ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Руководство (оператора) пользователя

11443195.4012.057 34

Листов 9

Москва
2016

АННОТАЦИЯ

Настоящий документ является руководством пользователя 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.

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

Перед началом эксплуатации ПАК «ГиперАккорд» 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 «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 для 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 инфраструктур виртуализации.

Система защиты «ГиперАккорд» полностью интегрируется в инфраструктуру виртуализации (построенную на базе платформ Hyper-V), 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.

Комплекс СЗИ НСД «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 средств и программных средств (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.

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 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 100 Мбайт *(*на сервере HV*).*

2 Работа пользователя ПАК «ГиперАккорд»

2.1 Общие сведения

Работа пользователя ПАК «ГиперАккорд» с виртуальными машинами, входящими в состав защищенной инфраструктуры виртуализации, производится на клиентских рабочих местах и сводится к выполнению пользовательских функций СПО «Аккорд-Win32 TSE»/«Аккорд-Win64 TSE» для виртуальных машин (в зависимости от установленной в ВМ ОС) (далее по тексту – «Аккорд»), установленного в виртуальной машине.

2.2 Порядок работы на защищенной ВМ

Процесс работы пользователя ПАК «ГиперАккорд» 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 подключении к ВМ, и необязательные, выполняемые при выполнении заданных условий.

К обязательным процедурам относятся

- процедура идентификации;
- процедура аутентификации.

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 подключении к ВМ, защищенной комплексом «ГиперАккорд», управление перехватывает СПО «ГиперАккорд», и на экран выводится сообщение с требованием выполнить процедуру идентификации.

Процесс выполнения процедуры идентификации описан в соответствующем подразделе «Руководства пользователя Аккорд-Win32»

(11443195.4012.036 34) (или «Руководства пользователя Аккорд-Win64» (11443195.4012.037 34)).

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 соответствующем подразделе «Руководства пользователя Аккорд-Win32» (11443195.4012.036 34) (или «Руководства пользователя Аккорд-Win64» (11443195.4012.037 34)).

2.3.3 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 соответствующем подразделе «Руководства пользователя Аккорд-Win32» (11443195.4012.036 34) (или «Руководства пользователя Аккорд-Win64» (11443195.4012.037 34)).

2.3.4 Проверка ограничения на время входа в систему

Администратор может установить временной интервал (по дням недели с дискретностью 0.5 часа), в который загрузка данной ВМ данным пользователем запрещена. 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, и загрузка ОС не производится.

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 по доступу

Проверка полномочий по доступу 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 соответствующем подразделе «Руководства пользователя Аккорд-Win32» (11443195.4012.036 34) (или «Руководства пользователя Аккорд-Win64» (11443195.4012.037 34)).

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

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/.