КОД БЕЗОПАСНОСТИ

Средство защиты информации

vGate R2

Руководство администратора

Принципы функционирования (Hyper-V)

RU.88338853.501410.012 91 1-2

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

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
FCM	Failover Cluster Manager — средство управления конфигурацией кластера серверов Hyper-V
SCVMM	System Center Virtual Machine Manager — средство централизованного управления серверами Hyper-V
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 http://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 for Hyper-V версии 4.2.

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" (http://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 http://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 Microsoft Hyper-V.

Принципы и средства защиты

Защита средств управления виртуальной инфраструктурой

К средствам управления виртуальной инфраструктурой относятся:

- Серверы Hyper-V, предназначенные для запуска виртуальных машин.
- Сервер System Center Virtual Machine Manager (SCVMM), предназначенный для централизованного управления виртуальной инфраструктурой.
- Failover Cluster Manager (FCM) — средство, предназначенное для управления конфигурацией кластера серверов Hyper-V.

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 ВМ 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
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

Функция	Описание
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

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 и контрольных точек 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 xml-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 экспорта виртуальных машин	Функция позволяет ограничить несанкционированное перемещение (экспорт) виртуальных машин, обрабатывающих данные ограниченного доступа. Реализована в рамках политик безопасности
Запрет создания и удаления контрольных точек (checkpoints) виртуальных машин	Функция применяется для противодействия нарушению целостности работы систем, обрабатывающих данные ограниченного доступа. Реализована в рамках политик безопасности
Затирание остаточных данных на СХД при удалении ВМ	Функция гарантирует отсутствие остаточной информации об обрабатываемых данных на жестких дисках после удаления ВМ. Затирание остаточных данных может выполняться посредством однократной записи нулевых значений. Реализована в рамках политик безопасности
Запрет включения репликации ВМ	Функция позволяет ограничить возможность несанкционированного копирования (репликации) виртуальных машин. Реализована в рамках политик безопасности
Запрет миграции ВМ	Функция позволяет ограничить несанкционированное перемещение (миграцию) виртуальных машин, обрабатывающих данные ограниченного доступа. Реализована в рамках политик безопасности
Ограничение скачивания файлов ВМ	С помощью данного механизма можно ограничить круг лиц, которым разрешено экспортировать файлы ВМ. 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 серверах Hyper-V. Редакции vGate различаются функциональными возможностями (см. стр.**11**).

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	• 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)
Резервный сервер авторизации	• Хранение настроек и списка пользователей. • Репликация данных. • Возможность замены основного сервера при сбое
Агент аутентификации	• 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 сервера Hyper-V и SCVMM	• Контроль целостности и доверенная загрузка ВМ. • Контроль целостности модулей и настроек vGate. • Регистрация событий безопасности. • Контроль за операциями с виртуальной инфраструктурой
Консоль управления	• Централизованное управление vGate. • Управление учетными записями пользователей и компьютеров. • Назначение прав доступа к защищаемым объектам. • Установка и настройка компонентов защиты серверов Hyper-V, кластеров серверов и SCVMM. • Настройка полномочного управления доступом. • Настройка политик безопасности защищаемых объектов. • Расчет контрольных сумм конфигурации ВМ. • Настройка и просмотр журналов регистрации событий
Веб-консоль	• Настройка правил фильтрации сетевого трафика. • Мониторинг событий безопасности. • Настройка и просмотр журналов регистрации событий и отчетов
Сервер мониторинга	Сбор и корреляция событий виртуальной инфраструктуры

Варианты размещения компонентов

Компоненты vGate могут размещаться следующим образом:

Компонент	Варианты размещения
Сервер авторизации	Выделенный компьютер (установка на ВМ допускается, но не рекомендуется)
Резервный сервер авторизации	Выделенный компьютер (установка на ВМ допускается, но не рекомендуется)
Агент аутентификации	Рабочее место АВИ, рабочее место АИБ (если рабочее место АИБ во внешнем периметре сети администрирования), серверы сервисных служб (DNS, AD и т. д.)
Модули защиты сервера Hyper-V и сервера SCVMM	Серверы Hyper-V или System Center Virtual Machine Manager (SCVMM)
Консоль управления	Сервер авторизации (если рабочее место АИБ на сервере авторизации), рабочее место АИБ
Сервер мониторинга	Виртуальная машина

Сервер авторизации устанавливается на специально выделенный для него компьютер. На этот же компьютер можно установить консоль управления. В данном случае этот компьютер может использоваться в качестве рабочего места АИБ.

Внимание! Установка сервера авторизации на ВМ допускается, но не рекомендуется по соображениям безопасности.

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.

Глава 3
Функциональные возможности vGate

ПО vGate версии 4.2 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 ВМ, доверенная загрузка	+	+	+
Регистрация событий, связанных с информационной безопасностью	+	+	+
Централизованное управление и аудит событий безопасности	+	+	+
Отправка уведомлений о событиях аудита по протоколам SNMP, 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	-	+	+
Контроль над операциями с виртуальной инфраструктурой, выполняемыми с помощью System Center Virtual Machine Manager (SCVMM)	-	+	+
Контроль над операциями с виртуальной инфраструктурой, выполняемыми с помощью Failover Cluster Manager (FCM)	-	+	+
Мониторинг виртуальной инфраструктуры	-	-	+

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	• 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 Hyper-V (в случае если настроены соответствующие правила разграничения доступа). • Настройка правил фильтрации сетевого трафика
АВИ	• Управление виртуальной инфраструктурой с помощью средств управления Hyper-V, FCM и SCVMM. • 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 Hyper-V

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 сервер Hyper-V;
- хранилище ВМ (локальный жесткий диск или сетевое хранилище);
- виртуальная машина;
- физический сетевой адаптер;
- виртуальная локальная сеть;
- виртуальный коммутатор (управление доступом осуществляется с помощью утилиты clacl.exe);
- 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, ВМ может одновременно использоваться бухгалтерией и отделом кадров); у пользователя — о наличии допуска к ресурсам нескольких таких групп (например, пользователь может одновременно управлять ВМ 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 ВМ, редактирование параметров ВМ,

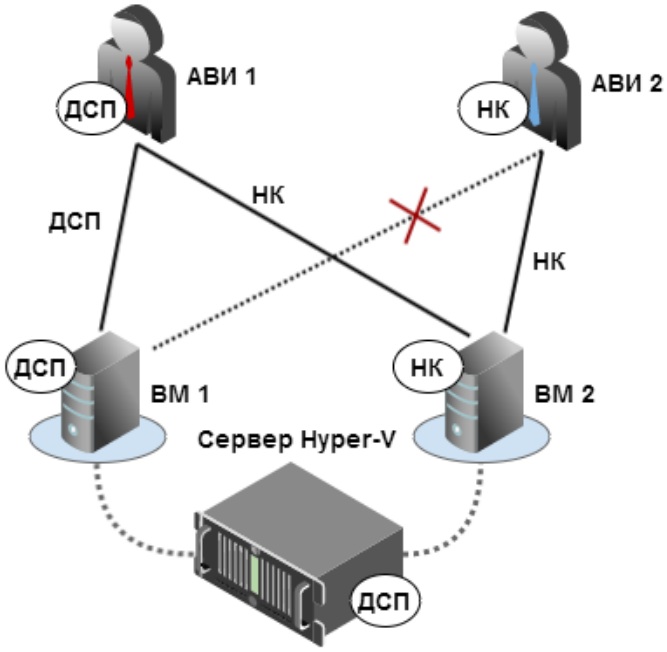
редактирование сетевых параметров и т. д. В приложении к документу [2] представлен полный перечень операций с конфиденциальными ресурсами, выполнение которых регламентируется полномочным управлением доступом, а также приведены условия их выполнения.

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

Рассмотрим на конкретных примерах порядок предоставления доступа для запуска ВМ.

Пример 1. Управление запуском ВМ при использовании уровней конфиденциальности

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



Условные обозначения

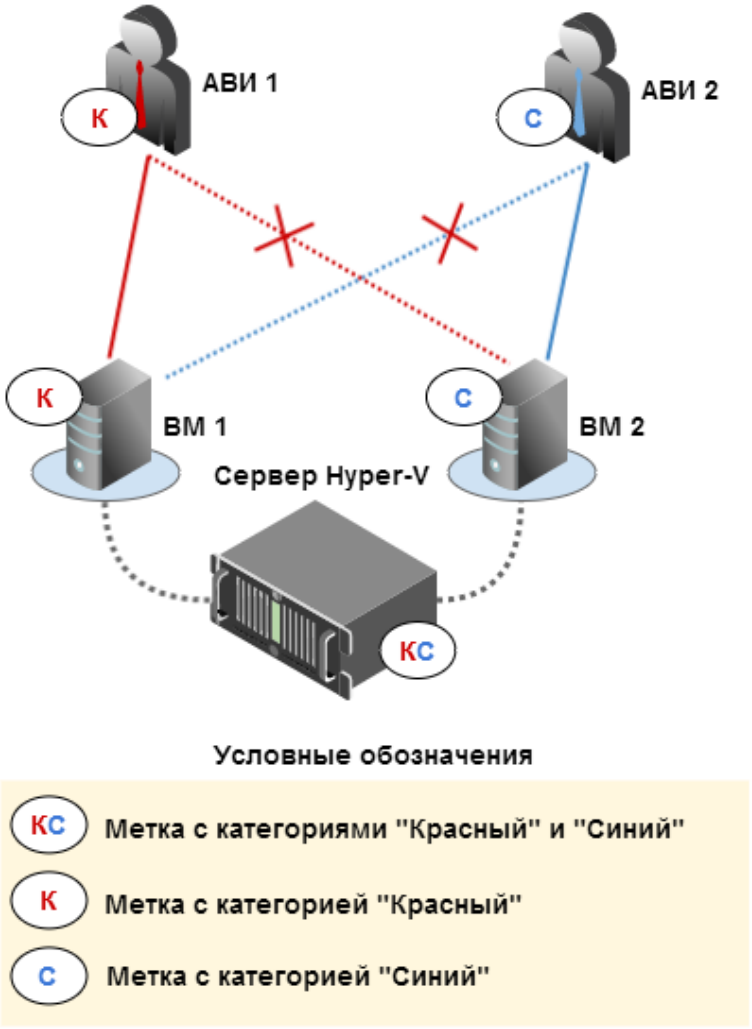
Уровни конфиденциальности		Уровни сессии	
НК	Неконфиденциально	НК	Неконфиденциально
ДСП	Для служебного пользования	ДСП	Для служебного пользования

При включенном контроле уровня сессий АВИ 1 может запускать обе ВМ (ВМ 1 и ВМ 2), выбрав уровень конфиденциальности сессии, соответствующий уровню конфиденциальности ВМ. АВИ 2 сможет запустить только ВМ 2; запуск ВМ 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 сервере Hyper-V, являющемся общим для категорий "Красный" и "Синий", исполняются ВМ 1 с категорией "Красный" и ВМ 2 с категорией "Синий".



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

Порядок назначения меток безопасности

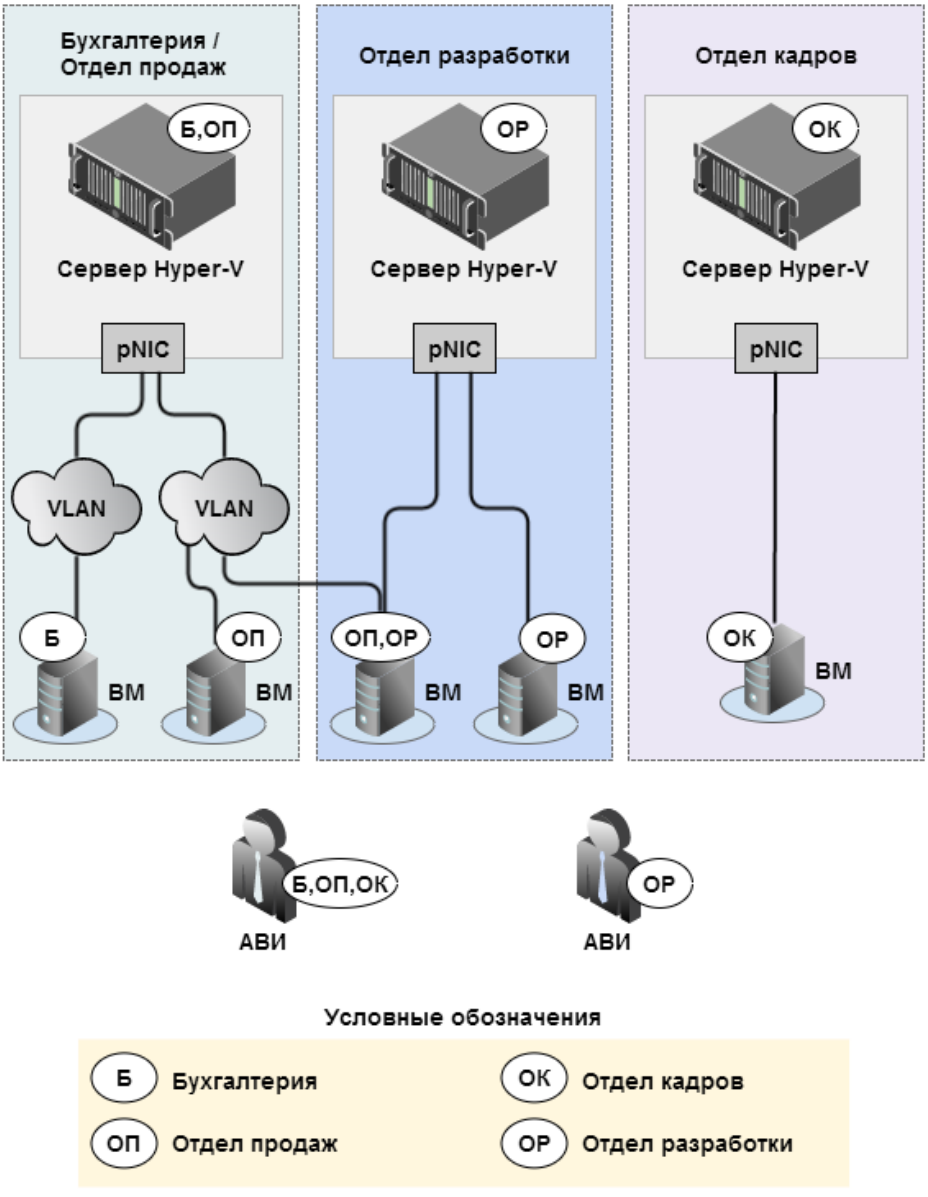
Метки безопасности назначает АИБ с помощью консоли управления в процессе настройки СЗИ (см. раздел "Настройка полномочного управления доступом к конфиденциальным ресурсам" в документе [2]).

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.

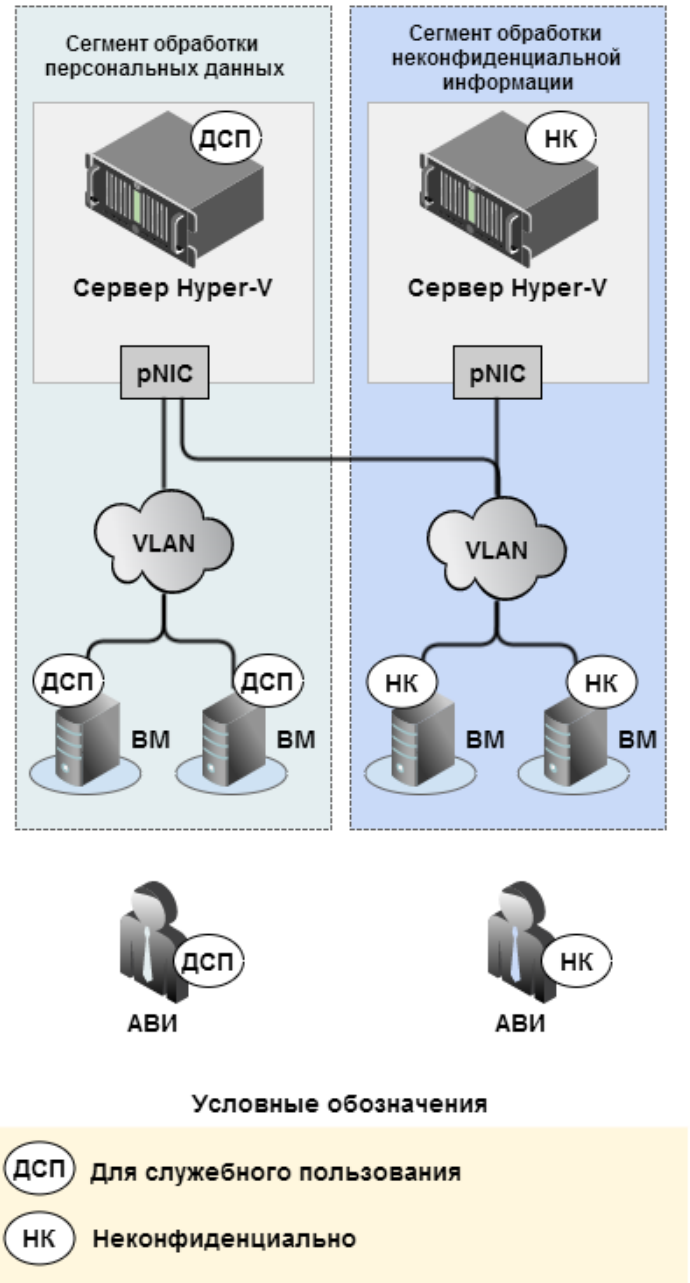


В примере отдел кадров и отдел разработки имеют по собственному серверу Hyper-V, а бухгалтерия и отдел продаж имеют общий сервер Hyper-V.

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.



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 серверов Hyper-V и ВМ.

Для простоты использования политики безопасности объединены в типовые наборы политик (или шаблоны). С помощью таких шаблонов можно быстро настроить защиту виртуальной среды.

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 сервера Hyper-V — политики сервера Hyper-V, 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 конфигурации ВМ и доверенная загрузка

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

- Контроль целостности настроек ВМ перед ее загрузкой.
- Контроль целостности контрольных точек ВМ.
- Доверенная загрузка ОС — осуществляется путем контроля целостности загрузочного сектора виртуального диска.

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 ВМ.
- Управление учетными записями пользователей и компьютеров (кроме учетной записи главного АИБ).

Из соображений безопасности главный АИБ не может скачивать файлы виртуальных машин.

В веб-консоли vGate доступны следующие функции:

- Мониторинг событий в виртуальной инфраструктуре.
- Настройка и просмотр журналов регистрации событий и отчетов.

Все настройки хранятся централизованно на сервере авторизации vGate.

Автоматизация развертывания

vGate содержит встроенный компонент для автоматизации развертывания агентов vGate на защищаемых серверах Hyper-V.

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.

Контроль доступа к объектам виртуальной инфраструктуры через SCVMM

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

System Center Virtual Machine Manager — средство централизованного управления серверами Hyper-V.

vGate позволяет контролировать действия, выполняемые с виртуальной инфраструктурой через SCVMM. Для обеспечения защиты на сервере SCVMM устанавливается агент vGate. Агент отправляет запросы на одобрение операций с ВИ на сервер авторизации vGate.

Объектами доступа в SCVMM являются:

- серверы Hyper-V;
- виртуальные машины;
- хранилища данных;
- виртуальные сети;
- виртуальные коммутаторы;
- сетевые адаптеры.

Примечание. Не поддерживается конфигурация, в которой защищаемые серверы Hyper-V и SCVMM располагаются на одном компьютере.

Контроль доступа к объектам виртуальной инфраструктуры через FCM

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

Failover Cluster Manager — средство управления конфигурацией кластера серверов Hyper-V.

vGate позволяет контролировать действия, выполняемые над кластером серверов Hyper-V через FCM. Для обеспечения защиты на серверах Hyper-V, входящих в кластер, устанавливаются агенты vGate, а точка доступа к кластеру добавляется в список защищаемых серверов виртуализации. В консоли управления vGate для точки доступа к кластеру необходимо добавить правила доступа из шаблона "Управление конфигурацией кластера серверов Hyper-V через FCM" (см. раздел "Управление доступом к защищаемым серверам" в документе [2]).

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.

Глава 4
Совместимость vGate с другими продуктами

Решения для защиты виртуальных машин

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

Документация

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