные в файле WinXP.hsh (или Win7.hsh – в зависимости от версии ОС, установленной на ВМ).

2.3.6 Настройка системы контроля запуска ВМ

Для настройки системы контроля запуска ВМ следует в главном окне программы выбрать вкладку «Настройка» и установить галочку «Включить систему контроля запуска виртуальных машин» (рисунок 10).

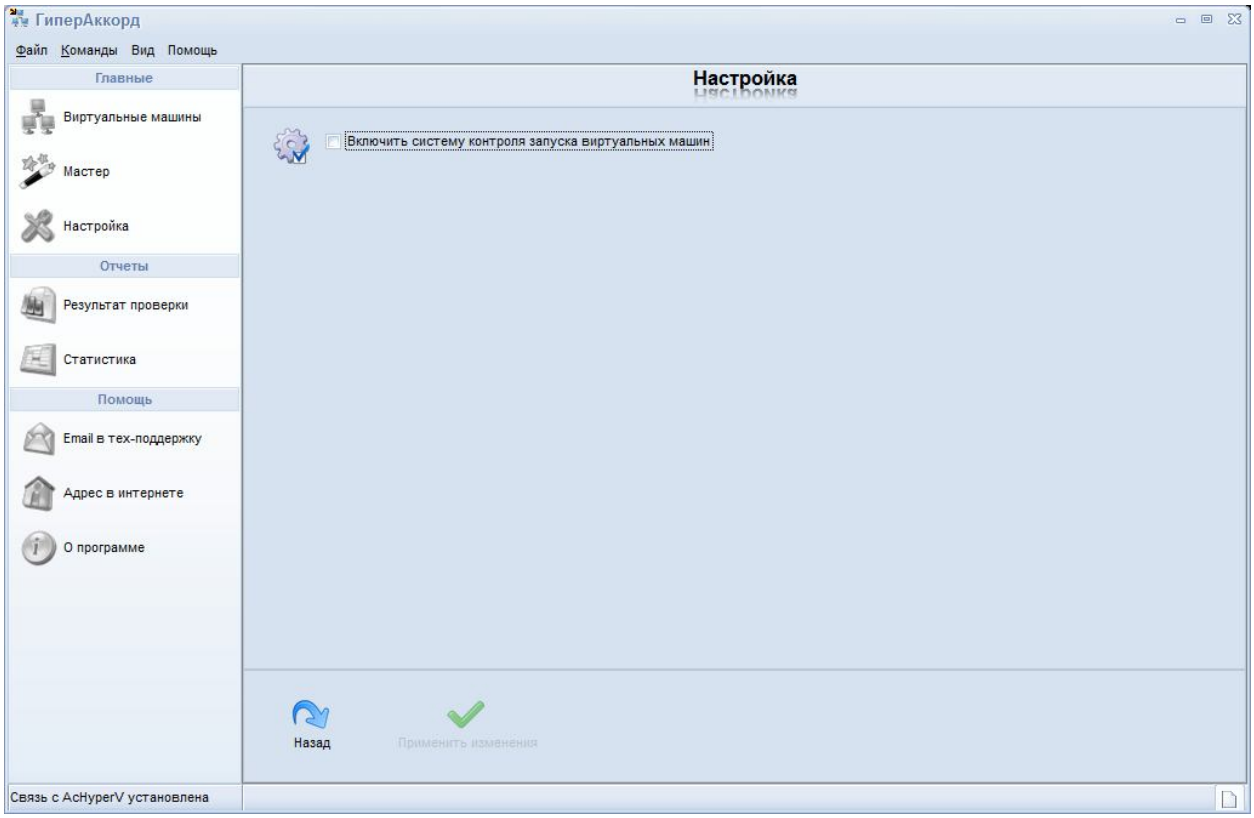

Рисунок 10 – Вкладка «Настройка»

В появившемся далее списке (рисунок 11) можно выполнить следующие настройки:

- блокировка запуска незарегистрированных машин – посредством установки соответствующей галочки;
- расположение файла с протоколированием результатов проверки – посредством выбора нужного каталога с помощью кнопки <…> в поле «Протоколировать результаты в:»;
- расположение каталога с базами виртуальных машин – посредством выбора нужного каталога с помощью кнопки <…> в поле «Каталог с базами виртуальных машин»;
- время задержки (в секундах) после подключения дисков;
- запуск СПО «ГиперАккорд» при включении компьютера – посредством установки соответствующей галочки;
- запуск СПО «ГиперАккорд» свернутым в системный трей – посредством установки соответствующей галочки.

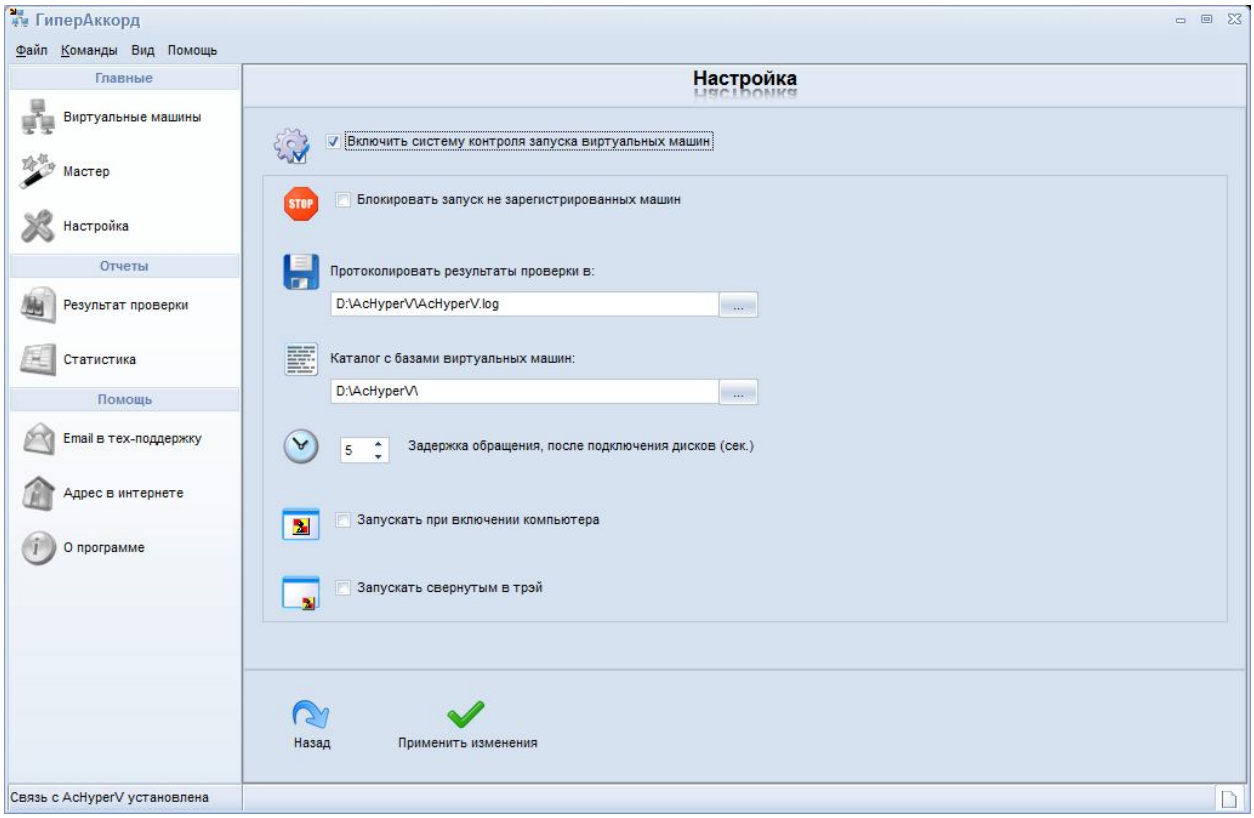

Рисунок 11 – Вкладка «Настройка» главного окна программы

Для того чтобы изменения вступили в силу, необходимо нажать кнопку <Применить изменения> и затем выполнить перезагрузку компьютера (рисунок 12).

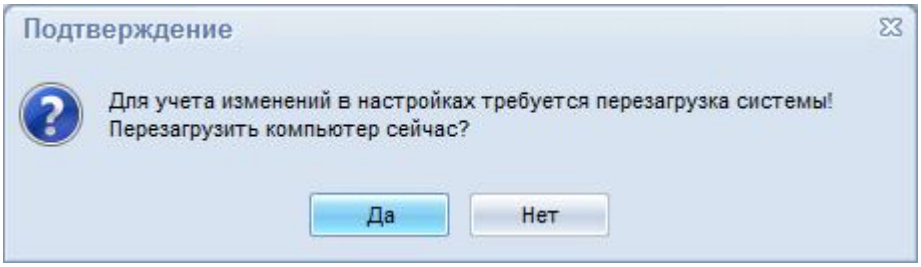

Рисунок 12 – Сообщение о необходимости перезагрузить компьютер

2.3.7 Отчеты о работе комплекса с виртуальными машинами

2.3.7.1 Отчет о проверке виртуальных машин

Для обеспечения возможности мониторинга работы ПАК «ГиперАккорд» с виртуальными машинами в ПО ПАК «ГиперАккорд» ведется журнал регистрации событий, представляющий собой отчет о проверке виртуальных машин, окно просмотра которого показано на рисунке 13.

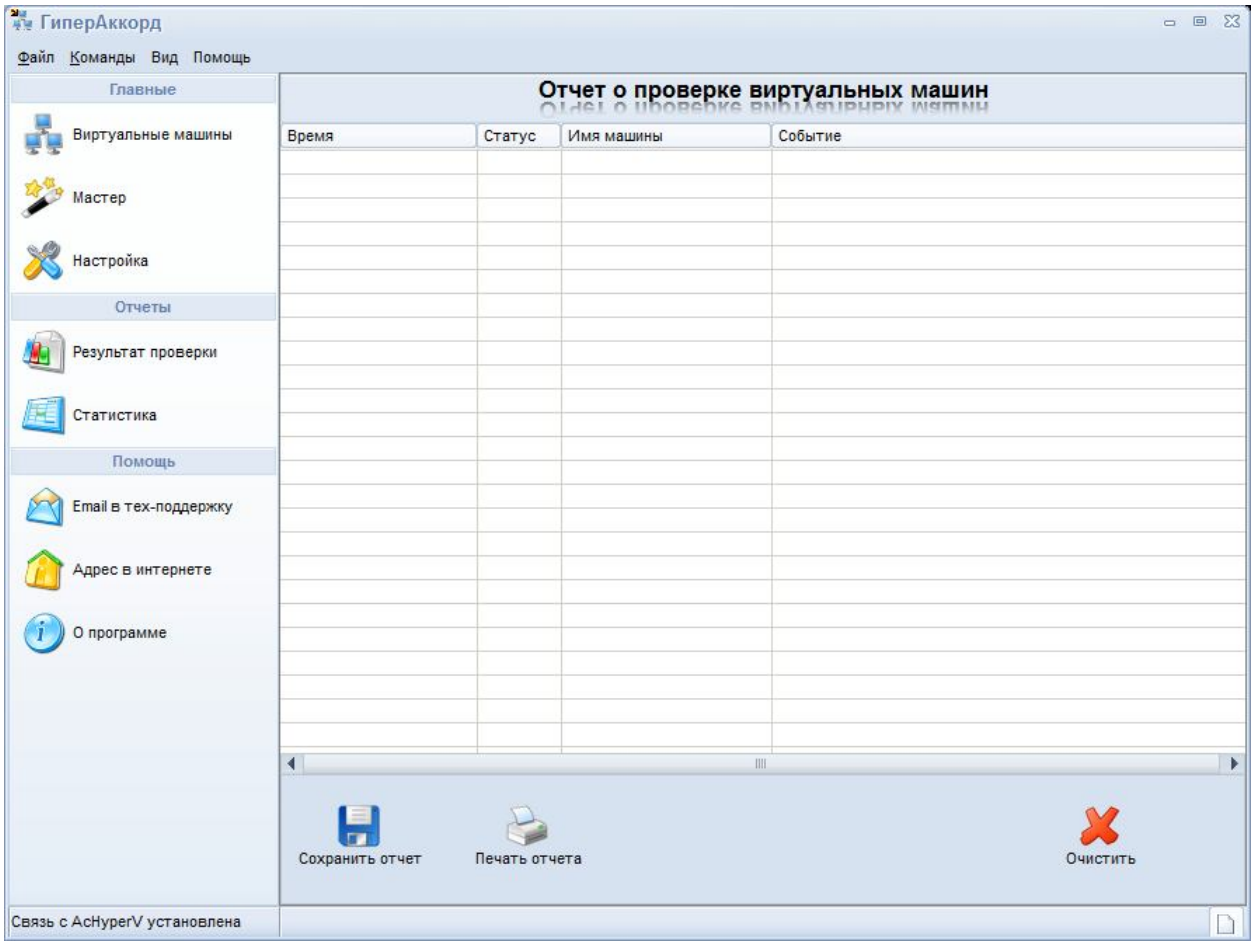

Рисунок 13 - Отчет о проверке виртуальных машин

Открыть отчет о проверке виртуальных машин можно посредством выбора вкладки «Результат проверки» в главном окне программы (рисунок 13).

Окно просмотра отчета о проверке виртуальных машин содержит следующую информацию:

- время – время, когда произошло событие, зафиксированное в процессе работы ПАК «ГиперАккорд» с виртуальными машинами, установленными на данном сервере HV;
- статус – статус события, произошедшего с ВМ;
- имя машины – имя виртуальной машины, действия с которой отражены в отчете;
- событие – информация о событиях.

Имеется возможность сохранить отчет в файл посредством нажатия кнопки <Сохранить отчет> или вывести его на печать посредством нажатия кнопки <Печать отчета>.

В случае необходимости, содержание отчета о проверке ВМ можно очистить, нажав кнопку <Очистить>.

2.3.7.2 Статистика

Работа с вкладкой «Статистика» в главном окне программы пока не доступна. Данная функция находится в разработке и будет доступна в ближайшем будущем.

2.3.8 Помощь в работе с СПО «ГиперАккорд»

В главном окне программы предусмотрен быстрый доступ к функциям помощи работы с ПАК «ГиперАккорд» (рисунок 14).

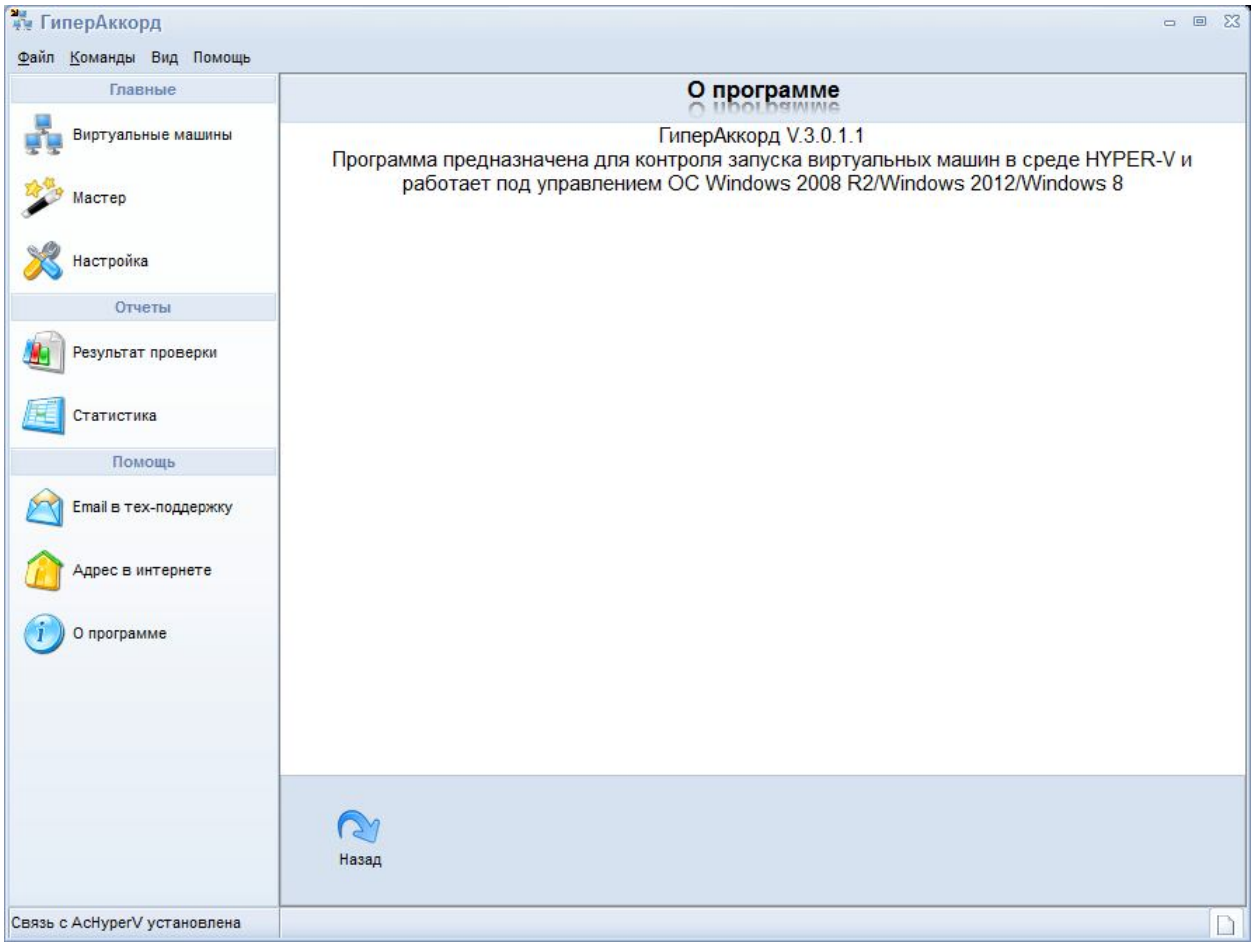

Рисунок 14 - Главное окно программы. Вкладка «О программе»

В случае возникновения каких-либо вопросов, имеется возможность написать e-mail в техподдержку, нажав в меню «Помощь» главного окна программы кнопку <E-mail в техподдержку> (данная функция доступна в том случае, если на компьютере установлен почтовый клиент). По нажатии кнопки <E-mail в техподдержку> на экране открывается окно почтового клиента с введенным адресом технической поддержки в поле «Получатель».

Возможно, что для того чтобы получить ответы на некоторые вопросы, достаточно будет посетить наш сайт в Интернете – www.okbsapr.ru. Для этого следует нажать кнопку <Адрес в интернете> – запустится Internet Explorer с открытой главной страницей сайта www.okbsapr.ru. Контакты ОКБ САПР

доступны в разделе сайта «Контакты». Сведения о технической поддержке см. также в разделе 3.

Версию установленного ПО «ГиперАккорд» всегда можно посмотреть во вкладке «О программе» главного окна программы (рисунок 14).

2.3.9 Особенности работы с «Аккорд-АМДЗ» на сервере HV и «Аккорд-Win32 TSE», «Аккорд-Win64 TSE» на виртуальных машинах

Процедуры администрирования «Аккорд-АМДЗ» и «Аккорд-Win32 TSE», «Аккорд-Win64 TSE», установленных на виртуальных машинах, описаны в соответствующих разделах документации на «Аккорд-АМДЗ» и «Аккорд-Win32», «Аккорд-Win64» соответственно (состав документации описан в подразделе 2.1).

При работе с «Аккорд-АМДЗ» на сервере HV и «Аккорд-Win32 TSE», «Аккорд-Win64 TSE» на виртуальных машинах следует учитывать два принципиальных обстоятельства:

1) на сервере HV необходимо (с помощью «Аккорд-АМДЗ») устанавливать на контроль СПО «ГиперАккорд». Для этого необходимо установить на контроль папку AcHyperV;

2) «Аккорд-Win32 TSE», «Аккорд-Win64 TSE», устанавливаемые в виртуальные машины, идентичны «Аккорду-Win32», «Аккорду-Win64» соответственно, за исключением того, что «Аккорд-Win32 TSE», «Аккорд-Win64 TSE», устанавливаемые в виртуальные машины, в процессе функционирования не синхронизируются с контроллером «Аккорд-АМДЗ».

2.4 Работа на клиентских рабочих местах

Работа на клиентских рабочих местах производится пользователем ПАК «ГиперАккорд» в соответствии с «Руководством пользователя» (11443195.4012.057 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.

3 Техническая поддержка и информация о комплексе

В случае необходимости консультации ЗАО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам: (495) 994-49-97, 8-926-762-17-72 или по адресу электронной почты help@okbsapr.ru. Наш адрес в Интернете http://www.okbsapr.ru/.