ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Руководство пользователя

11443195.4012.028-34

Листов 11

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством пользователя программно-аппаратного комплекса СЗИ НСД «Аккорд-В.» v.1.3 (далее по тексту – ПАК «Аккорд-В.», либо «Аккорд-В.»), 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.

В документе приведено описание особенностей работы пользователей инфраструктуры виртуализации с использованием средств комплекса «Аккорд-В.».

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

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.

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

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 Состав ПАК «Аккорд-В.»

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

1.1.1 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 оговаривается при поставке комплекса.

1.1.2 Программные средства

Программные средства ПАК «Аккорд-В.»:

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

1) модули СПО «Аккорд-В.»:

[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

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, 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.

1.2 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)*.

1.3 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 1.2;
- 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 Работа пользователя ПАК «Аккорд-В.»

2.1 Общие сведения

Работа пользователя ПАК «Аккорд-В.» с виртуальными машинами, входящими в состав защищенной инфраструктуры виртуализации, производится на клиентских рабочих местах и сводится к выполнению

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

пользовательских функций модуля «Аккорд-Win32 TSE» / «Аккорд-Win64 TSE» / «Аккорд-X» /«Аккорд-XL» (далее по тексту – «Аккорд»), установленного в виртуальной машине.

2.2 Порядок работы на защищенной ВМ

Процесс работы пользователя ПАК «Аккорд-В.» можно разделить на 3 этапа:

1) выполнение контрольных процедур;

2) работа пользователя в соответствии с функциональными обязанностями и правами доступа;

3) завершение работы и выход из системы.

2.3 Выполнение контрольных процедур

Контрольные процедуры делятся на обязательные, выполняемые при каждом запуске ВМ, и необязательные, выполняемые при выполнении заданных условий.

К обязательным процедурам относятся:

- процедура идентификации;
- процедура аутентификации;
- проверка целостности системных областей, системных файлов, программ и данных ВМ.

К необязательным процедурам относится процедура смены пароля, выполняемая, когда время жизни пароля превысило установленный администратором БИ интервал времени и проверка ограничения на время входа в систему.

2.3.1 Процедура идентификации

При загрузке ВМ, защищенной комплексом «Аккорд-В.», управление перехватывает модуль «Аккорд-В.», и на экран выводится сообщение с требованием выполнить процедуру идентификации.

Процесс выполнения процедуры идентификации описан в соответствующих подразделах документации, входящей в комплект поставки комплексов:

- «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).

2.3.2 Процедура аутентификации

После идентификации пользователя, при условии, что ему при регистрации был задан пароль для входа в систему, пользователь проходит процедуру аутентификации.

Процесс выполнения процедуры аутентификации описан в соответствующих подразделах документации, входящей в комплект поставки комплексов:

- «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).

2.3.3 Проверка целостности системных областей, системных файлов, программ и данных ВМ

Данная процедура осуществляется до загрузки ОС виртуальной машины и предназначена для исключения несанкционированных модификаций (случайных или злоумышленных) программной среды ВМ, системных областей и системных файлов ОС, обрабатываемых пользователем данных, если они поставлены на контроль целостности.

При проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным значением.

2.3.4 Смена пароля

Смена пароля производится в случае, когда время действия пароля превысило отведенный интервал, или в случае его компрометации. Время действия пароля устанавливается администратором БИ при регистрации пользователя либо при последующем администрировании системы. По решению администратора БИ пользователю может предоставляться право самостоятельной смены пароля.

Процесс выполнения процедуры смены пароля описан в соответствующих подразделах документации, входящей в комплект поставки комплексов:

- «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)..

2.3.5 Проверка ограничения на время входа в систему

Администратор может установить временной интервал (по дням недели с дискретностью 0.5 часа), в который вход в гостевую ОС ВМ данному пользователю запрещен. Если для пользователя установлены такие ограничения, то при попытке загрузки в неположенное время после процедуры

идентификации/аутентификации и контроля целостности выводится сообщение о том, что в данное время вход в систему запрещен.

2.4 Работа пользователя в соответствии с функциональными обязанностями

После выполнения контрольных процедур выполняется загрузка операционной системы, и пользователь может приступить к работе, определяемой его функциональными обязанностями и правами доступа к ресурсам ВМ.

При регистрации пользователя для него создается функционально замкнутая программная среда, которая позволяет контролировать права доступа пользователя к объектам доступа.

2.4.1 Проверка полномочий пользователя на доступ

Проверка полномочий пользователя на доступ выполняется при запуске пользователем какой-либо программы или при попытке получить доступ к какому-либо ресурсу. Средствами комплекса «Аккорд» выполняется проверка полномочий пользователя, которая заключается в том, что в списке прав доступа пользователя осуществляется поиск описания данного ресурса.

Если в списке прав доступа пользователя разрешена работа с данной программой или файлом, то пользователь может легально работать в соответствии со своими функциональными обязанностями.

Если в списке прав доступа пользователя не разрешена работа с данной программой или файлом (или ограничен набор функций, которые может выполнить пользователь с данным ресурсом), то выводится стандартное сообщение операционной системы, например: «Файл не найден», «Невозможно удалить файл» и т. д.

2.4.2 Работа с хранителем экрана

Для временной блокировки компьютера по истечении установленной паузы в работе пользователя или с помощью «горячих» клавиш в комплексе используется процедура гашения экрана.

Подробнее данная процедура описана в соответствующих подразделах документации, входящей в комплект поставки комплексов:

- «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)..

2.5 Завершение работы и выход из системы

Завершение работы прикладных программ происходит в порядке, установленном для конкретного прикладного программного обеспечения,

описанном в соответствующих руководствах. Никаких специфических окон или сообщений «Аккорд» при этом не выводит. Перед завершением работы ОС выводится окно с заголовком «Комплекс Аккорд» и остается на экране, пока монитор разграничения доступа не завершит корректно свою работу.

3 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 accord-v.ru.

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