КОД БЕЗОПАСНОСТИ

Средство защиты информации

# vGate R2

## Руководство пользователя

Работа в защищенной среде (Hyper-V)

RU.88338853.501410.012 92 2


**© Компания "Код Безопасности", 2019. 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**<br>**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 |
| **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 http://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 4.2.

## 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.

# 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 АВИ 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.

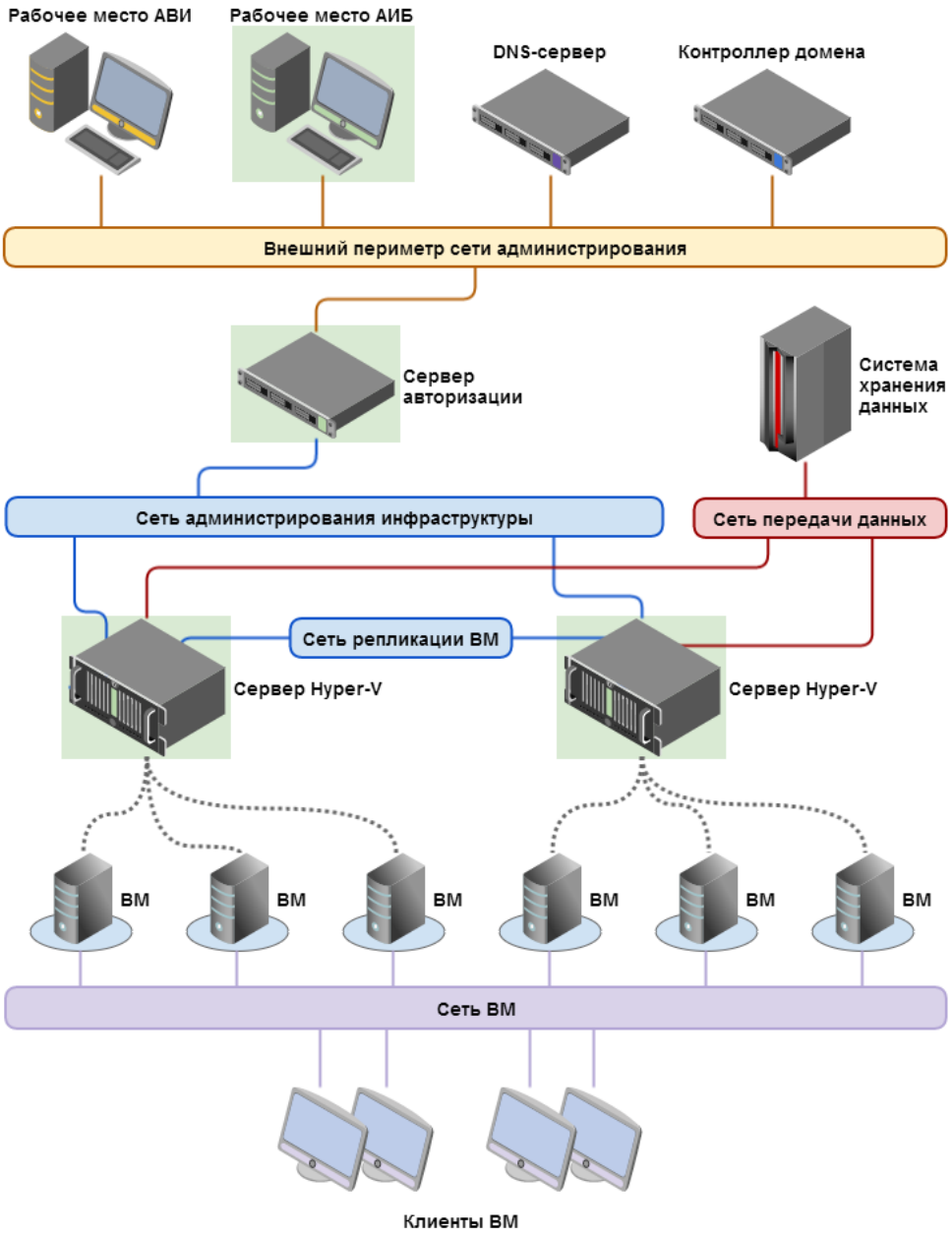



**Рис.1 Архитектура сети и размещение компонентов (маршрутизацию трафика выполняет сервер авторизации vGate)**

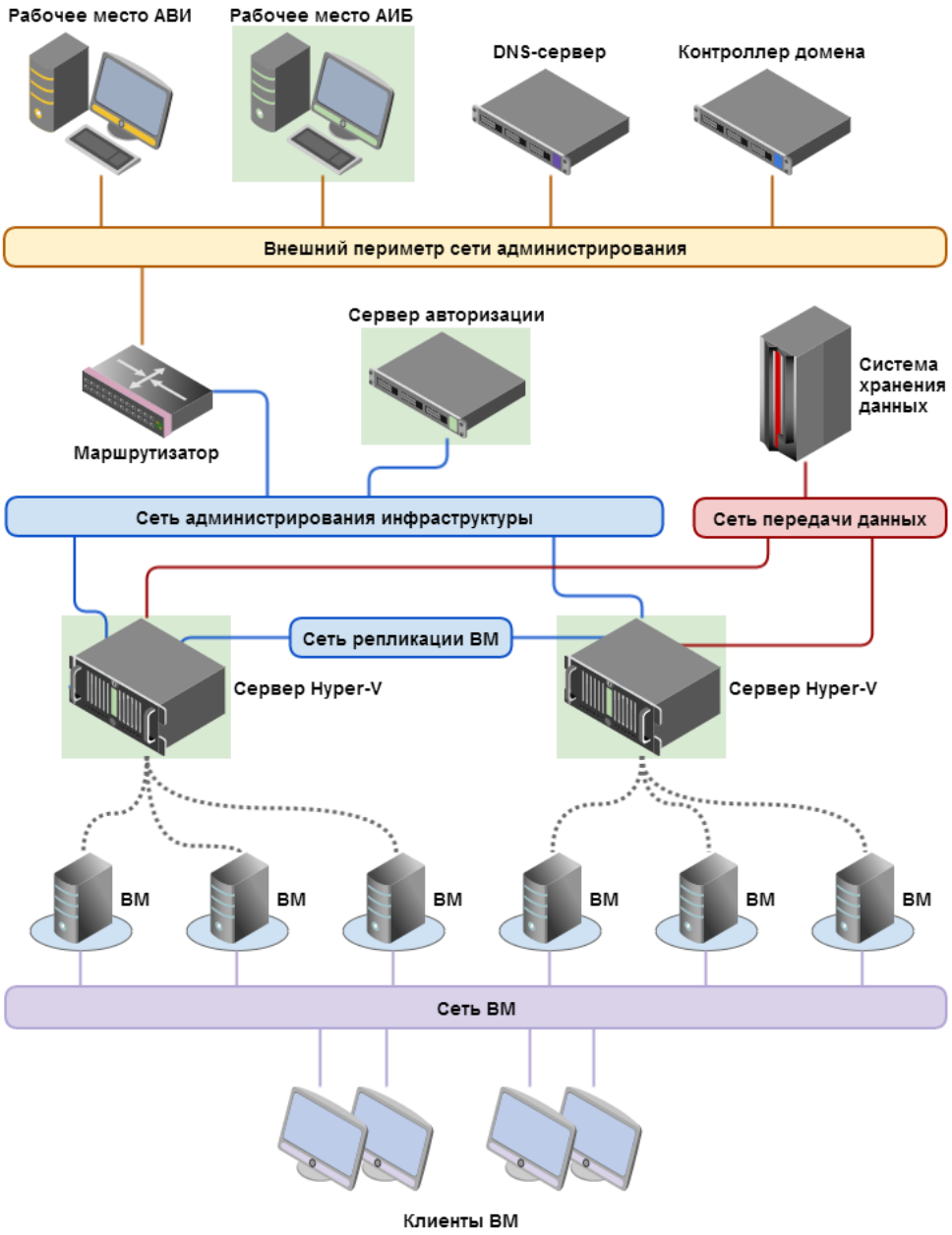



**Рис.2 Архитектура сети и размещение компонентов (маршрутизация с помощью существующего маршрутизатора в сети)**

# 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.

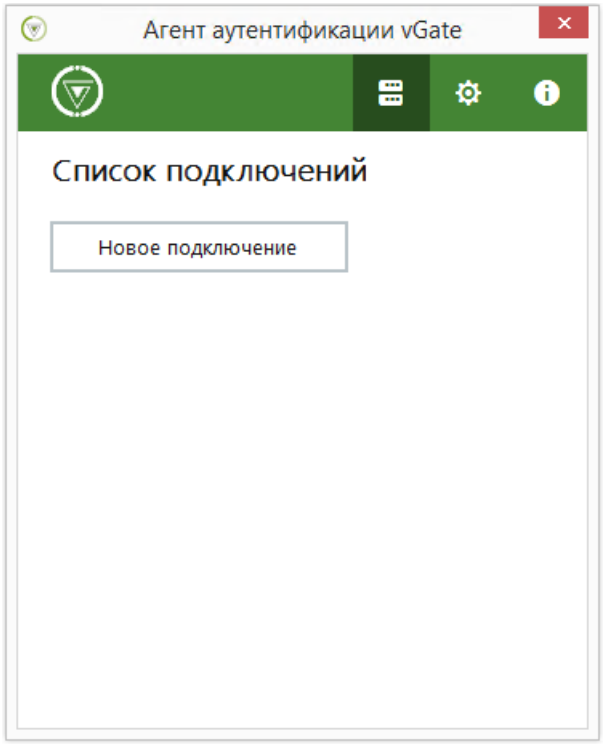
### Аутентификация пользователя

**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".

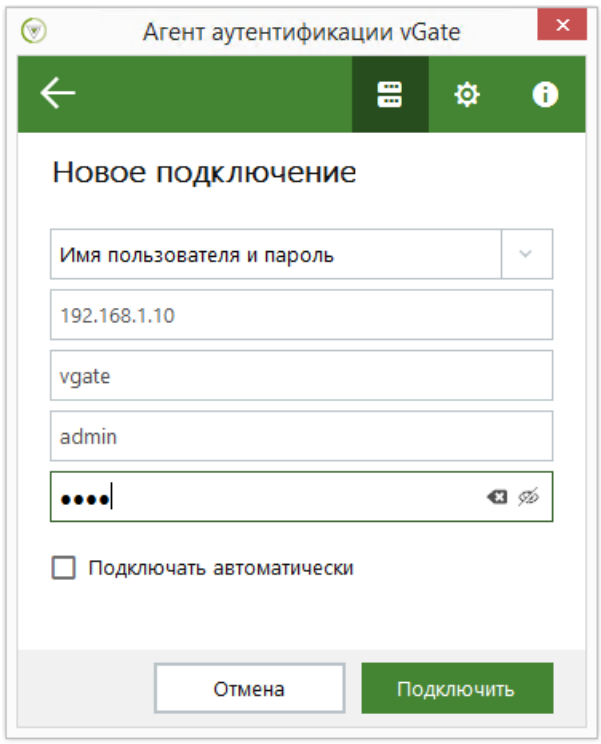
   На экране появится следующий диалог.




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.



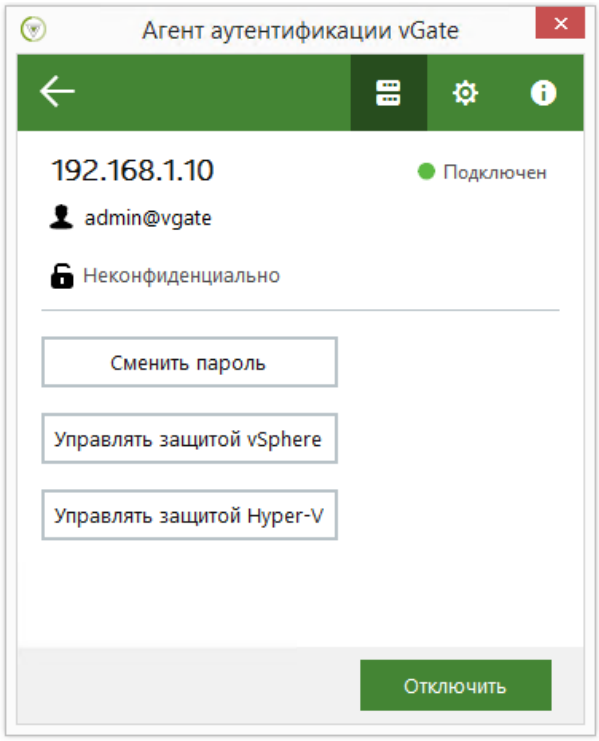

**3.** Введите учетные данные пользователя, при необходимости измените остальные параметры соединения и нажмите кнопку "Подключить".

| 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.

## Авторизация по персональному идентификатору

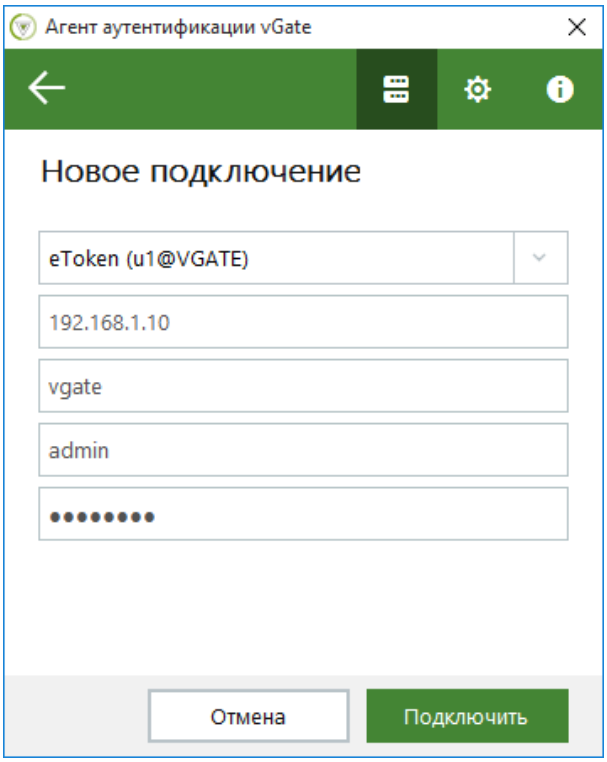
Для аутентификации пользователя возможно применение персонального идентификатора Рутокен или JaCarta.

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

**Для аутентификации с помощью персонального идентификатора:**

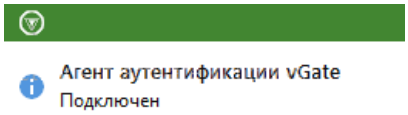
1. Запустите агент аутентификации (см. стр.**10**).
2. Подключите персональный идентификатор к компьютеру, на котором установлен агент аутентификации vGate.

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.

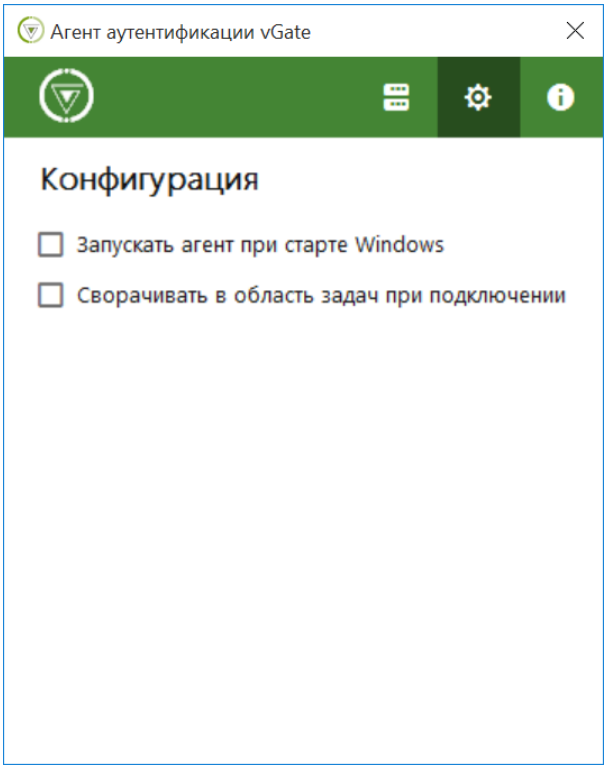



## Настройка конфигурации

**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.

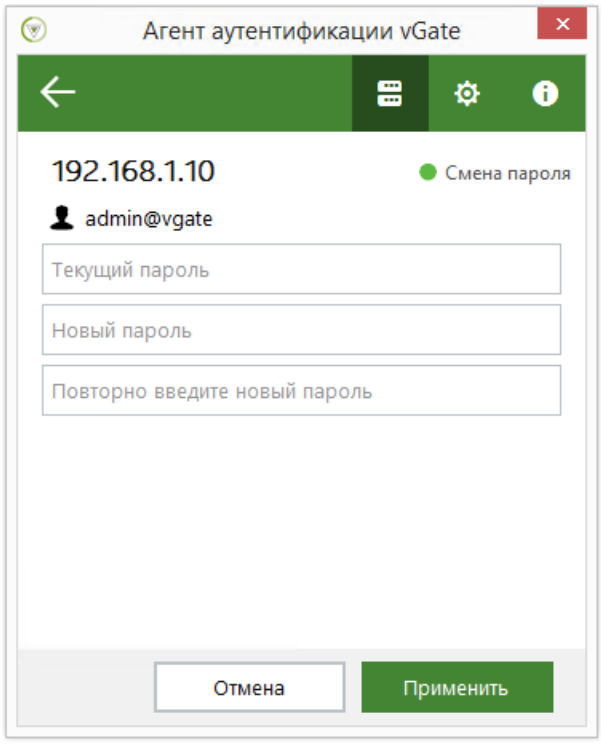
## Смена пароля

**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.




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.

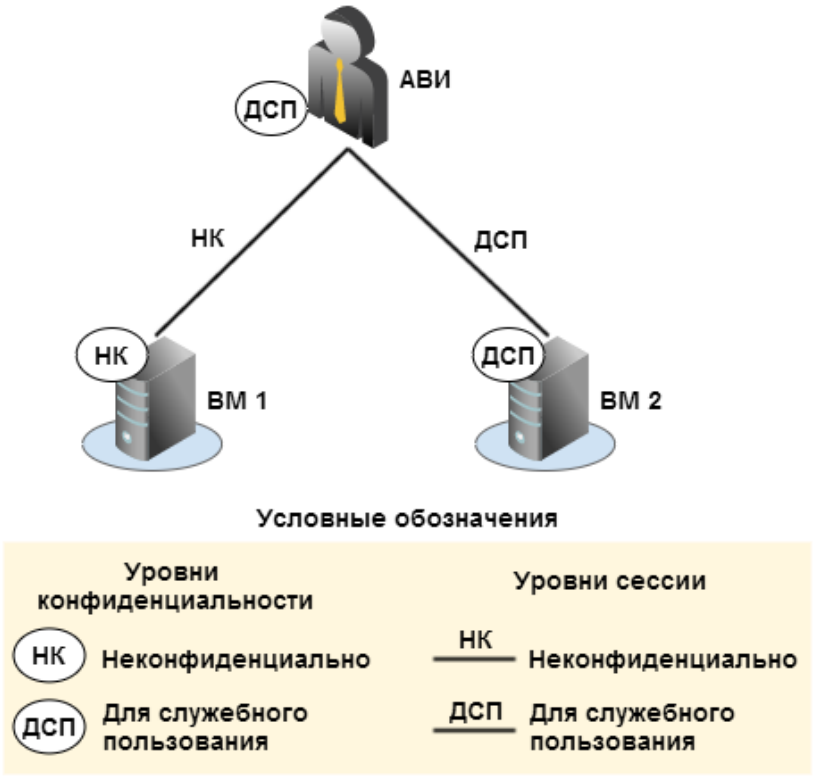
**Примечание.** Возможность изменения уровня сессии в агенте аутентификации vGate контролируется администратором информационной безопасности. По умолчанию возможность отключена. Подробности в разделе "Включение контроля уровня сессий" в документе [2].

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).

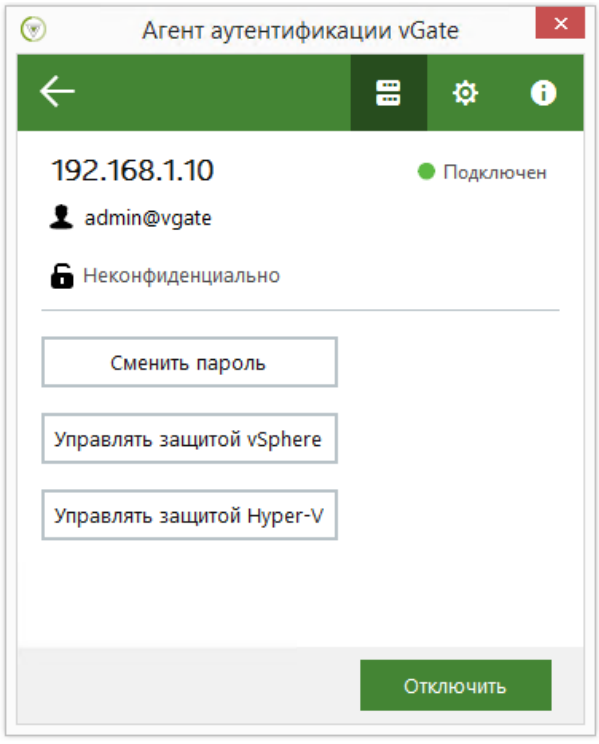
Например, АВИ может запускать ВМ 1 или ВМ 2, выбрав уровень сессии, соответствующий уровню конфиденциальности одной из этих ВМ.



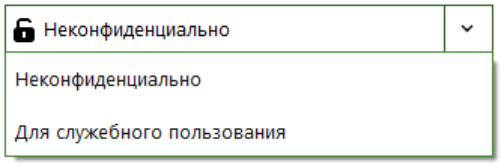

## Выбор уровня сессии

**Для выбора уровня сессии:**

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



2. Выберите нужный уровень сессии:




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.

# Глава 2
# Работа агента аутентификации в ОС Linux

Поддерживается работа агента аутентификации vGate в ОС Linux.

Выполнение команд возможно из меню программы аутентификации vGate (см. ниже) или напрямую из командной строки (см. стр.**21**).

## Выполнение команд из меню

Запустите программу аутентификации пользователя из командной строки:

```
/opt/vgate/vgcconsole
```

В случае успешного подключения к службе аутентификации на экране появится меню с доступными командами.

```
[client-linux@vgclient_fedora64 ~]$ /opt/vgate/vgcconsole
***** vGate console (version: 1.3.0001) *****

connecting to service ...
connection was extablished successfully (session id: 3)

commands:
  1 - display session state
  2 - get authentication servers
  3 - add authentication server
  4 - remove authentication server
  5 - authenticate
  6 - exit

enter a number of command:
```

Чтобы выполнить нужное действие, введите соответствующий номер команды и нажмите клавишу Enter:

- 1 – запрос информации о состоянии программы аутентификации vGate;
- 2 – запрос списка серверов авторизации vGate;
- 3 – добавление подключения к серверу авторизации;
- 4 – удаление подключения к серверу авторизации;
- 5 – аутентификация пользователя;
- 6 – завершение работы программы аутентификации.

### Запрос информации

Если аутентификация пользователя пройдена, после выполнения команды на экране появится уникальный идентификатор пользователя, его текущий уровень конфиденциальности, информация о возможности изменения уровня (параметр "level changeable") и максимально возможный уровень конфиденциальности.

Если аутентификация не пройдена, идентификатор будет равен 0.

```
current session state:
  session id: 1  user id: 238  level changeable: true  current level: 1000  max level: 2000

commands:
  1 - display session state
  2 - get authentication servers
  3 - add authentication server
  4 - remove authentication server
  5 - change user password
  6 - change level of confidentiality
  7 - logout
  8 - exit

enter a number of command:
```

Действия, доступные только для аутентифицированных пользователей:

- 5 – изменение пароля пользователя;
- 6 – изменение уровня конфиденциальности пользователя. Команда доступна только для серверов авторизации, которые поддерживают учет уровня конфиденциальности ("level changeable: true");
- 7 – выход пользователя из системы (без завершения работы программы аутентификации).

### Запрос списка серверов авторизации

После выполнения команды на экране появится список поддерживаемых серверов авторизации vGate. Для каждого сервера отображается IP-адрес, порт, состояние подключения и режим работы ("Simple mode"/"Route mode").

### Добавление подключения к серверу авторизации

После выполнения команды будут запрошены параметры добавляемого сервера авторизации: IPv4-адрес сервера и сетевой адрес шлюза для связи клиент-сервер (необходим для режима "Simple Mode").

При успешном добавлении сервера отобразится соответствующее сообщение.

**Примечание.** Убедиться в том, что сервер авторизации добавлен в список поддерживаемых серверов, можно выполнив команду "get authentication servers".

### Удаление подключения к серверу авторизации

После выполнения команды будет запрошен IPv4- адрес сервера авторизации, подключение для которого нужно удалить.

При успешном удалении сервера авторизации из списка поддерживаемых серверов отобразится соответствующее сообщение.

**Примечание.** Убедиться в том, что сервер авторизации удален из списка поддерживаемых серверов, можно выполнив команду "get authentication servers".

### Аутентификация пользователя

После выполнения команды пользователю будет предложено пройти аутентификацию с помощью учетных данных сервера авторизации или ключа JaCarta-2, если он используется.

**Для аутентификации с помощью учетных данных:**

1. Введите номер команды "authenticate by credentials" и нажмите Enter.

   На экране появится запрос параметров для аутентификации.

```
|-> commands (authenticate):
      1 - authenticate by credentials
      2 - authenticate by hardware
      3 - step back

    enter a number of command: 1

    input parameters:
      input server address (IPv4): 192.168.1.10
      input server domain: VGATE
      input user name: xxx
      input user password:
```

2. Укажите параметры (IPv4-адрес сервера авторизации, имя домена, имя и пароль пользователя) и нажмите Enter.

При успешном выполнении аутентификации отобразится соответствующее сообщение, содержащее информацию об идентификаторе пользователя, текущем и максимально возможном уровне конфиденциальности.

**Примечание.** Чтобы вернуться в основное меню, выполните команду "step back".

**Для аутентификации с помощью ключа JaCarta:**

1. Введите номер команды "authenticate by hardware" и нажмите Enter.

   На экране появится список доступных ключей.

2. Введите номер с названием нужного ключа и нажмите Enter.

   На экране появится запрос параметров для аутентификации (IPv4-адрес сервера авторизации, имя домена и PIN доступа к защищенному контейнеру ключа, в котором хранятся имя пользователя и пароль).

При успешном выполнении аутентификации отобразится соответствующее сообщение, содержащее информацию об идентификаторе пользователя, текущем и максимально возможном уровне конфиденциальности.

**Примечание.** Процесс аутентификации с помощью ключа может занять некоторое время.

### Завершение работы программы аутентификации

После выполнения команды "exit" работа программы аутентификации будет завершена.

## Работа из командной строки

Программа аутентификации vGate может быть запущена с командой, сразу выполняющей одно из действий.

Для вызова подробной информации о программе введите следующую команду:

```
/opt/vgate/vgcconsole --help
```

Доступны следующие команды управления программой аутентификации.

- Запросить версию vGate:

  ```
  /opt/vgate/vgcconsole --version
  ```

- Запросить информацию о состоянии программы аутентификации vGate:

  ```
  /opt/vgate/vgcconsole --display session state
  ```

  Если аутентификация пользователя пройдена, пользователю будет присвоен уникальный идентификатор. Если аутентификация не пройдена, идентификатор будет равен 0.

  Также в информации отображается текущий уровень конфиденциальности пользователя, информация о возможности его изменения и максимально возможный уровень конфиденциальности.

- Запросить список поддерживаемых серверов авторизации:

  ```
  /opt/vgate/vgcconsole --cmd=get_authentication_servers
  ```

- Добавить сервер авторизации в список поддерживаемых серверов:

  ```
  /opt/vgate/vgcconsole --cmd=add_authentication_server
  --server-address=IP_address
  ```

  где **server- address** – IP- адрес добавляемого сервера (например, 192.168.1.11).

- Удалить сервер авторизации из списка поддерживаемых серверов:

  ```
  /opt/vgate/vgcconsole --cmd=remove_authentication_server
  --server-address=192.168.1.11
  ```

  где **server- address** – IP- адрес удаляемого сервера (например, 192.168.1.11).

- Аутентификация пользователя:

  ```
  /opt/vgate/vgcconsole --cmd=authenticate
  --server-address=192.168.1.11 --domain=VGATE
  --user-name=test --user-password=`123qwe
  ```

где:

- **server- address** – IP- адрес сервера авторизации (например, 192.168.1.11);
- **domain** – имя реестра учетных записей vGate, указанное при установке сервера авторизации (например, VGATE);
- **user-name** – имя пользователя (например, test);
- **user-password** – пароль пользователя (например, `123qwe).

# Документация

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