ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Специальное программное обеспечение «Аккорд-В.»

Руководство пользователя

37222406.26.20.40.140.086 34

Листов 10

Москва
2020

АННОТАЦИЯ

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

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

Перед началом эксплуатации СПО «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 «Аккорд-В.».

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

АРМ - автоматизированное рабочее место.

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

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

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

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 Назначение СПО «Аккорд-В.»

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

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

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

– управления размещением и перемещением исполняемых виртуальных машин между контролируемыми СПО «Аккорд-В.» серверами виртуализации путем контроля запуска ВМ.

1.2 Состав СПО «Аккорд-В.»

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

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

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

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

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

1.3 Технические условия применения СПО «Аккорд-В.»

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

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

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

2 Работа пользователя СПО «Аккорд-В.»

2.1 Общие сведения

Работа пользователя СПО «Аккорд-В.» с виртуальными машинами, входящими в состав защищенной инфраструктуры виртуализации, производится на клиентских рабочих местах и сводится к выполнению пользовательских функций модуля «Аккорд-Win64 К» / «Аккорд-X К», установленного в виртуальной машине.

2.2 Порядок работы на защищенной ВМ

Процесс работы пользователя «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 времени входа в систему.

2.3.1 Процедура идентификации

При загрузке ВМ, защищенной СПО «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 на модули, используемые для разграничения доступа.

2.3.2 Процедура аутентификации

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

Процесс выполнения процедуры аутентификации описан в соответствующих подразделах документации на модули, используемые для разграничения доступа.

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 на модули, используемые для разграничения доступа.

2.3.5 Проверка ограничения времени 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 «Аккорд-В.» 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 используется процедура гашения экрана.

Подробнее данная процедура описана в соответствующих подразделах документации на модули, используемые для разграничения доступа.

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-В.» 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

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

+7(495) 994-49-96,

+7(495) 994-49-97,

+7(926) 235-89-17,

+7(926) 762-17-72.