ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Руководство пользователя

11443195.4012.069 34

Листов 8

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством пользователя модуля разграничения доступа к vCenter и ESXi – программно-аппаратного комплекса (ПАК) «Сегмент-В.» v.1.3 (далее по тексту – «Сегмент-В.» или комплекс), предназначенного для защиты инфраструктуры виртуализации на основе VMware vSphere версий 5.1, 5.5, 6.0.

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

Перед началом эксплуатации комплекса 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 модуля «Сегмент-В.» должно дополняться общими мерами предосторожности и физической безопасности.

СОДЕРЖАНИЕ

1. Общие сведения.....5
1.1. Назначение комплекса 5
1.2. Состав ПАК «Сегмент-В.».....5
1.2.1. Аппаратные средства.....6
1.2.2. Программные средства.....6
1.3. Технические условия применения комплекса.....7
2. Работа пользователя с установленным ПАК «Сегмент-В.».....8
3. Техническая поддержка и информация о комплексе 8

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.

Сервер виртуализации (или хост) – объект виртуальной инфраструктуры, предоставляющий доступ к платформе виртуализации (гипервизору) посредством команд управления.

Сервер управления виртуальной инфраструктурой (vCenter) – сервер со специализированным программным обеспечением, отвечающий за распределение нагрузки в автоматическом режиме, перемещение виртуальных машин (миграцию) и настройку всех компонентов виртуализации посредством посылки команд управления остальным элементам виртуальной инфраструктуры.

Сетевое устройство (сеть, группа портов) – сеть, разделяемая между хостами и/или виртуальными машинами; может быть физической (подключена к физической сетевой карте) или логической (VLAN).

Хранилище – виртуальное представление физического хранилища, является местом хранения файлов виртуальных машин. Хранилище скрывает особенности своей физической реализации и предоставляет единую модель для хранения виртуальных машин.

Пользователь – субъект доступа к объектам (ресурсам) виртуальной инфраструктуры.

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 «Сегмент-В.» предназначен для защиты инфраструктур виртуализации, построенных на базе платформ виртуализации:

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

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

- идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
- управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре.
- регистрации событий безопасности в виртуальной инфраструктуре.
- управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.
- разбиения виртуальной инфраструктуры на сегменты (сегментирования виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

1.2. Состав ПАК «Сегмент-В.»

ПАК «Сегмент-В.» представляет собой комплекс программных и аппаратных средств, предназначенный для разграничения доступа пользователей к объектам инфраструктуры виртуализации VMware vSphere. При этом комплекс обеспечивает защиту от утечек информации, предоставляя возможность работы под одной учетной записью с различными сегментами виртуальной инфраструктуры (ВИ), запрещая их смешивание.

Основу комплекса составляет прокси-сервер, устанавливаемый в разрыв между vCenter сервером и рабочим местом администратора виртуальной инфраструктуры (АВИ).

Прокси-сервер представлен в следующих исполнениях:

1) аппаратное исполнение: физический сервер с предустановленным ПО;
2) программное исполнение: ISO-образ, предназначенный:

- для установки в ВМ;
- для установки на сторонний сервер организации-Заказчика.

ВНИМАНИЕ! В случае использования варианта исполнения, предназначенного для установки на сторонний сервер организации-Заказчика, следует учитывать, что аппаратная часть стороннего сервера должна быть совместима с базовой сборкой CentOS 6.5 и поддерживать работу с «Аккорд-АМДЗ».

«Сегмент-В.» не требует установки дополнительного ПО на АРМ администраторов виртуальной инфраструктуры и позволяет «бесшовно» интегрировать систему защиты в инфраструктуру виртуализации vSphere. При этом поддерживается режим Linked mode для vCenter, а также сохраняется возможность использования vCenter в качестве ВМ (в том числе VCSA – VMware vCenter Server Appliance).

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

1.2.1. Аппаратные средства

Аппаратные средства ПАК «Сегмент-В.» включают в себя следующие компоненты:

- физический сервер Aquarius T40 S24 (опционально; возможны варианты использования собственных серверов);
- установленная в сервер (Aquarius T40 S24 или собственный сервер) плата «Аккорд-АМДЗ» семейства GX (подробнее см. документацию на «Аккорд-АМДЗ»);
- usb -> Ethernet адаптер – поставляется (опционально) в составе решения для использования функционала отказоустойчивости (High Availability).

1.2.2. Программные средства

Программные средства ПАК «Сегмент-В.» включают в себя следующие компоненты:

1) модули СПО «Сегмент-В.»:

а) *ПО управления комплексом* **Segment-V. (exe)**, устанавливаемое на АРМ Администратора БИ (АРМ АБИ), предназначенное для настройки разграничения доступа к виртуальной инфраструктуре. Может устанавливаться отдельно или как расширение «СПО Аккорд-В.». Включает в себя следующие утилиты:.

- «Segment-V.» – утилита управления комплексом «Сегмент-В.»;
- «Installer-V.» – утилита настройки соединения с vCenter, а также точек сбора событий с прокси-серверов (в случае совместного использования с «Аккорд-В.» используется также для установки агентов «Аккорд-В.» на ESXi);
- «LogViewer-V.» – утилита 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) Segment-V. Module (iso) – *прокси-сервер* – специально настроенный образ операционной системы, устанавливаемый на физический сервер или внутрь ВМ, предназначенный для перехвата команд управления vCenter/ESXi и организации разграничения доступа на основе заранее заданных правил. Segment-V. Module включает в себя СПО *«Аккорд-X»*, применение которого на прокси-сервере обеспечивает выполнение процедур идентификации и аутентификации пользователей root и accord, а также выполнение динамического контроля целостности исполняемых файлов из состава ПАК «Сегмент-В.».

Примечание: В случае программного исполнения (ВМ), в силу невозможности использования контроллеров «Аккорд-АМДЗ», рекомендуется использовать ПАК «Аккорд-В.».

1.3. Технические условия применения комплекса

Для установки комплекса «Сегмент-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;
- 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];
- наличие ресурсов на сервере для создания ВМ и установки в нее ОС прокси-сервера или наличие x86-64 совместимого сервера[2] с требованиями, аналогичными предъявляемым к ВМ.

Минимальные системные требования к ВМ:

- двухъядерный процессор, 2 Гб ОЗУ, 16 Гб свободного места на диске;
- две сетевых карты (E1000) – в случае использования одного прокси-сервера;
- три сетевых карты (E1000) – в случае использования механизмов резервирования;
- USB контроллер – для подключения устройства хранения с сертификатами;

Для корректной работы сервиса регистрации событий может потребоваться, чтобы АРМ, на котором он запущен, был включен в домен (если АРМ совпадает с vCenter, то возможно использование локальной учетной записи) (подробнее см. «Руководство по установке» (11443195.4012.069 98)).

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

[2)] В зависимости от варианта исполнения ПАК «Сегмент-В.», может входить в комплект поставки

Необходимо организовать схему подключения, при которой все запросы к vCenter и ESXi будут проходить через прокси-сервер (чтобы не существовало путей в обход модуля «Сегмент-В.»).

2. Работа пользователя с установленным ПАК «Сегмент-В.»

Работа пользователя ПАК «Сегмент-В.» производится на клиентских рабочих местах и сводится к выполнению функциональных обязанностей пользователя VMware vSphere (через подключение к vCenter при помощи vClient) в соответствии с установленными для него правами доступа к ресурсам ВИ.

В своей работе пользователь может столкнуться со следующими ситуациями, связанными с функционированием ПАК «Сегмент-В.»:

1) При выполнении какого-либо действия появление на экране следующего сообщения:

```
Task was blocked by Segment-V
```

означает, что АБИ заблокировал данное действие для пользователя. Если пользователь уверен, что действие заблокировано ошибочно, следует обратиться к АБИ.

2) При попытке включения ВМ, включение которой запрещено пользователю средствами ПАК «Сегмент-В.», и при попытке изменения virtual adapter для Distributed Switch действия блокируются. При этом на экран не выводятся никакие информационные сообщения, в том числе сообщение, указанное в п.1. Такое поведение связано с реализацией работы vSphere.

В остальном работа прикладных программ происходит в порядке, установленном для конкретного прикладного программного обеспечения, описанном в соответствующих руководствах. Никаких специфических окон или сообщений «Сегмент-В.» при этом не выводит.

3. Техническая поддержка и информация о комплексе

Все вопросы, связанные с поддержкой ПАК «Сегмент-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

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