



КОД БЕЗОПАСНОСТИ

Средство защиты информации

vGate R2

Руководство пользователя

Работа в защищенной среде (Hyper-V)



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
Назначение vGate	6
Подготовка к установке vGate	7
Создание учетной записи для АИБ	7
Подготовка сети к установке vGate	7
Работа в защищенной среде ОС Windows	10
Подключение к защищенной среде	10
Аутентификация пользователя	10
Авторизация по персональному идентификатору	12
Проверка состояния подключения	13
Настройка конфигурации	13
Смена пароля	14
Доступ к элементам управления виртуальной инфраструктурой	15
Особенности работы с конфиденциальными ресурсами	16
Управление уровнем доступа	16
Выбор уровня сессии	17
Ввод в эксплуатацию нового оборудования	18
Завершение работы в защищенной среде	18
Документация	19

Список сокращений

AD	Active Directory — служба каталогов MS Windows
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
ВМ	Виртуальная машина (англ. — VM)
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 виртуальной инфраструктуры, защищаемой средствами изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся сведения, необходимые для работы в защищенной среде.

Документ предназначен для vGate for Hyper-V 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.

Назначение vGate

vGate предназначен для обеспечения безопасности виртуальной инфраструктуры, развернутой с использованием системы виртуализации Microsoft Hyper-V.

Глава 1

Подготовка к установке vGate

Создание учетной записи для АИБ

Для доступа к виртуальной инфраструктуре администратору информационной безопасности необходимо создать учетную запись в среде Microsoft Hyper-V. Эта учетная запись должна ограничить полномочия АИБ по управлению виртуальной инфраструктурой только возможностью просмотра конфигурации элементов виртуальной инфраструктуры.

Подготовка сети к установке vGate

До установки vGate необходимо:

- Подключить необходимое дополнительное оборудование (рабочее место АИБ, сервер авторизации и т. д.).
- Выполнить конфигурирование локальной сети.
- Настроить маршрутизацию между подсетями.

После этого необходимо убедиться в возможности доступа с рабочих мест АИБ к элементам управления виртуальной инфраструктурой (серверам Hyper-V, SCVMM).

Правила конфигурирования сети, требования к оборудованию, а также порядок настройки маршрутизации приведены в документе [2].

Примеры виртуальной инфраструктуры и размещения компонентов vGate представлены на следующих рисунках.

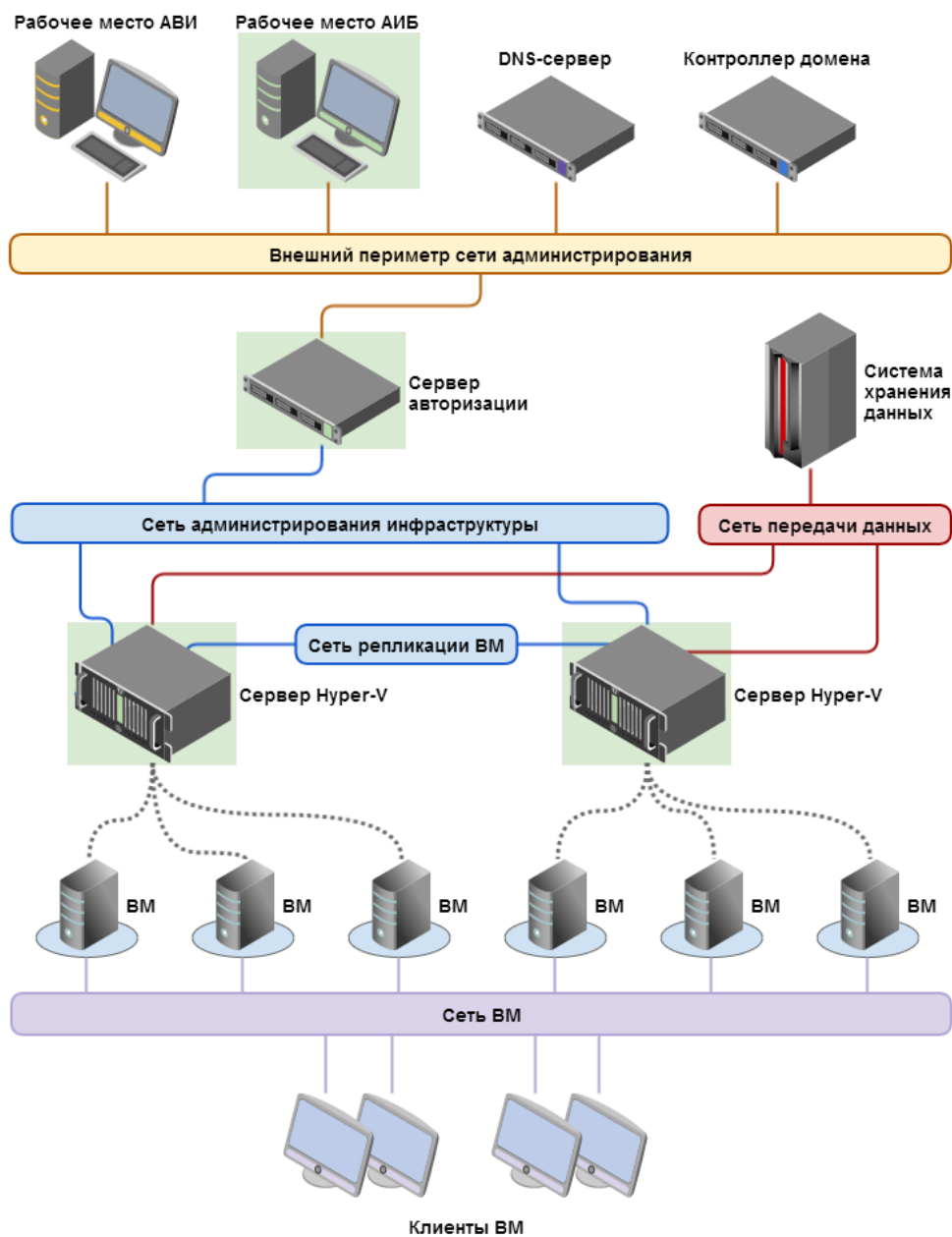


Рис.1 Архитектура сети и размещение компонентов (маршрутизацию трафика выполняет сервер авторизации vGate)

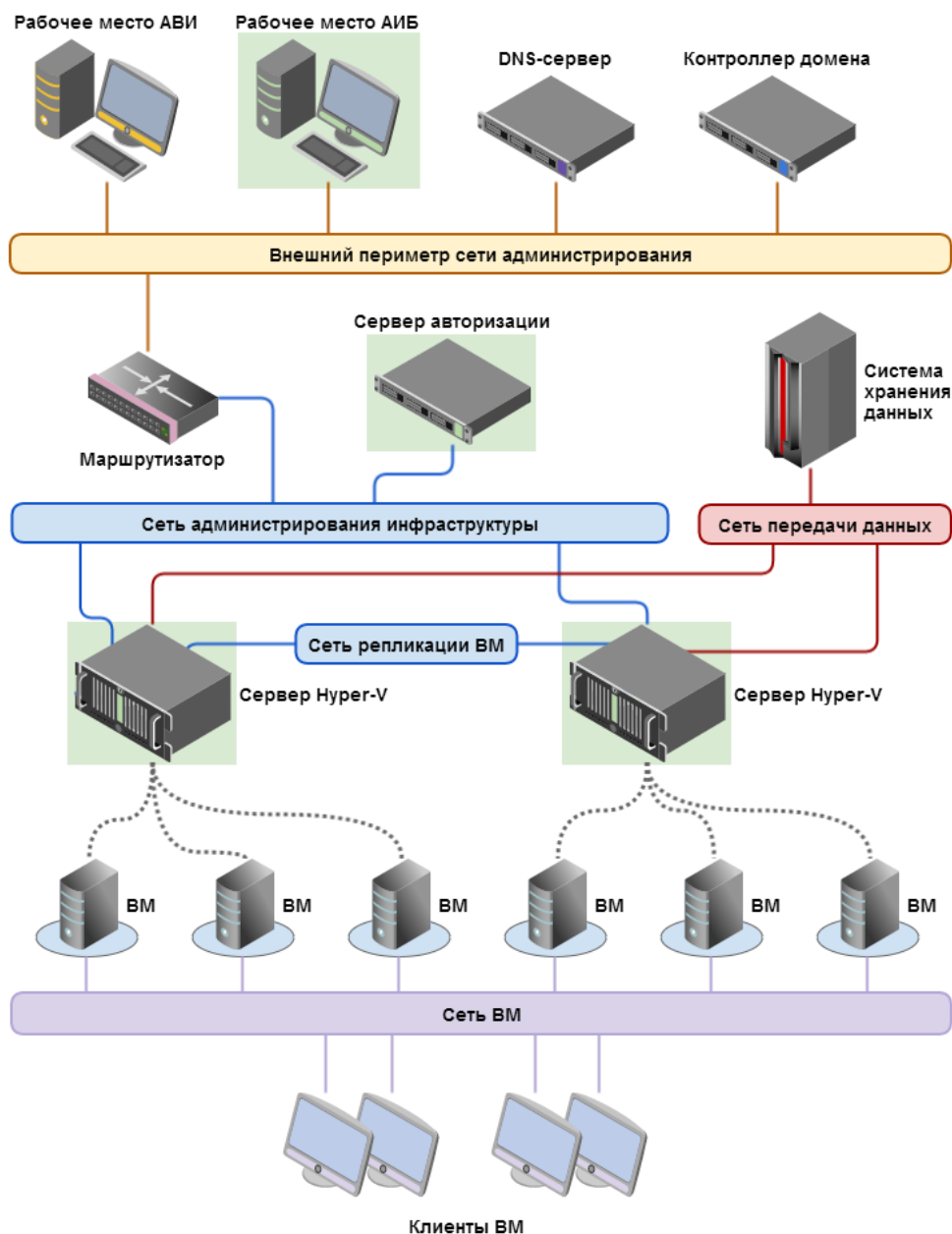


Рис.2 Архитектура сети и размещение компонентов (маршрутизация с помощью существующего маршрутизатора в сети)

Глава 2

Работа в защищенной среде ОС Windows

Подключение к защищенной среде

Доступ к управлению виртуальной инфраструктурой получают только пользователи, прошедшие аутентификацию. В vGate предусмотрена процедура аутентификации пользователей (администраторов виртуальной инфраструктуры) и компьютеров. Аутентификация компьютеров выполняется автоматически.

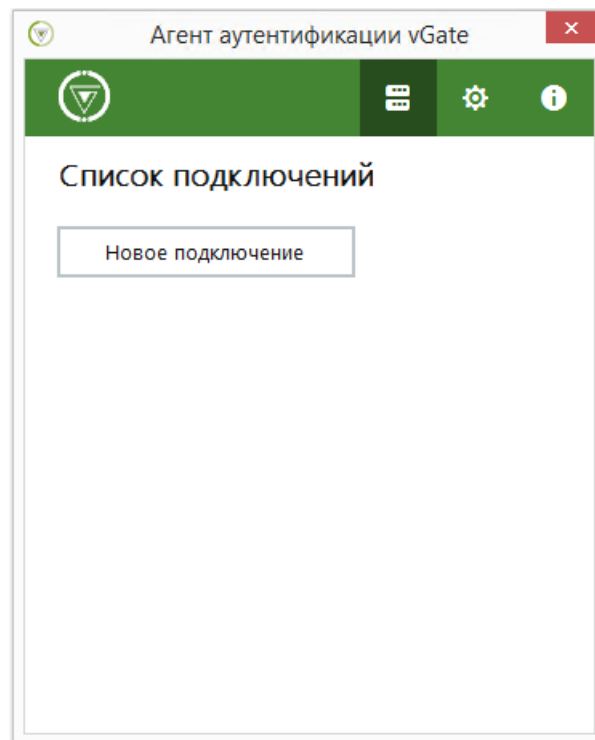
Аутентификация пользователя

Для выполнения процедуры аутентификации:

1. Выберите в меню "Пуск" команду "Приложения | Код Безопасности | vGate | Вход в систему".

В ОС Windows более ранней версии, чем Windows 8 или Windows Server 2012, следует выбрать команду "Программы | Код Безопасности | vGate | Вход в систему".

На экране появится следующий диалог.



2. Чтобы создать подключение к серверу авторизации, нажмите кнопку "Новое подключение". Если в сети используются несколько серверов авторизации, необходимо настроить подключение к защищенной среде для каждого из них.



Функция подключения к нескольким серверам авторизации доступна только в vGate Enterprise и Enterprise Plus (подробнее см. документ [1]).

Появится следующий диалог.

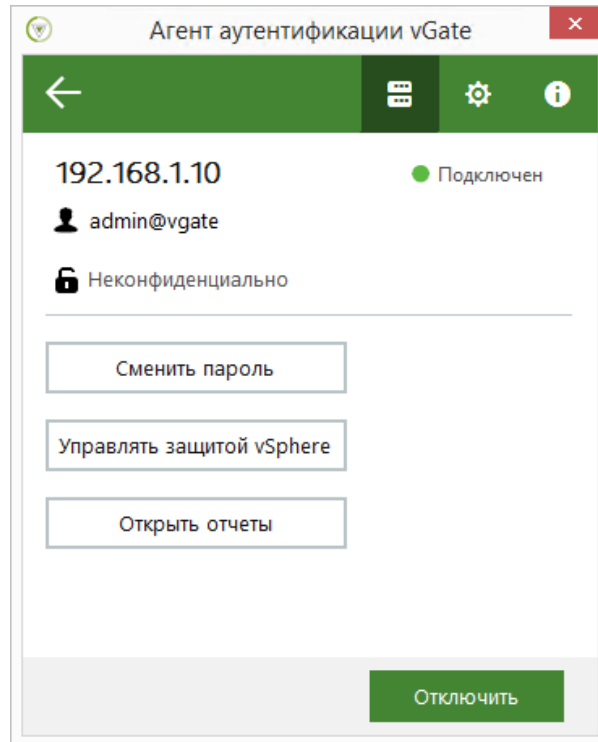
3. Введите учетные данные пользователя, при необходимости измените остальные параметры соединения и нажмите кнопку "Подключить".

Параметр	Описание
Способ аутентификации	Для подключения к защищенной среде с использованием учетной записи vGate выберите вариант "Имя пользователя и пароль" (предлагается по умолчанию). Чтобы использовать учетные данные пользователя Windows, выберите из списка вариант "Данные текущей сессии Windows"
IP-адрес или имя сервера	Сетевое имя или IP-адрес сервера авторизации vGate
Домен	Для учетной записи из Active Directory выберите из списка домен. При аутентификации пользователя vGate укажите имя реестра учетных записей vGate, указанное при установке сервера авторизации (например "VGATE")
Имя пользователя	Имя учетной записи администратора виртуальной инфраструктуры
Пароль	Пароль администратора виртуальной инфраструктуры
Подключать автоматически	Установите отметку в этом поле, чтобы последующие подключения пользователя к защищенной среде выполнялись автоматически (без запроса пароля)

Совет.

- Для изменения настроек запуска агента аутентификации vGate нажмите кнопку  в области главного меню программы аутентификации (см. стр. 13).
- Для просмотра сведений о версии агента аутентификации и сообщения об авторских правах нажмите кнопку  в области главного меню.

4. Подключение к серверу авторизации появится в списке.



Примечание.

- Нажмите кнопку "Управлять защитой Hyper-V", чтобы открыть консоль управления vGate для Hyper-V.
- Если на компьютере установлено средство просмотра отчетов (см. раздел "Подготовка отчетов" в документе [2]), нажмите кнопку "Открыть отчеты", чтобы открыть диалог для настройки параметров отчетов. Функция просмотра отчетов доступна только в vGate для vSphere.

Авторизация по персональному идентификатору

Для аутентификации пользователя возможно применение персонального идентификатора Рутoken или JaCarta.

Для получения персонального идентификатора обратитесь к администратору безопасности. Процедура настройки персонального идентификатора описана в документе [2].

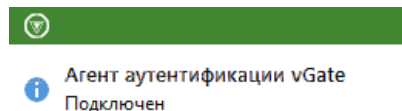
Для аутентификации с помощью персонального идентификатора:

1. Запустите агент аутентификации (см. стр. 10).
2. Подключите персональный идентификатор к компьютеру, на котором установлен агент аутентификации vGate.

3. Выберите сервер авторизации, способ аутентификации, введите ПИН-код и нажмите кнопку "Подключить".

Проверка состояния подключения


После успешной аутентификации будет выполнено подключение к виртуальной инфраструктуре. Подтверждением этого служит появление всплывающего сообщения к значку на панели задач в области уведомлений.



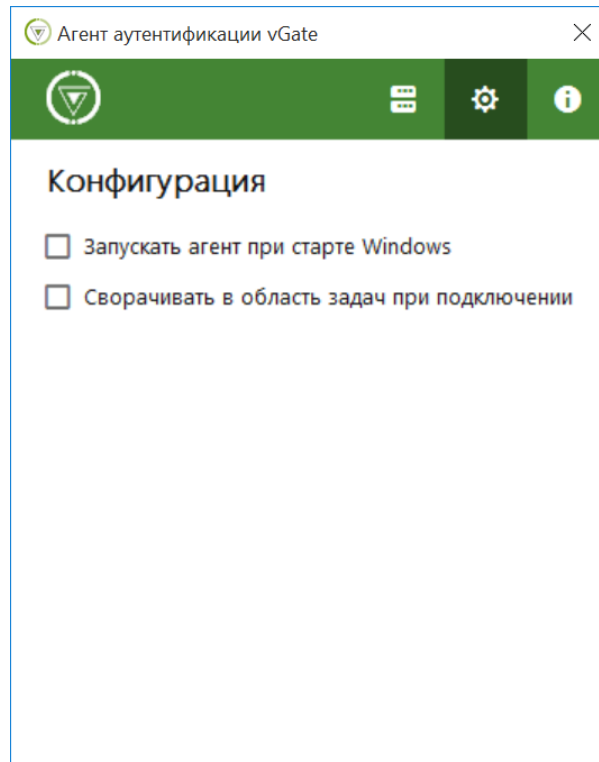
Настройка конфигурации



Для настройки конфигурации агента аутентификации:

1. Вызовите на экран диалог агента аутентификации, дважды щелкнув значок в правой части панели задач.
2. Нажмите кнопку  в области главного меню.

Появится диалог:



3. Настройте параметры работы программы.

Смена пароля



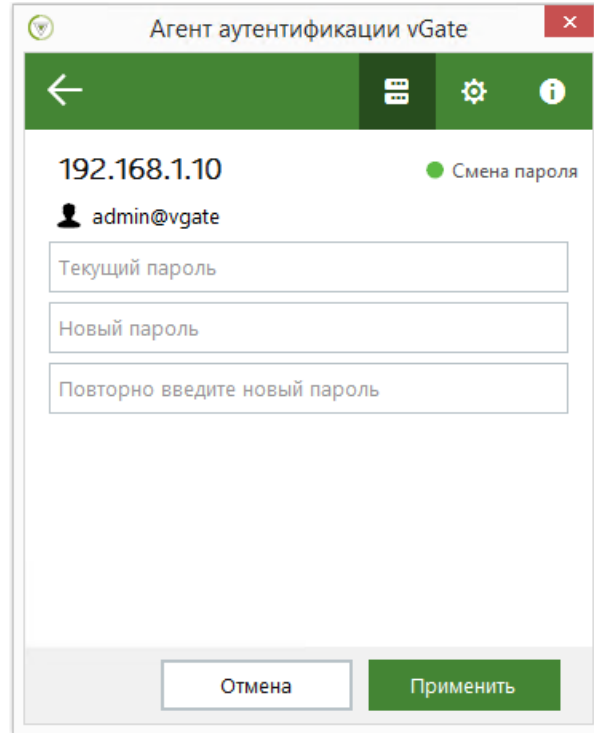
Внимание! Новый пароль должен соответствовать требованиям к паролю, заданным администратором информационной безопасности. Если новый пароль не будет соответствовать этим требованиям, появится сообщение с предложением указать другой пароль.



Для смены пароля пользователя:

1. Вызовите на экран диалог агента аутентификации, дважды щелкнув значок в правой части панели задач.

2. Выберите подключение и нажмите кнопку "Сменить пароль".
На экране появится следующий диалог.



The screenshot shows a mobile application window titled "Агент аутентификации vGate". The interface has a green header bar with a back arrow, a menu icon, a settings gear, and an information icon. Below the header, the IP address "192.168.1.10" is displayed next to a green dot and the text "Смена пароля". Underneath, the email address "admin@vgate" is shown with a person icon. There are three input fields: "Текущий пароль", "Новый пароль", and "Повторно введите новый пароль". At the bottom, there are two buttons: "Отмена" (grey) and "Применить" (green).

3. Введите старый пароль, дважды введите новый пароль и нажмите кнопку "Применить".

Примечание. Для учетных записей из Active Directory изменение пароля с помощью vGate не поддерживается. Для этого можно использовать средства администрирования Active Directory.

Доступ к элементам управления виртуальной инфраструктурой

Права на управление правилами разграничения доступа к защищаемым элементам управления виртуальной инфраструктурой закреплены за администратором безопасности. Поэтому если АВИ для выполнения своих производственных задач требуются иные права или АВИ не может получить доступ к необходимым элементам управления, ему следует обратиться к администратору безопасности для разрешения возникшей проблемы.

Особенности работы с конфиденциальными ресурсами

Каждому пользователю назначается уровень конфиденциальности, позволяющий ему выполнять операции с ресурсами (серверами Hyper-V) определенного уровня конфиденциальности. При этом пользователь может выполнять операции с ресурсами, уровень конфиденциальности которых не выше его собственного уровня конфиденциальности.

На основании этого правила осуществляется управление доступом к выполнению таких операций, как запуск и остановка ВМ, редактирование параметров ВМ (в том числе и сетевых), перемещение ВМ и т. д.

Управление уровнем доступа

Каждый сеанс работы пользователя при подключении к защищенной среде получает уровень сессии, равный уровню конфиденциальности, который назначен пользователю. При этом пользователь может выполнять операции с ресурсами того же или меньшего уровня конфиденциальности.

Пользователям может быть предоставлена возможность контроля уровня сессии. В этом случае при подключении к защищенной среде уровень сессии также равен уровню конфиденциальности пользователя, но пользователь может выполнять операции только с ресурсами такого же уровня. Для доступа к ресурсам другого уровня конфиденциальности пользователь может в процессе работы изменить уровень сессии, но не выше собственного уровня конфиденциальности.

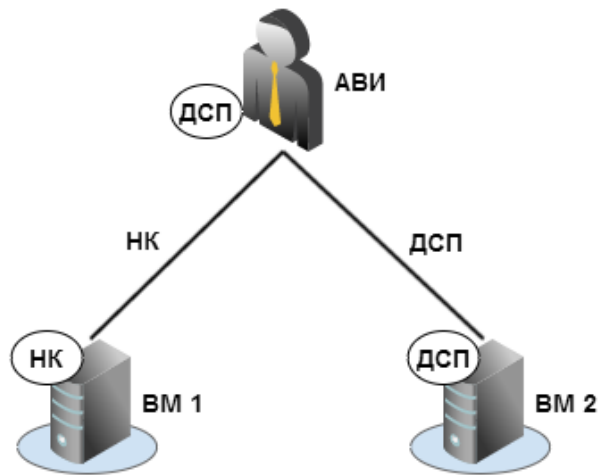
Примечание. Возможность изменения уровня сессии в агенте аутентификации vGate контролируется администратором информационной безопасности. По умолчанию возможность отключена. Подробности в разделе "Включение контроля уровня сессий" в документе [2].

Если пользователям предоставлена возможность изменять уровень сессии, то он может принимать одно из следующих значений (указаны в порядке возрастания):

- неконфиденциально;
- для служебного пользования.

Таким образом, выбирая необходимый уровень сессии, пользователь сможет выполнять операции с ресурсами разного уровня конфиденциальности (от уровня "неконфиденциально" до максимально доступного для данного пользователя уровня).

Например, АВИ может запускать ВМ 1 или ВМ 2, выбрав уровень сессии, соответствующий уровню конфиденциальности одной из этих ВМ.



Условные обозначения

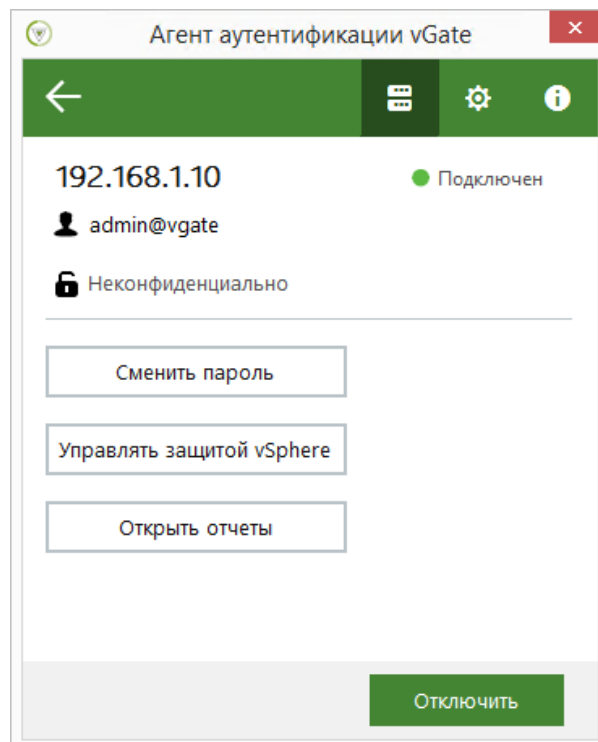
Уровни конфиденциальности		Уровни сессии	
	Неконфиденциально		Неконфиденциально
	Для служебного пользования		Для служебного пользования

Выбор уровня сессии

Для выбора уровня сессии:



1. Вызовите на экран диалог агента аутентификации, дважды щелкнув значок в правой части панели задач.



2. Выберите нужный уровень сессии:

🔒 Неконфиденциально	▼
Неконфиденциально	
Для служебного пользования	

3. В появившемся подменю выберите нужный уровень сессии.

Ввод в эксплуатацию нового оборудования

В случае ввода в эксплуатацию нового оборудования виртуальной инфраструктуры (серверов Hyper-V) необходимо проинформировать АИБ об этом и обозначить круг лиц, которым следует предоставить доступ к этим ресурсам.

Завершение работы в защищенной среде

Для завершения работы в защищенной среде:

1. Вызовите на экран диалог агента аутентификации, дважды щелкнув значок в правой части панели задач.
2. Выберите подключение и нажмите кнопку "Отключить". Подключение к серверу авторизации будет разорвано.

Примечание. Команда контекстного меню "Выход" закрывает программу. При этом также удаляется значок программы с панели задач в области уведомлений.

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