



КОД БЕЗОПАСНОСТИ

Средство защиты информации

vGate R2

Руководство администратора

Принципы функционирования



КОД БЕЗОПАСНОСТИ

© Компания "Код Безопасности", 2020. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес: **115127, Россия, Москва, а/я 66**
ООО "Код Безопасности"

Телефон: **8 495 982-30-20**

E-mail: **info@securitycode.ru**

Web: **https://www.securitycode.ru**

Оглавление

Список сокращений	4
Введение	5
Описание vGate	6
Принципы и средства защиты	6
Защита средств управления виртуальной инфраструктурой	6
Механизмы защиты виртуальных машин	7
Правила использования лицензий	8
Архитектура vGate	9
Компоненты vGate	9
Варианты размещения компонентов	10
Особенности установки vGate при разных архитектурах vCSA	11
Функциональные возможности vGate	15
Разделение административных функций	16
Полномочное управление доступом к конфиденциальным ресурсам	16
Виды меток безопасности	17
Управление уровнем конфиденциальности	17
Операции, регламентируемые функцией управления доступом	17
Порядок назначения меток безопасности	19
Варианты применения функции управления доступом	20
Политики безопасности	22
Контроль целостности и доверенная загрузка	22
Регистрация событий информационной безопасности	23
Централизованное управление и аудит	23
Подготовка отчетов	23
Автоматизация развертывания	23
Управление несколькими серверами авторизации	24
Синхронизация настроек серверов авторизации	24
Резервирование сервера авторизации	24
Поддержка VMware Auto Deploy	24
Мониторинг безопасности	25
Сегментирование сети	25
Совместимость vGate с другими продуктами	26
Поддержка работы с VMware View	26
Поддержка работы со стандартным Distributed vSwitch и Distributed vSwitch	
Cisco Nexus 1000v	26
Решения для защиты виртуальных машин	26
Документация	27

Список сокращений

AD	Active Directory — служба каталогов MS Windows
DNS	Domain Name System (система доменных имен)
iSCSI	Internet Small Computer System Interface — протокол для управления системами хранения и передачи данных на основе TCP/IP
vCenter	Централизованное средство управления ESXi-серверами и виртуальными машинами
vCSA	vCenter Server Appliance — виртуальный модуль с установленным сервером vCenter и связанными с ним службами
PSC	Platform Services Controller — компонент, обеспечивающий работу служб виртуальной инфраструктуры VMware
АВИ	Администратор виртуальной инфраструктуры
АИБ	Администратор информационной безопасности
АС	Автоматизированная система
БД	База данных
ВМ	Виртуальная машина (англ. — VM)
Главный АИБ	Главный администратор информационной безопасности
ИБ	Информационная безопасность
НСД	Несанкционированный доступ
ОС	Операционная система
ОЗУ	Оперативное запоминающее устройство
ПО	Программное обеспечение
ПРД	Правила разграничения доступа
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СХД	Система хранения данных (англ. — SAN)
КЦ	Контроль целостности
ЦПУ	Центральное процессорное устройство

Введение

Актуальная версия эксплуатационной документации на изделие "Средство защиты информации vGate R2" находится на сайте компании по адресу

<https://www.securitycode.ru/products/vgate/documentation/>.

Последнюю версию Release Notes можно запросить по электронной почте vgateinfo@securitycode.ru.

Данное руководство предназначено для администраторов изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся общие сведения о назначении и функциональных возможностях vGate.

Документ предназначен для vGate версии 4.3.

Условные обозначения

В руководстве для выделения некоторых элементов текста используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.



- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.



- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.



- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Примечания могут не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в интернете. Вы можете посетить сайт компании "Код Безопасности" (<https://www.securitycode.ru/>) или связаться с представителями компании по электронной почте support@securitycode.ru.

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании <https://www.securitycode.ru/company/education/training-courses/>. Связаться с представителем компании по вопросам организации обучения можно по электронной почте education@securitycode.ru.

Глава 2

Описание vGate

vGate предназначен для обеспечения безопасности виртуальной инфраструктуры, развернутой с использованием системы виртуализации VMware vSphere.

Принципы и средства защиты

Защита средств управления виртуальной инфраструктурой

К средствам управления виртуальной инфраструктурой относятся:

- ESXi-серверы, предназначенные для запуска виртуальных машин.
- Серверы vCenter (vCSA), предназначенные для централизованного управления виртуальной инфраструктурой.
- vSphere Host Client — веб-клиент, предназначенный для управления серверами ESXi.
- Средства, предназначенные для обслуживания инфраструктуры, например, VMware Consolidated Backup, VMware Update Manager, vCenter Server Appliance.
- Сторонние средства мониторинга и управления инфраструктурой.

Компрометация любых из этих элементов может привести к компрометации группы виртуальных машин или всей виртуальной инфраструктуры.

Средства управления виртуальной инфраструктурой размещаются внутри периметра, защищаемого vGate. Для обеспечения их защиты от НСД в vGate предусмотрены следующие функции.

Функция	Описание
Аутентификация субъектов доступа	Аутентификация пользователей и компьютеров, которые пытаются получить доступ к защищаемым объектам, осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и предотвращающим вмешательство в передачу данных
Дискреционное разграничение доступа к средствам управления виртуальной инфраструктурой	Дискреционное разграничение доступа к объектам, которые размещены внутри защищаемого периметра, осуществляется на основе заданных списков управления доступом и параметров соединения (протоколов, портов). Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами подписывается, тем самым обеспечивается защита от атак типа Man in the Middle в процессе сетевого взаимодействия
Ограничение полномочий АИБ по управлению виртуальной инфраструктурой	Полномочия АИБ по управлению виртуальной инфраструктурой ограничены только возможностью просмотра конфигурации элементов виртуальной инфраструктуры. По умолчанию АИБ не имеет доступа к дискам VM и не может получить доступ к находящейся на них конфиденциальной информации. Паролей АВИ он также не знает, поскольку они в обязательном порядке должны быть изменены АВИ при первом входе в систему. Таким образом, АИБ не имеет возможности производить потенциально опасные действия с виртуальной инфраструктурой
Контроль действий АВИ	В vGate реализована возможность контроля действий АВИ на уровне отдельных команд управления виртуальной инфраструктурой

Функция	Описание
Блокирование доступа через веб-интерфейс в защищаемый периметр	Возможность доступа из внешней сети через браузер к элементам управления виртуальной инфраструктурой заблокирована. При необходимости доступ через веб-интерфейс может быть разрешен АИБ
Управляемые парольные политики	Управляемые парольные политики позволяют обеспечить соблюдение отраслевых требований к парольной защите
Полномочное управление доступом к конфиденциальным ресурсам	Функция полномочного управления доступом позволяет обеспечить более гранулированный доступ (по сравнению с дискреционным разграничением доступа) к конфиденциальным сведениям
Блокирование любого сетевого трафика со стороны ВМ к средствам управления виртуальной инфраструктурой	Обеспечивает защиту средств управления виртуальной инфраструктурой от НСД со стороны скомпрометированной виртуальной машины
Фильтрация сетевого трафика к vCenter внутри сети администрирования	На vCenter устанавливается компонент защиты, обеспечивающий фильтрацию входящего трафика. Функция обеспечивает защиту от несанкционированного доступа АБИ к средствам управления виртуальной инфраструктурой внутри сети администрирования
Обеспечение доверенной программной среды ESXi-сервера	Список исполняемых модулей, которые могут быть штатно запущены на ESXi-сервере, ограничен штатными модулями ESXi и штатными модулями vGate. При необходимости АИБ может расширить список программ, разрешенных для запуска на ESXi-сервере
Контроль монтирования устройств к ESXi-серверу	Контроль монтирования устройств к ESXi-серверу гарантирует невозможность присоединения к хосту переносных устройств, таких как USB-флеш-накопитель

Механизмы защиты виртуальных машин

Для обеспечения защиты ВМ и данных, обрабатываемых на них, предусмотрены следующие функции.

Функция	Описание
Контроль целостности ВМ и подробный аудит изменений в конфигурационном файле	Функция контроля целостности, включающая контроль целостности настроек ВМ перед ее загрузкой, снимков ВМ и образа BIOS виртуальной машины, а также контроль целостности шаблонов ВМ. Функция обеспечивает доверенную программную загрузку ВМ. Контроль целостности ВМ основан на неизменности контрольных сумм. Вместе с контролем целостности включается также подробный аудит изменений в vpx-файле защищаемой ВМ с возможностью отклонения изменений (при необходимости). Функции реализованы в рамках политик безопасности
Утверждение изменения конфигурации ВМ у АИБ	При изменении конфигурации у ВМ с включенным контролем целостности меняются контрольные суммы. У АИБ есть возможность принять или отклонить изменения конфигурации ВМ. При принятии изменений контрольная сумма ВМ пересчитывается
Запрет создания снимков (take snapshot)	Функция применяется для противодействия нарушению целостности работы систем, обрабатывающих данные ограниченного доступа. Реализована в рамках политик безопасности

Функция	Описание
Запрет клонирования VM	Функция позволяет ограничить несанкционированное копирование (клонирование) виртуальных машин, обрабатывающих данные ограниченного доступа. Реализована в рамках политик безопасности
Очистка памяти VM	Функция гарантирует отсутствие остаточной информации об обрабатываемых данных в памяти VM. Возможна как однократная, так и двукратная очистка памяти. Функция реализована в рамках политик безопасности
Затирание остаточных данных на СХД при удалении VM	Функция гарантирует отсутствие остаточной информации об обрабатываемых данных на жестких дисках после удаления VM. Затирание остаточных данных может выполняться посредством записи нулевых значений (однократной или двукратной). Реализована в рамках политик безопасности
Контроль подключаемых устройств	Функция позволяет ограничить возможность несанкционированного копирования данных с VM посредством подключения виртуальных устройств. Реализована в рамках политик безопасности
Ограничение доступа к консоли VM	Функция позволяет задать более строгие правила доступа к отдельной VM, заблокировав доступ к ее консоли. Реализована как привилегия пользователя
Ограничение скачивания файлов VM	С помощью данного механизма можно ограничить круг лиц, которым разрешено экспортировать файлы VM. Механизм реализован как привилегия пользователя

Правила использования лицензий

В vGate возможны следующие варианты лицензирования:

- vGate Standard;
- vGate Enterprise;
- vGate Enterprise Plus.

Для каждой из этих редакций лицензия приобретается на определенное количество физических процессоров (sockets), установленных на защищаемых ESXi-серверах. Редакции vGate различаются функциональными возможностями (см. стр. 15).

Для ознакомления с ПО vGate в демонстрационном режиме необходим ключ активации. Чтобы получить ключ активации для демонстрационной версии vGate, отправьте запрос с указанием редакции и срока действия лицензии по адресу vgateinfo@securitycode.ru.

Примечание. На указанный почтовый адрес вы также можете отправлять свои вопросы и пожелания, связанные с работой vGate. Вопросы, связанные с технической поддержкой, необходимо отправлять по адресу support@securitycode.ru.

Для использования vGate по истечении демонстрационного периода следует приобрести лицензию и зарегистрировать полученный ключ активации в консоли управления vGate. Ключи активации могут быть как бессрочные, так и ограниченного срока действия. Сведения о статусе того или иного ключа отображаются в консоли управления.

Глава 2

Архитектура vGate

Компоненты vGate

Компоненты vGate и их функции приведены в таблице ниже.

Компонент	Функции
Сервер авторизации	<ul style="list-style-type: none"> • Аутентификация пользователей и компьютеров. • Разграничение доступа к средствам управления виртуальной инфраструктурой. • Регистрация событий безопасности. • Хранение данных (учетной информации, журналов аудита и конфигурации vGate). • Репликация данных (при наличии резервного сервера). • Синхронизация настроек серверов авторизации. • Автоматическое развертывание компонентов защиты vGate на ESXi-серверах
Резервный сервер авторизации	<ul style="list-style-type: none"> • Хранение настроек и списка пользователей. • Репликация данных. • Возможность замены основного сервера при сбое
Агент аутентификации	<ul style="list-style-type: none"> • Идентификация и аутентификация пользователя. • Идентификация и аутентификация компьютера. • Контроль целостности компонентов агента аутентификации. • Выбор уровня сессии при работе с конфиденциальными ресурсами (при включенном контроле уровня сессий). • Регистрация событий безопасности
Модули защиты ESXi-сервера	<ul style="list-style-type: none"> • Контроль целостности и доверенная загрузка VM. • Контроль целостности модулей и настроек vGate. • Регистрация событий безопасности. • Защита от НСД внутри сети администрирования. • Контроль монтирования устройств. • Обеспечение доверенной программной среды
Компонент защиты vCenter	<ul style="list-style-type: none"> • Защита от НСД внутри сети администрирования. • Управление фильтрацией входящего трафика
Компонент защиты PSC	Защита от НСД внутри сети администрирования
Консоль управления	<ul style="list-style-type: none"> • Централизованное управление vGate. • Управление учетными записями пользователей и компьютеров. • Назначение прав доступа к защищаемым объектам. • Установка и настройка компонентов защиты ESXi-серверов, серверов vCenter. • Настройка полномочного управления доступом. • Настройка политик безопасности защищаемых объектов. • Расчет контрольных сумм конфигурации VM. • Настройка и просмотр журналов регистрации событий
Веб-консоль	<ul style="list-style-type: none"> • Настройка правил фильтрации сетевого трафика. • Мониторинг событий безопасности. • Настройка и просмотр журналов регистрации событий и отчетов
Сервер мониторинга	Сбор и корреляция событий виртуальной инфраструктуры
Средство просмотра отчетов	Формирование отчетов о состоянии параметров безопасности виртуальной инфраструктуры, произошедших событиях и внесенных в конфигурацию изменениях

Компонент	Функции
Служба развертывания vGate	Установка агентов vGate на защищаемые ESXi-серверы

Варианты размещения компонентов

Компоненты vGate могут размещаться следующим образом:

Компонент	Варианты размещения
Сервер авторизации	Выделенный компьютер (установка на VM допускается, но не рекомендуется)
Резервный сервер авторизации	Выделенный компьютер (установка на VM допускается, но не рекомендуется)
Агент аутентификации	Рабочее место АБИ, рабочее место АИБ (если рабочее место АИБ во внешнем периметре сети администрирования), серверы сервисных служб (DNS, AD и т. д.)
Модули защиты ESXi-сервера	ESXi-серверы
Компонент защиты vCenter	Сервер vCenter
Компонент защиты PSC	Сервер Platform Services Controller
Консоль управления	Сервер авторизации (если рабочее место АИБ на сервере авторизации), рабочее место АИБ
Средство просмотра отчетов	Сервер авторизации (если рабочее место АИБ на сервере авторизации), рабочее место АИБ
Служба развертывания vGate	Сервер vCenter
Сервер мониторинга	Виртуальная машина

Сервер авторизации устанавливается на специально выделенный для него компьютер. При установке сервера авторизации программа установки также по умолчанию предлагает установить на этот компьютер консоль управления. В данном случае этот компьютер может использоваться в качестве рабочего места АИБ.



Внимание! Установка сервера авторизации на VM допускается, но не рекомендуется по соображениям безопасности. Размещение сервера авторизации на VM может привести к неработоспособности системы. Например, в случае выхода из строя ESXi-сервера, на котором должна запускаться данная VM, возможен доступ к виртуальной инфраструктуре в обход сервера авторизации.

Если предполагается размещение сервера авторизации в серверном помещении (в целях соблюдения необходимых температурных условий или реализации организационных мер по защите компьютеров внутри защищаемого периметра), то рабочее место АИБ организуется на отдельном компьютере. В этом случае в состав клиентского ПО, помимо агента аутентификации, входит также консоль управления, которая должна быть установлена на компьютер АИБ.

Примечание. На другие компьютеры, входящие во внешний периметр сети администрирования, при установке клиентского ПО консоль управления не устанавливается.

Особенности установки vGate при разных архитектурах vCSA

vGate 4.3 может использоваться в виртуальных инфраструктурах под управлением vCenter Server Appliance версий 6.0, 6.5 и 6.7. Ниже перечислены поддерживаемые архитектуры vCSA и характерные для них особенности установки ПО vGate.

vCSA со встроенным PSC, развернутый на принадлежащем ему ESXi-сервере

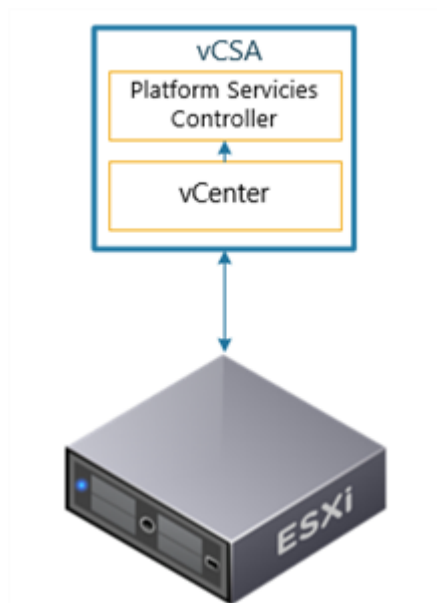


Рис.1 vCSA со встроенным PSC на принадлежащем ему ESXi-сервере

При установке ПО vGate запрашиваются учетные данные для доступа к PhotonOS.

vCSA с внешним PSC, развернутый на принадлежащем ему ESXi-сервере

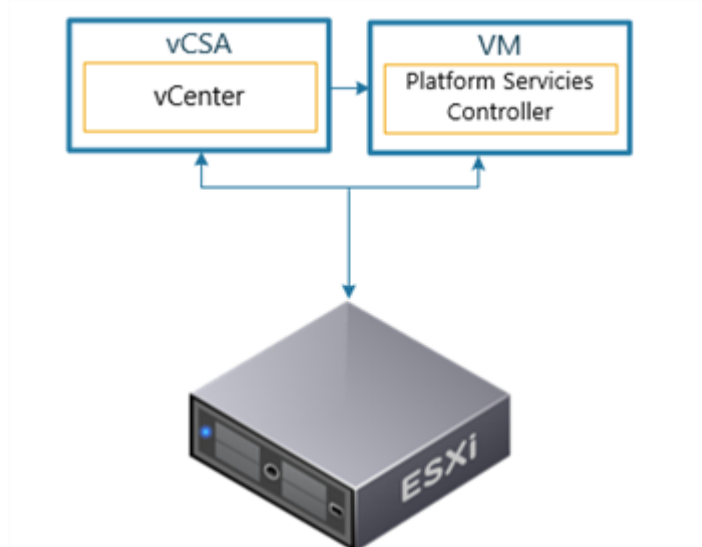
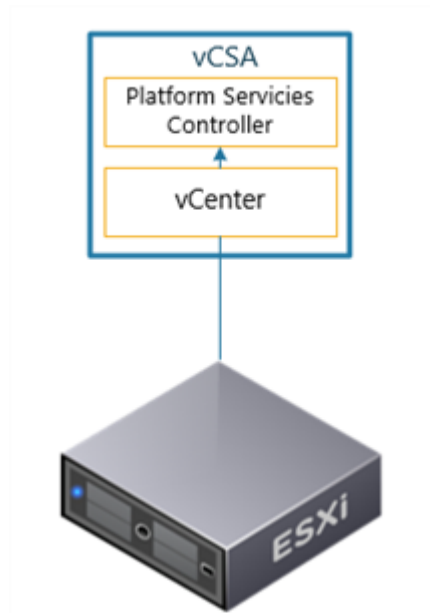
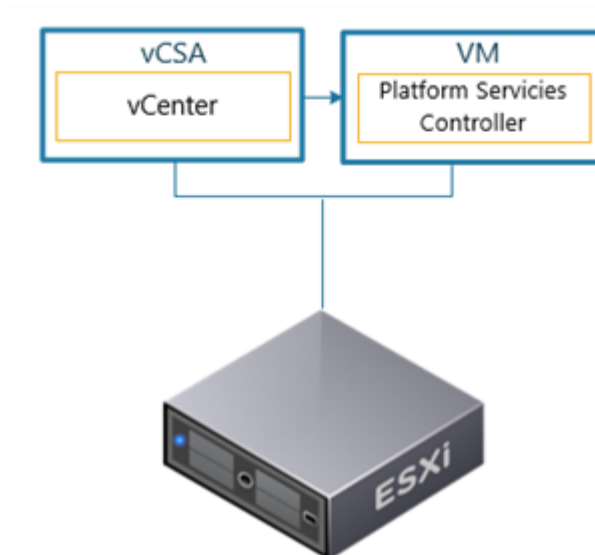


Рис.2 vCSA с внешним PSC на принадлежащем ему ESXi-сервере

При установке ПО vGate запрашиваются учетные данные для доступа к PhotonOS.

vCSA со встроенным PSC, развернутый на не принадлежащем ему ESXi-сервере**Рис.3 vCSA со встроенным PSC на не принадлежащем ему ESXi-сервере**

При установке ПО vGate запрашиваются параметры подключения к ESXi-серверу и учетные данные для доступа к PhotonOS.

vCSA с внешним PSC, развернутый на не принадлежащем ему ESXi-сервере**Рис.4 vCSA с внешним PSC на не принадлежащем ему ESXi-сервере**

При установке ПО vGate запрашиваются параметры подключения к ESXi-серверу и учетные данные для доступа к PhotonOS.

vCSA High Availability, развернутый на принадлежащем ему ESXi-сервере

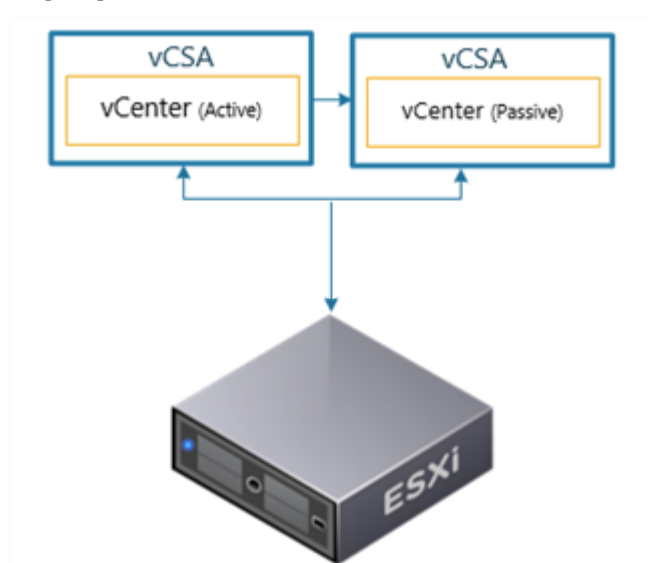


Рис.5 vCSA High Availability на принадлежащем ему ESXi-сервере

При установке ПО vGate запрашиваются учетные данные для доступа к PhotonOS. После установки vGate на пассивном узле кластера серверов vCenter сервисы vSphere остановлены.

vCSA High Availability развернут на не принадлежащем ему ESXi-сервере

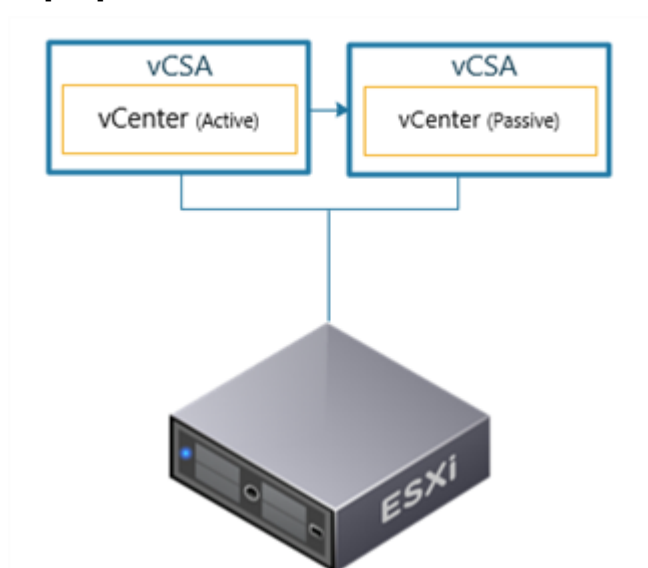


Рис.6 vCSA High Availability на не принадлежащем ему ESXi-сервере

При установке ПО vGate запрашиваются параметры подключения к ESXi-серверу и учетные данные для доступа к PhotonOS. После установки vGate на пассивном узле кластера серверов vCenter сервисы vSphere остановлены.

vCSA High Availability развернут на нескольких принадлежащих ему ESXi-серверах

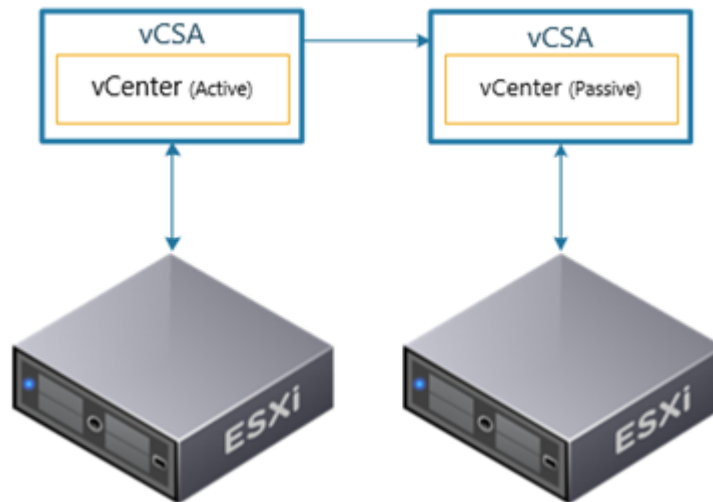


Рис.7 vCSA High Availability на нескольких принадлежащих ему ESXi-серверах

При установке ПО vGate запрашиваются учетные данные для доступа к PhotonOS. После установки vGate на пассивном узле кластера серверов vCenter сервисы vSphere остановлены.

vCSA High Availability развернут на нескольких не принадлежащих ему ESXi-серверах

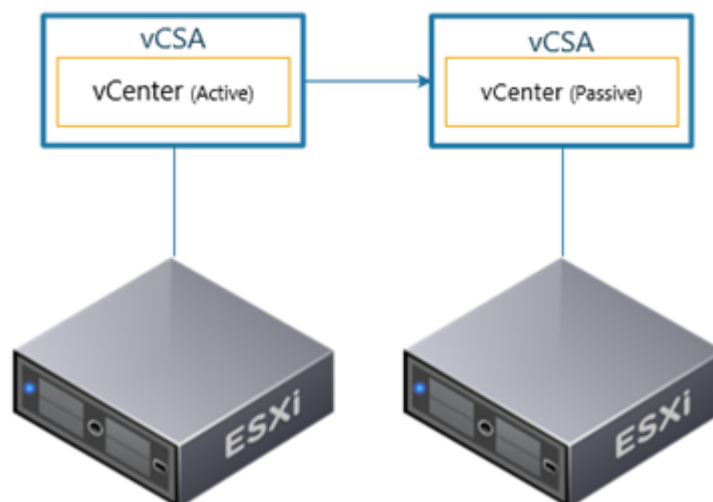


Рис.8 vCSA High Availability на нескольких не принадлежащих ему ESXi-серверах

При установке ПО vGate запрашиваются параметры подключения ко всем ESXi-серверам и учетные данные для доступа к PhotonOS. После установки vGate на пассивном узле кластера серверов vCenter сервисы vSphere остановлены.

Глава 3

Функциональные возможности vGate

ПО vGate версии 4.3 поставляется в трех редакциях: Standard, Enterprise и Enterprise Plus. vGate Enterprise и Enterprise Plus представляют собой расширенные версии vGate Standard и содержат дополнительный функционал для осуществления защиты виртуальной инфраструктуры. В сравнительной таблице приводится полный перечень функциональных возможностей ПО vGate.

Функция	vGate Standard	vGate Enterprise	vGate Enterprise Plus
Разделение прав на управление виртуальной инфраструктурой и на управление безопасностью	+	+	+
Аутентификация администраторов виртуальной инфраструктуры, администраторов информационной безопасности и компьютеров	+	+	+
Полномочное управление доступом к конфиденциальным ресурсам	+	+	+
Политики безопасности средств управления виртуальной инфраструктурой и объектов защищаемого периметра	+	+	+
Контроль целостности конфигурации VM, доверенная загрузка	+	+	+
Регистрация событий, связанных с информационной безопасностью	+	+	+
Централизованное управление и аудит событий безопасности	+	+	+
Отправка уведомлений о событиях аудита по протоколам SMTP и Syslog	+	+	+
Автоматизация развертывания агентов vGate	+	+	+
Резервное копирование конфигурации и журнала событий vGate	+	+	+
Управление несколькими серверами авторизации vGate одновременно	-	+	+
Синхронизация настроек серверов авторизации	-	+	+
Горячее резервирование сервера авторизации vGate для повышения отказоустойчивости	-	+	+
Поддержка vCenter Linked Mode	-	+	+
Поддержка VMware Auto Deploy	-	+	+
Поддержка vCenter High Availability	-	+	+
Подготовка отчетов о состоянии и событиях ИБ	-	-	+
Мониторинг виртуальной инфраструктуры	-	-	+
Сегментирование сети	-	-	+

Разделение административных функций

В vGate реализован принцип разделения ролей — разделение прав на управление виртуальной инфраструктурой и управление информационной безопасностью.

При установке сервера авторизации vGate (см. документ [2]) создается учетная запись главного администратора информационной безопасности.



Внимание! Роль главного АИБ только одна и не может быть передана другому АИБ. Учетная запись главного АИБ имеет ряд привилегий по сравнению с другими АИБ. Только эта учетная запись обладает правами добавлять ПРД для внешнего адаптера основного или резервного сервера авторизации, а также редактировать учетную запись главного АИБ. Однако из соображений безопасности главный АИБ не имеет доступа к виртуальной инфраструктуре.

Изначально главный АИБ распределяет права между пользователями vGate, используя для этого две основные роли — администратор виртуальной инфраструктуры (АВИ) и администратор информационной безопасности (АИБ).

Данные роли обладают следующими полномочиями.

Роль	Полномочия
АИБ	<ul style="list-style-type: none"> • Дискреционное разграничение доступа к средствам управления виртуальной инфраструктурой. • Настройка полномочного управления доступом к конфиденциальным ресурсам. • Управление политиками безопасности средств управления виртуальной инфраструктурой и объектов защищаемого периметра. • Аудит событий безопасности. • Настройка vGate. • Управление учетными записями пользователей (создание, удаление, редактирование), кроме учетной записи главного АИБ. • Настройка и управление резервным сервером (при его наличии). • Просмотр настроек элементов управления виртуальной инфраструктурой с помощью средств управления VMware vSphere. • Настройка правил фильтрации сетевого трафика
АВИ	<ul style="list-style-type: none"> • Управление виртуальной инфраструктурой с помощью средств управления VMware vSphere. • Выбор уровня конфиденциальности сессии при работе с конфиденциальными ресурсами (для использования данной возможности необходима настройка vGate, по умолчанию функция отключена). • Настройка учетной записи АИБ для просмотра настроек элементов управления виртуальной инфраструктурой с помощью средств управления VMware vSphere



Примечание. В отношении указанных выше ролей в vGate принята следующая терминология:

- "Администратор" — пользователь, выполняющий функции администратора информационной безопасности.
- "Пользователи" — администраторы виртуальной инфраструктуры.

Полномочное управление доступом к конфиденциальным ресурсам

В vGate реализовано полномочное управление доступом к конфиденциальным ресурсам.

При выполнении ряда стандартных операций с объектами виртуальной инфраструктуры осуществляется сравнение меток безопасности учетных записей АВИ и ресурсов.

Метки безопасности назначаются следующим ресурсам:

- защищаемый ESXi-сервер;
- хранилище VM;

- виртуальная машина;
- физический сетевой адаптер;
- виртуальная локальная сеть;
- группа объектов.

Виды меток безопасности

В vGate могут использоваться следующие виды меток безопасности.

Метка	Описание
Иерархическая метка	Содержит только один уровень конфиденциальности
Неиерархическая метка	Содержит одну или несколько равноправных категорий конфиденциальности
Составная метка	Содержит одновременно один уровень конфиденциальности и одну или несколько категорий конфиденциальности

Уровень конфиденциальности характеризует уровень доступа применительно к ресурсу или уровень допуска к ресурсу применительно к пользователю.

В системе могут использоваться следующие уровни конфиденциальности (указаны в порядке возрастания):

- неконфиденциально;
- для служебного пользования.

Категория конфиденциальности определяет принадлежность ресурса или доступ пользователя к некой группе (например, к подразделению компании). Метка безопасности может одновременно содержать несколько категорий конфиденциальности. Наличие такой метки у ресурса говорит о совместном использовании ресурса несколькими различными группами одновременно (например, VM может одновременно использоваться бухгалтерией и отделом кадров); у пользователя — о наличии допуска к ресурсам нескольких таких групп (например, пользователь может одновременно управлять VM бухгалтерии и отдела кадров).

По умолчанию в системе настроен список из пяти категорий конфиденциальности, обозначенных цветом ("Синий", "Зеленый", "Желтый" и т. д.). АИБ может изменить список доступных категорий по своему усмотрению.

Управление уровнем конфиденциальности

При настроенном полномочном управлении доступом на базе иерархических или составных меток пользователь может выполнять операции с ресурсами, уровень конфиденциальности которых меньше или равен его собственному уровню конфиденциальности.

При включенном контроле уровня сессий (эта функция контролируется АИБ и по умолчанию отключена) пользователь может управлять собственным уровнем конфиденциальности. Для этого пользователь может выбрать уровень сессии, равный или ниже собственного уровня конфиденциальности. В этом случае пользователь получает доступ к ресурсам, уровень конфиденциальности которых равен выбранному уровню сессии.

Операции, регламентируемые функцией управления доступом

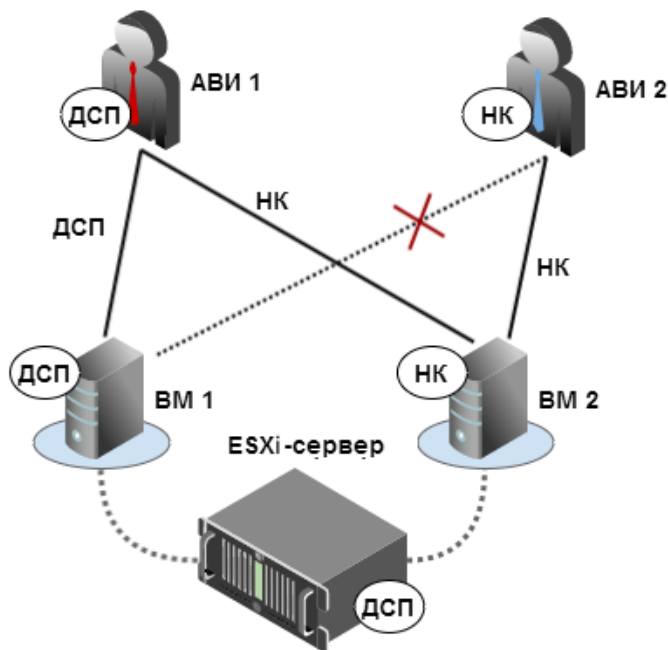
Полномочное управление доступом используется для управления правами на выполнение таких операций, как запуск VM, редактирование параметров VM, редактирование сетевых параметров и т. д. В приложении к документу [2] представлен полный перечень операций с конфиденциальными ресурсами, выполнение которых регламентируется полномочным управлением доступом, а также приведены условия их выполнения.

Следует отметить, что доступ АВИ к ESXi-серверу определяется правилами разграничения доступа (ПРД).

Рассмотрим на конкретных примерах порядок предоставления доступа для запуска VM.

Пример 1. Управление запуском VM при использовании уровней конфиденциальности

На ESXi-сервере с уровнем конфиденциальности "для служебного пользования", для которого задан дополнительный параметр "Разрешено исполнять VM с меньшим уровнем", исполняются VM 1 с уровнем конфиденциальности "для служебного пользования" и VM 2 с уровнем конфиденциальности "неконфиденциально". Рассмотрим, какие VM смогут запустить АВИ 1 с уровнем конфиденциальности "для служебного пользования" и АВИ 2 с уровнем конфиденциальности "неконфиденциально".



Условные обозначения

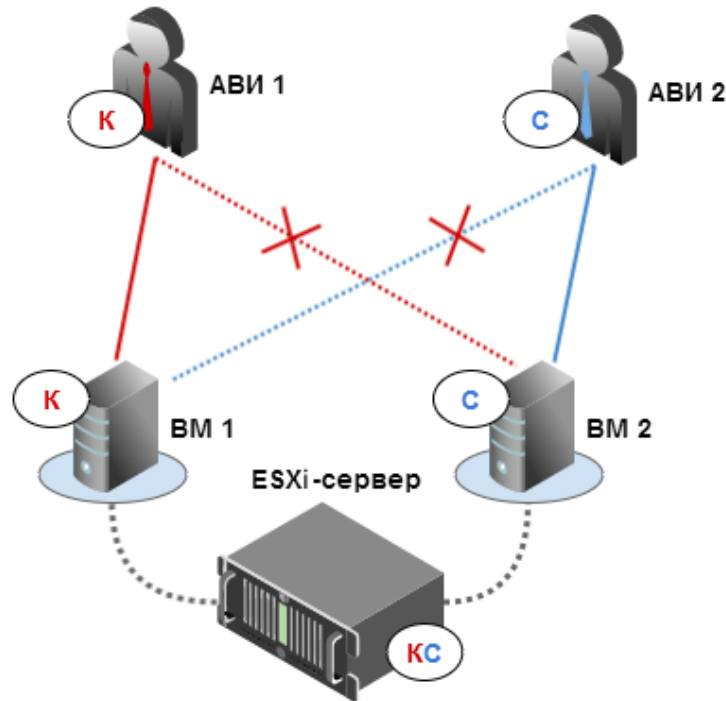
Уровни конфиденциальности		Уровни сессии	
	Неконфиденциально	<u>НК</u>	Неконфиденциально
	Для служебного пользования	<u>ДСП</u>	Для служебного пользования

При включенном контроле уровня сессий АВИ 1 может запускать обе VM (VM 1 и VM 2), выбрав уровень конфиденциальности сессии, соответствующий уровню конфиденциальности VM. АВИ 2 сможет запустить только VM 2; запуск VM 1 для него запрещен.




Пример 2. Управление запуском ВМ при использовании категорий конфиденциальности

Примечание. Контроль доступа по категориям конфиденциальности по умолчанию отключен. Данная функция может быть настроена и включена АИБ с помощью консоли управления vGate.

На ESXi-сервере, являющемся общим для категорий "Красный" и "Синий", исполняются ВМ 1 с категорией "Красный" и ВМ 2 с категорией "Синий".



Условные обозначения

-  Метка с категориями "Красный" и "Синий"
-  Метка с категорией "Красный"
-  Метка с категорией "Синий"

АВИ 1 может запускать только ВМ 1; АВИ 2 — только ВМ 2.

Порядок назначения меток безопасности

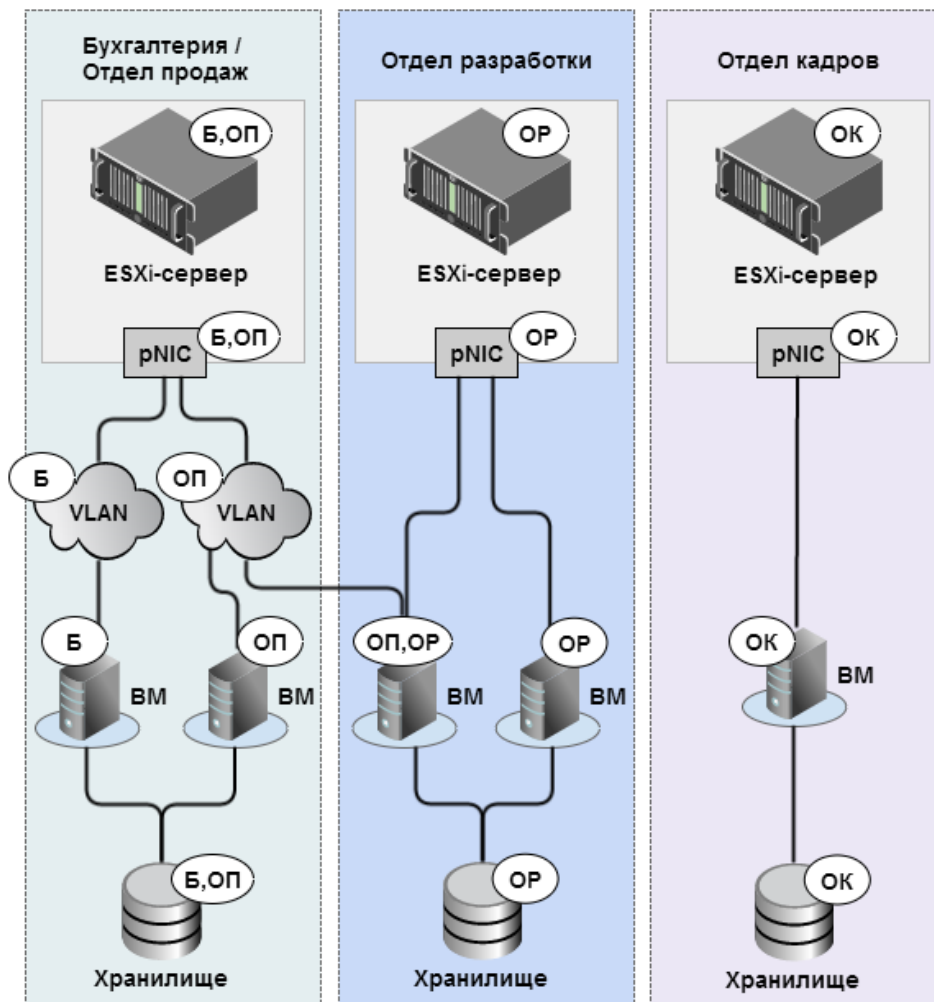
Метки безопасности назначает АИБ с помощью консоли управления в процессе настройки СЗИ (см. раздел "Настройка полномочного управления доступом к конфиденциальным ресурсам" в документе [2]).

Вновь создаваемым виртуальным машинам метки безопасности присваиваются автоматически (см. раздел "Перечень основных операций с конфиденциальными ресурсами и условия их выполнения" в приложении к документу [2]).

Варианты применения функции управления доступом

1. Разграничение доступа АВИ к ресурсам разных отделов

Для разграничения доступа к ресурсам разных отделов применяются неиерархические метки. На рисунке показан пример настройки неиерархических меток для такого случая.



Условные обозначения

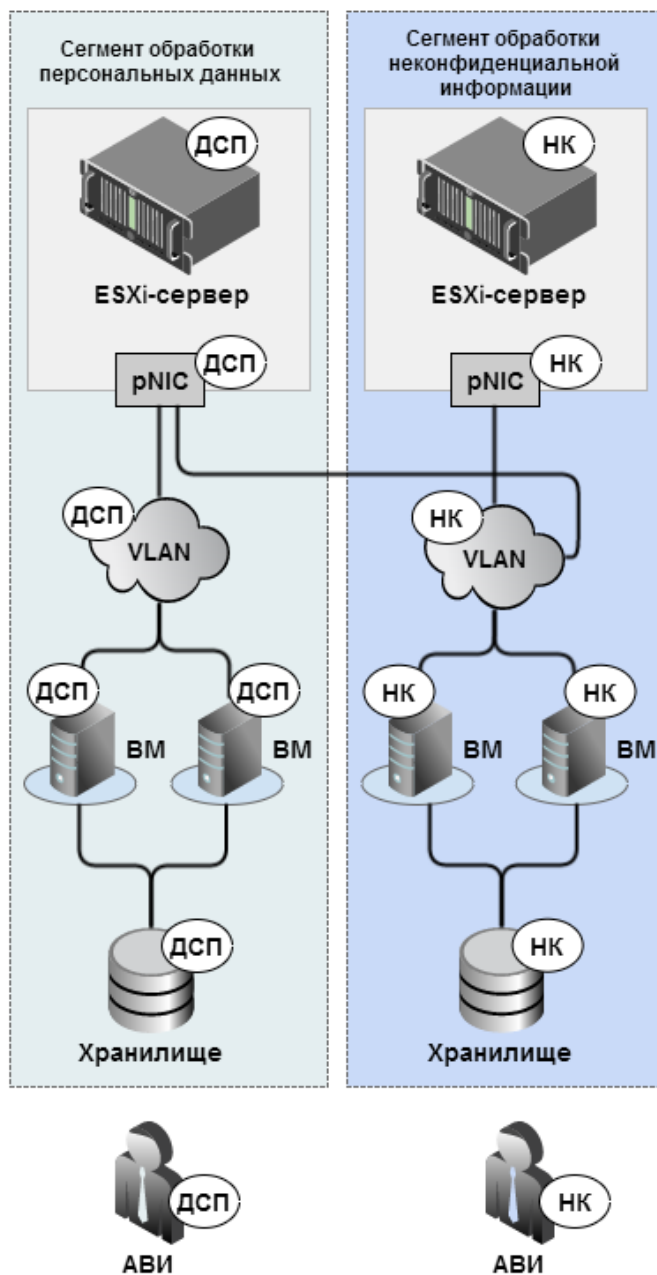
Б	Бухгалтерия	ОК	Отдел кадров
ОП	Отдел продаж	ОП	Отдел разработки

В примере отдел кадров и отдел разработки имеют по собственному ESXi-серверу, а бухгалтерия и отдел продаж имеют общий ESXi-сервер.

Пояснение. В примере стандартные категории конфиденциальности переопределены под задачи пользователя.

2. Разграничение доступа АВИ к неконфиденциальным сведениям и персональным данным

Для разграничения доступа АВИ к персональным данным и неконфиденциальным сведениям используют иерархические метки. На рисунке показан пример настройки иерархических меток для такого случая.



Условные обозначения

- ДСП** Для служебного пользования
- НК** Неконфиденциально

3. Разграничение доступа АВИ к неконфиденциальным сведениям и персональным данным, обрабатываемым в разных отделах

Иногда необходимо разграничить доступ не только к ресурсам разных отделов, но и к информации разного уровня внутри одного отдела.

В этом случае применяют составные метки.

Политики безопасности

Политики безопасности, реализованные в vGate, контролируют критичные для безопасности виртуальной среды настройки ESXi-серверов и ВМ.

Для простоты использования политики безопасности объединены в типовые наборы политик (или шаблоны). С помощью таких шаблонов можно быстро настроить защиту виртуальной среды в соответствии с требованиями отраслевых стандартов (например, таких как PCI DSS и СТО БР ИББС), законом о персональных данных, требованиями ФСТЭК России для конкретного класса АС и рекомендациями производителя (такими как VMware vSphere 6.7 Security Hardening Guide и CIS Security Configuration Benchmark for VMware vSphere (ESXi 6.5)).

В зависимости от специфики предприятия шаблоны могут использоваться в любом сочетании. Кроме того, АИБ по своему усмотрению может применять политики в шаблоне выборочно, т. е. включить необходимые политики и отключить неиспользуемые.

Назначение сформированного на основе шаблонов набора политик осуществляется напрямую на объекты или группы объектов.

Следует отметить, что из набора политик, назначенных объекту, для него действуют только политики, предназначенные для этого объекта: для ESXi-сервера — политики ESXi-сервера, для ВМ — политики ВМ.

Каждая из политик в наборе может находиться в одном из следующих состояний:

- включена (политика действует);
- отключена (политика не действует).

При назначении объекту нескольких наборов политик действует следующее правило: политика считается включенной, если она включена хотя бы в одном из наборов политик.

Контроль целостности и доверенная загрузка

Для обеспечения контроля целостности программной среды и доверенной загрузки ОС виртуальных машин в vGate на каждый ESXi-сервер устанавливаются компоненты, выполняющие следующие защитные функции:

- Контроль целостности настроек ВМ перед ее загрузкой.
- Контроль целостности снимков точек ВМ.
- Контроль целостности образа BIOS виртуальной машины.
- Доверенная загрузка ОС — осуществляется путем контроля целостности загрузочного сектора виртуального диска.
- Контроль целостности шаблона виртуальной машины.
- Контроль целостности образа BIOS шаблона виртуальной машины.
- Контроль целостности образов виртуальных дисков шаблонов виртуальных машин.

Совет. Для обеспечения полноценной защиты виртуальных машин от НСД рекомендуется дополнительно развернуть на каждой из них СЗИ Secret Net Studio.

Регистрация событий информационной безопасности

В vGate события безопасности регистрируются для всех защищаемых компьютеров, в том числе и компьютеров, относящихся к средствам управления виртуальной инфраструктурой.

События хранятся на сервере авторизации централизованно, в журнале событий безопасности. Регистрируемые события описываются рядом характеристик (см. раздел "Характеристики событий" в документе [2]).

vGate располагает средствами отбора и просмотра событий из журнала безопасности.

Централизованное управление и аудит

Для централизованного управления и аудита используются консоль управления и веб-консоль vGate.

С помощью консоли управления АИБ может выполнять следующие функции:

- Предоставление прав доступа к защищаемым объектам.
- Настройка полномочного управления доступом.
- Настройка политик безопасности.
- Настройка и просмотр журналов регистрации событий.
- Обновление контрольных сумм конфигурации VM.
- Управление учетными записями пользователей и компьютеров (кроме учетной записи главного АИБ).

Из соображений безопасности главный АИБ не может скачивать файлы виртуальных машин и создавать назначенные задания.

В веб-консоли vGate доступны следующие функции:

- Мониторинг событий в виртуальной инфраструктуре.
- Управление настройками сегментирования сети.
- Настройка и просмотр журналов регистрации событий и отчетов.

Все настройки хранятся централизованно на сервере авторизации vGate.

Подготовка отчетов

Данная функция доступна только в vGate Enterprise Plus.

В vGate реализована возможность построения отчетов, которые позволяют в любой момент получить актуальную информацию о текущей лицензии, состоянии настроек безопасности, соответствии объектов виртуальной инфраструктуры и политик безопасности, а также об изменениях конфигурации и произошедших событиях информационной безопасности за определенный промежуток времени.

vGate позволяет подобрать оптимальный для каждой компании вариант оформления отчетов (выбрать цветовое оформление отчета, добавить название и логотип компании на бланк отчета).

Подготовленный отчет можно выгрузить в следующие форматы:

- файл Adobe Acrobat (PDF);
- файл Excel (XLS).

Автоматизация развертывания

vGate содержит встроенный компонент для автоматизации развертывания агентов vGate на всех защищаемых ESXi-серверах, зарегистрированных в vCenter.

Компонент "Служба развертывания vGate" устанавливается автоматически при установке компонента защиты vCenter.



Внимание! vGate Standard позволяет осуществлять защиту только одного сервера vCenter. Если в компании эксплуатируются несколько серверов vCenter, объединенных с помощью режима VMware vCenter Linked Mode, необходимо установить компонент защиты vGate на каждый из них. Эта функция доступна только в vGate Enterprise (см. раздел "Функциональные возможности" в документе [1]).

Управление несколькими серверами авторизации

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

Реализована возможность подключения агента аутентификации к нескольким серверам авторизации vGate. Управление каждым сервером авторизации осуществляется с помощью отдельной консоли управления. Консоль управления, установленная на сервере авторизации, может подключаться только к этому серверу авторизации.

Примечание. Серверы авторизации должны принадлежать одному домену либо доверенным доменам.

Синхронизация настроек серверов авторизации

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

vGate поддерживает одновременную работу агента аутентификации с несколькими серверами авторизации. Администратор vGate может включить синхронизацию меток безопасности, учетных записей пользователей, политик безопасности и групп объектов между этими серверами авторизации. При недоступности одного из серверов авторизации АИБ может выполнить подключение к любому другому серверу авторизации из леса.

Резервирование сервера авторизации

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

Для обеспечения отказоустойчивости серверов авторизации vGate применяется горячее резервирование. В случае выхода из строя основного сервера авторизации (отказ оборудования, системы или служб vGate) резервный сервер автоматически принимает все управление на себя. Получив управление, резервный сервер начинает выполнять все функции по управлению vGate и авторизации администраторов виртуальной инфраструктуры.

Таким образом, работа системы не блокируется надолго. Поскольку на резервном сервере хранится актуальная информация о конфигурации системы, учетных записях и т. д., замена сервера авторизации станет практически незаметной для АВИ, работающих в защищенной виртуальной среде.

После восстановления или замены основного сервера авторизации можно вернуть управление системой этому серверу или оставить эти функции за бывшим резервным сервером.

Примечание. Функцию автоматического переключения на резервный сервер авторизации необходимо включить в консоли управления vGate R2 (см. документ [2]). По умолчанию данная функция отключена.

Поддержка VMware Auto Deploy

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

VMware vSphere включает в себя функцию "Auto Deploy", предназначенную для автоматического развертывания ESXi-сервера. В состав ПО vGate входит утилита VibModifcator.exe, которая позволяет создать архив файлов установки компонентов защиты vGate, чтобы затем добавить его в образ ESXi-сервера, используемый VMware Auto Deploy.

Мониторинг безопасности

Данная функция доступна только в vGate Enterprise Plus.

С помощью веб-интерфейса мониторинга vGate осуществляется сбор и анализ данных о событиях на объектах виртуальной инфраструктуры: сервере авторизации vGate, защищаемых серверах, компьютерах внешнего периметра сети администрирования, на которых установлен агент аутентификации vGate.

Реализована возможность создания и гибкой настройки правил корреляции. Правила позволяют отслеживать конкретные события, происходящие при заданных условиях в виртуальной инфраструктуре.

Данные о срабатывании правил корреляции и о событиях аудита в графическом виде отображаются на панели мониторинга в веб-консоли vGate.

Сегментирование сети

Данная функция доступна только в vGate Enterprise Plus.

Сегментирование сети позволяет осуществлять фильтрацию сетевого трафика в сети виртуальных машин, в том числе и расположенных на разных серверах виртуализации.

Фильтрация сетевого трафика осуществляется по правилам, настроенным в веб-консоли vGate. Правила фильтрации могут создаваться для конкретной виртуальной машины или для нескольких виртуальных машин, объединенных в сегменты.

Глава 4

Совместимость vGate с другими продуктами

Поддержка работы с VMware View

vGate поддерживает работу с VMware View версии 5.1, VMware Horizon View версий 6.1, 6.2, 7.0, 7.1, 7.6, 7.8 и 7.10. Для обеспечения доступа View Connection Server внутрь защищаемого периметра или доступа АБИ к View Connection Server требуется выполнить предварительную настройку (см. раздел "Настройка работы View Connection Server" в документе [2]).

Поддержка работы со стандартным Distributed vSwitch и Distributed vSwitch Cisco Nexus 1000v

vGate поддерживает работу со стандартным распределенным виртуальным сетевым коммутатором Distributed vSwitch (DVS), а также с коммутатором Distributed vSwitch Cisco Nexus 1000v от компании VMware. Сетевой коммутатор должен быть установлен до ПО vGate.

Решения для защиты виртуальных машин

vGate обеспечивает защиту среды администрирования виртуальной инфраструктуры и контроль целостности файлов виртуальных машин, выполняемых на защищаемых ESXi-серверах. Для обеспечения дополнительной защиты виртуальных машин рекомендуется использовать вспомогательные средства защиты информации (например, СЗИ Secret Net Studio). vGate совместим с СЗИ Secret Net Studio версий 8.4, 8.5.

Документация

1.	Средство защиты информации vGate R2. Руководство администратора. Принципы функционирования	RU.88338853.501410.012 91 1-1
2.	Средство защиты информации vGate R2. Руководство администратора. Установка, настройка и эксплуатация	RU.88338853.501410.012 91 2-1
3.	Средство защиты информации vGate R2. Руководство администратора. Быстрый старт	RU.88338853.501410.012 91 3-1
4.	Средство защиты информации vGate R2. Руководство пользователя. Работа в защищенной среде	RU.88338853.501410.012 92 1