КОД безопасности

Средство защиты информации

vGate R2

Руководство пользователя

Работа в защищенной среде

RU.88338853.501410.012 92 1

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**

Учетная запись для доступа к виртуальной инфраструктуре ... 7

Подготовка сети к установке vGate ... 7

Работа в защищенной среде ОС Windows ... **10**

Подключение к защищенной среде ... 10

Аутентификация пользователя с помощью агента аутентификации ... 10

Аутентификация 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

Надежное удаление ВМ ... 18

Формат командной строки утилиты ... 18

Пример надежного удаления ... 19

Завершение работы в защищенной среде ... 20

Доступ к виртуальной инфраструктуре через веб-интерфейс ... **21**

Работа агента аутентификации в ОС Linux ... **23**

Выполнение команд из меню ... 23

Работа из командной строки ... 25

Документация ... **27**

Список сокращений

AD	Active Directory — служба каталогов MS Windows
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
ВМ	Виртуальная машина (англ. — VM)
ИБ	Информационная безопасность
КЦ	Контроль целостности
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)
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/.

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.

Данное руководство предназначено для администраторов изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся сведения, необходимые для установки компонента vGate Service Pack 1.

Документ предназначен для vGate версии 4.5.

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 VMware vSphere.

Глава 1
Подготовка к установке vGate

Учетная запись для доступа к виртуальной инфраструктуре

Для доступа к виртуальной инфраструктуре пользователю потребуется учетная запись администратора виртуальной инфраструктуры или администратора информационной безопасности с привилегией "Разрешен доступ к виртуальной инфраструктуре" (см. документ [2]).

В целях безопасности при создании учетной записи АИБ рекомендуется указать соответствующую учетную запись администратора VMware vSphere, ограниченную в полномочиях возможностью просмотра конфигурации элементов виртуальной инфраструктуры (Read-Only).

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 vCenter (vCSA), ESXi-серверам и т. д.).

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.

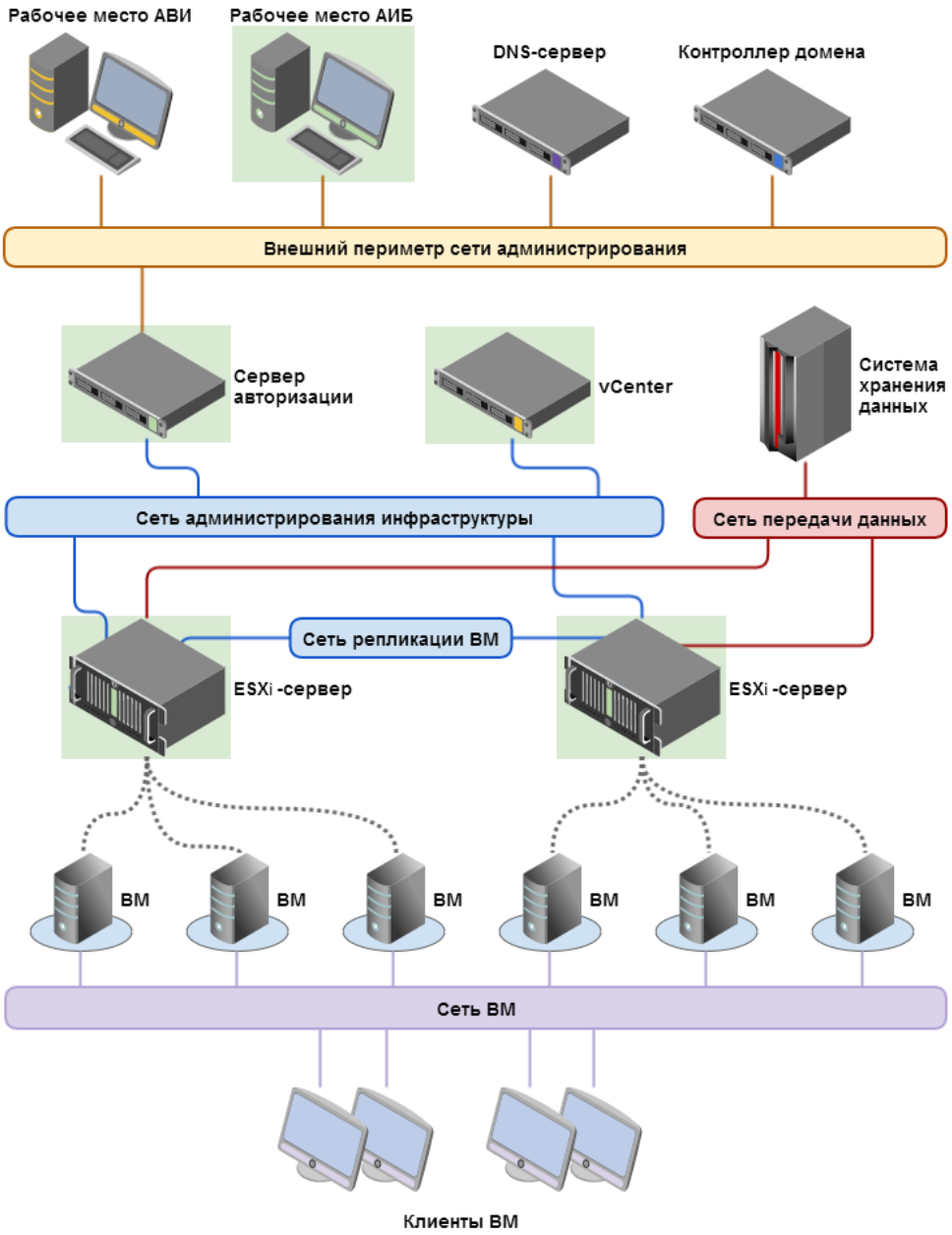


Рис.1 Архитектура сети и размещение компонентов (маршрутизацию трафика выполняет сервер авторизации vGate)

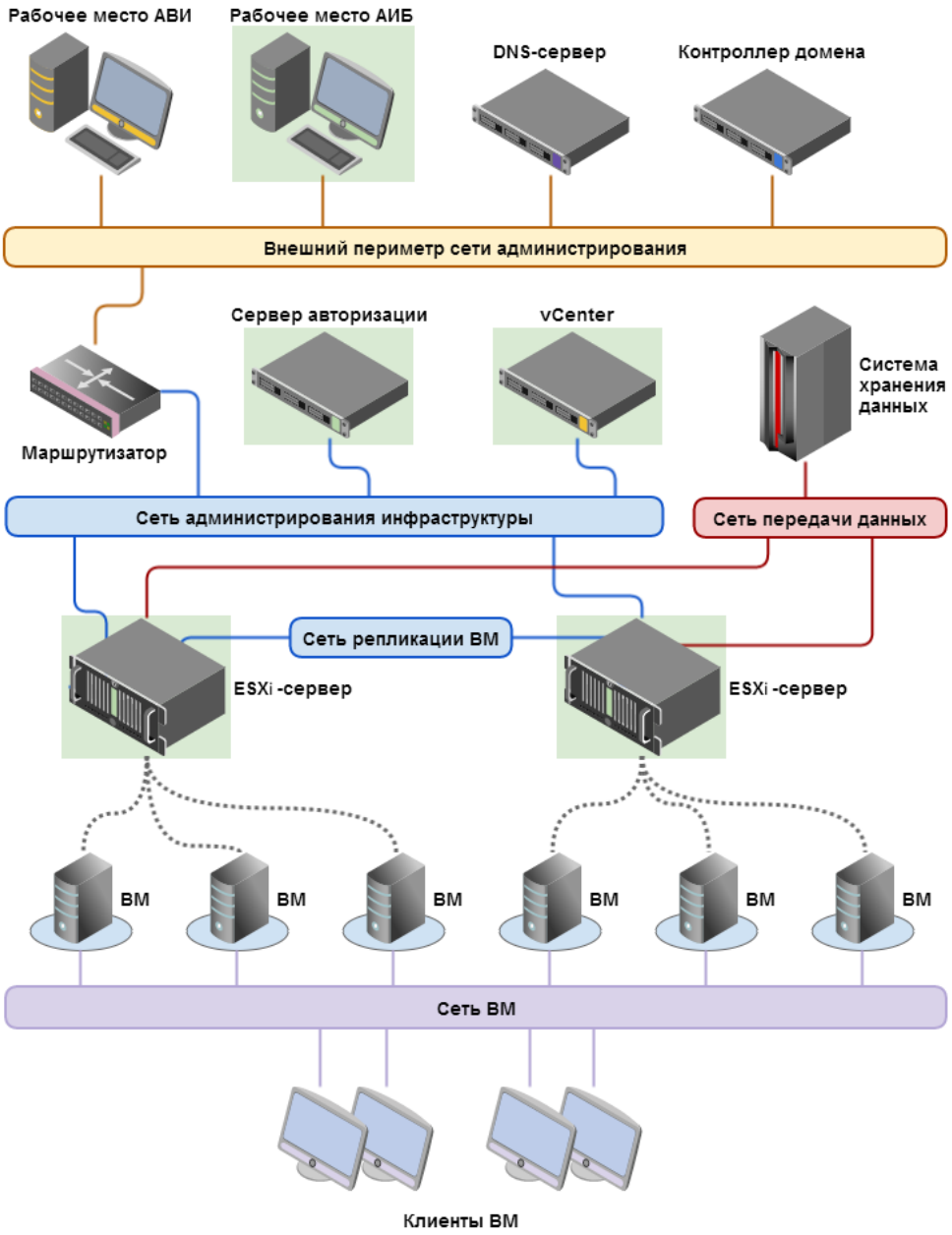


Рис.2 Архитектура сети и размещение компонентов (маршрутизация с помощью существующего маршрутизатора в сети)

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), администраторов информационной безопасности и компьютеров. Аутентификация компьютеров выполняется автоматически.

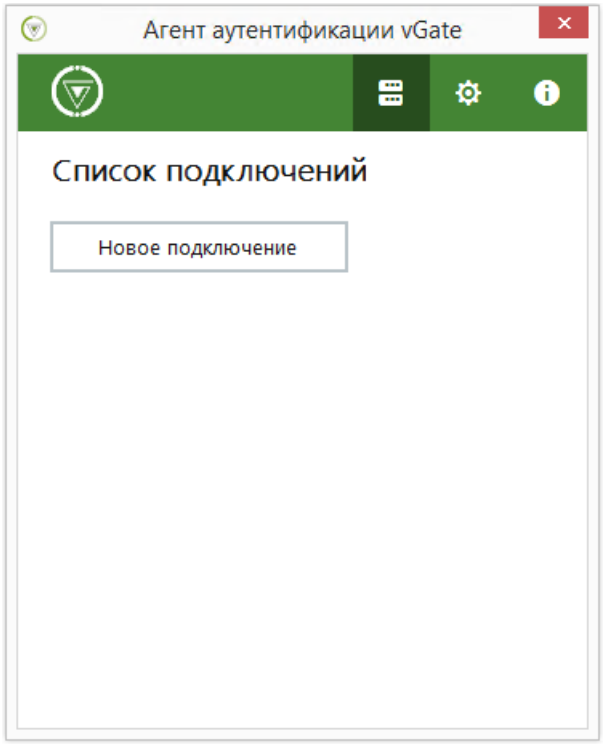
Аутентификация пользователя выполняется с помощью агента аутентификации (см. стр.**10**) или через веб-интерфейс vGate (см. стр.**21**).

Аутентификация пользователя с помощью агента аутентификации

Для выполнения процедуры аутентификации:

1. Войдите в систему с правами администратора компьютера.
2. Выберите в меню "Пуск" команду "Приложения | Код Безопасности | Агент аутентификации vGate".

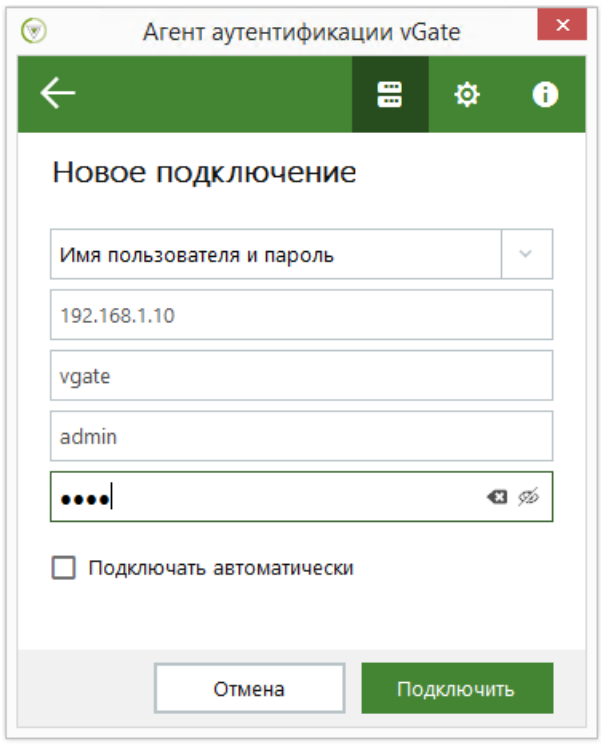
   На экране появится следующий диалог.



3. 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.



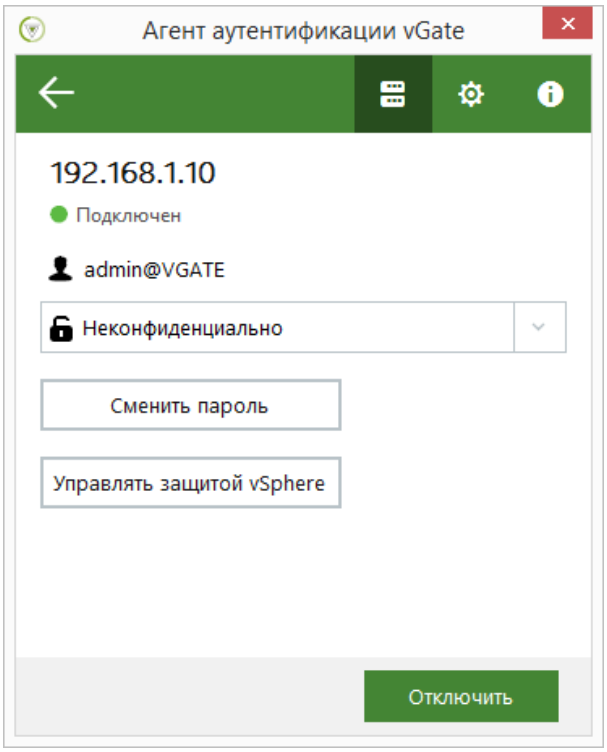
4. Введите учетные данные пользователя, при необходимости измените остальные параметры соединения и нажмите кнопку "Подключить".

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 или администратора информационной безопасности
Пароль	Пароль администратора
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.

5. Подключение к серверу авторизации появится в списке.



Примечание.

- Если на компьютере установлена консоль управления vGate и вход в агент аутентификации выполнен с помощью учетной записи АИБ, консоль управления будет доступна по кнопке "Управлять защитой vSphere".
- 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.

Аутентификация по персональному идентификатору

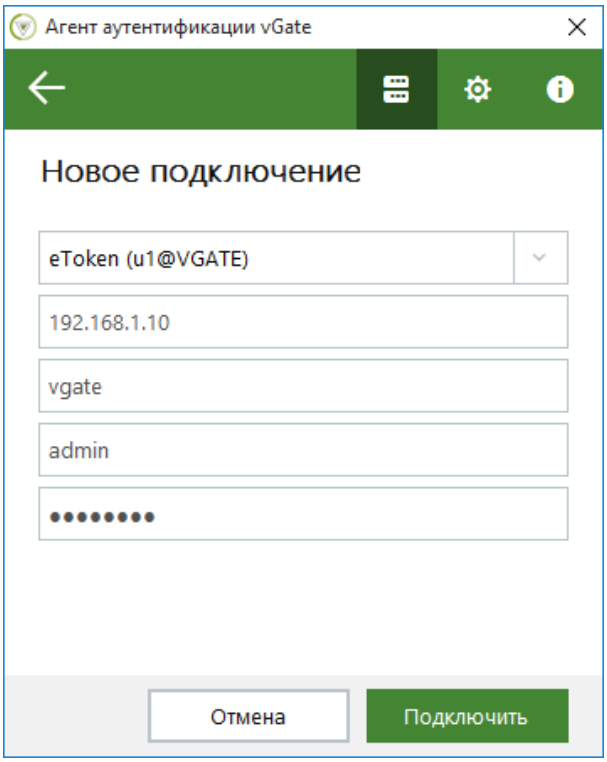
Для аутентификации пользователя возможно применение персонального идентификатора Рутокен или JaCarta.

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

Для аутентификации с помощью персонального идентификатора:

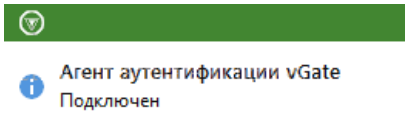
1. Подключите персональный идентификатор к компьютеру, на котором установлен агент аутентификации vGate.
2. Запустите агент аутентификации (см. стр.**10**).

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.



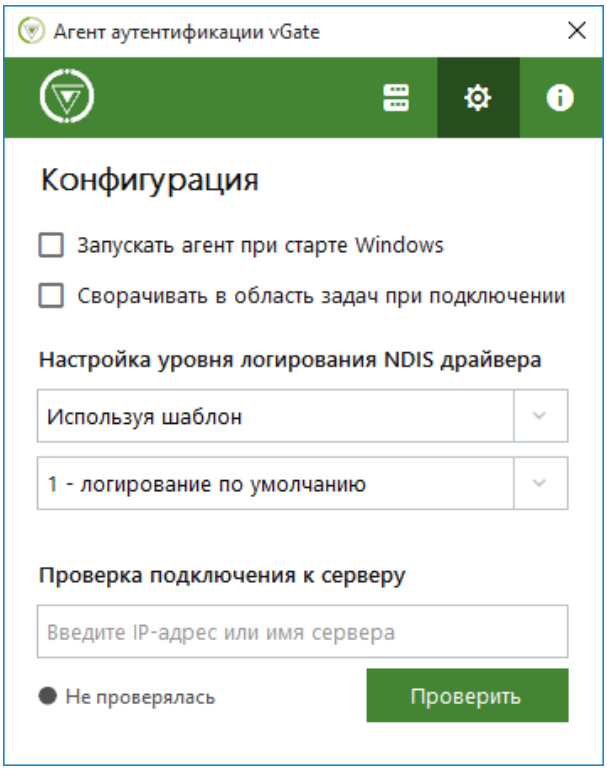
При последующих подключениях в сообщении будет отображаться время предыдущего входа в агент аутентификации.

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, отметив нужные пункты.
4. При необходимости настройте уровень логирования NDIS-драйвера. Это может понадобиться при диагностике и решении проблем vGate. Укажите уровень логирования вручную или используя шаблон. Будет установлено шестнадцатеричное значение параметра EnableLogging в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vGateNdisDriver.

Примечание. Для настройки уровня логирования необходимо запустить агент аутентификации vGate от имени администратора.

5. Чтобы проверить подключение к серверу авторизации, укажите IP-адрес или полное доменное имя (FQDN) сервера в поле "Проверка подключения к серверу". По умолчанию в поле содержится адрес сервера, указанный для первого подключения списка подключений (см. стр.**10**).

Примечание. Для корректной работы функции проверки подключения к серверу необходимо отключить на компьютере Windows Firewall или выполнить следующие действия:

- в Windows Firewall добавить правило типа "Для программы", разрешив входящий трафик службам drvmgr.exe и client.exe, или добавить правила, разрешающие входящий трафик по протоколам ICMP и 144;
- на сервере авторизации добавить правило, разрешающее входящий трафик по протоколу ICMP.

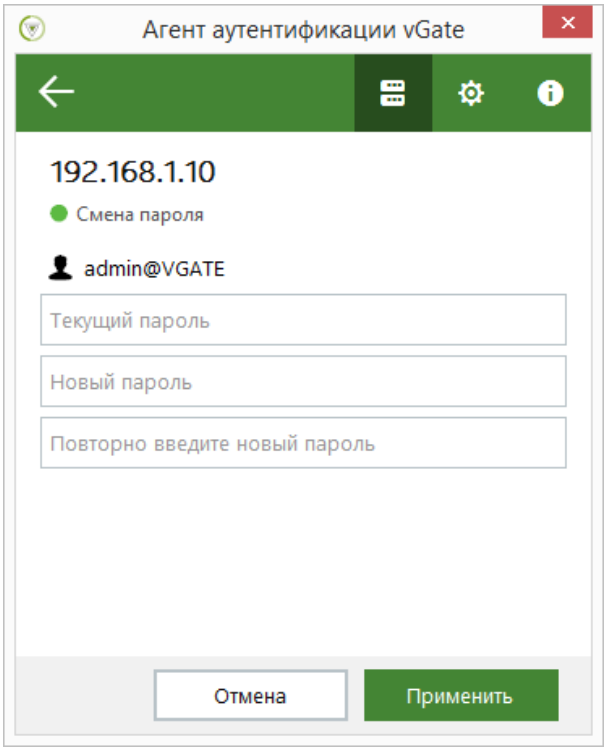
Смена пароля

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.

Примечание.

- В случае отсутствия у АВИ прав доступа к серверу виртуализации при попытке авторизации в vSphere Web Client рядом с областью уведомлений на панели задач отображается сообщение агента аутентификации vGate "Соединение заблокировано".
- В случае отказа в выполнении операции по управлению виртуальной инфраструктурой соответствующее уведомление отображается в vSphere Web Client с сообщением о том, что операция заблокирована vGate.

Особенности работы с конфиденциальными ресурсами

Каждому пользователю назначается уровень конфиденциальности, позволяющий ему выполнять операции с ресурсами (ESXi-серверы, ВМ, хранилища, виртуальные сети) 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), доступ к хранилищу ВМ, 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.

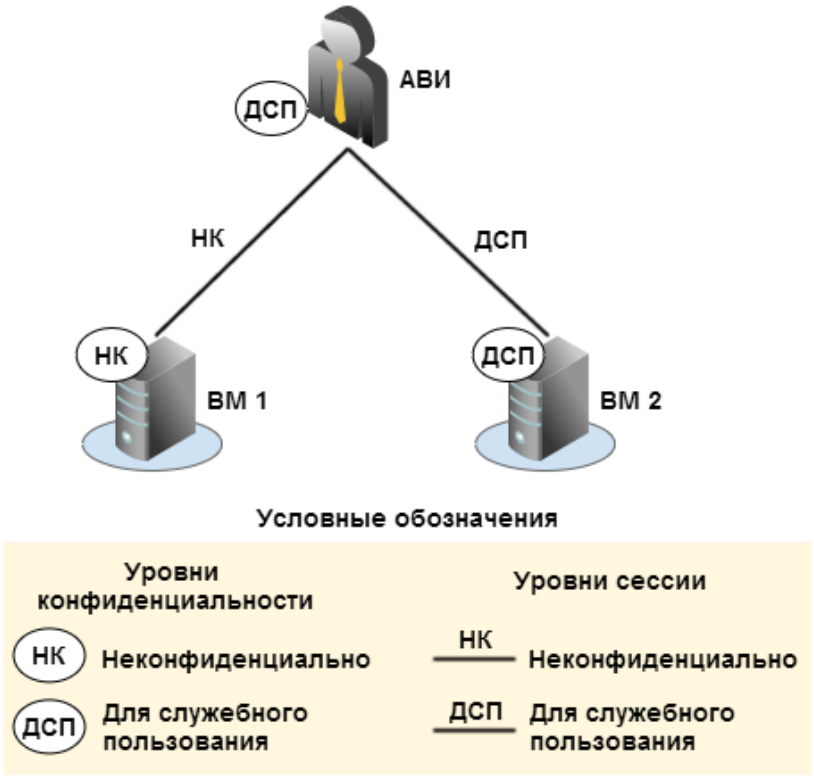
Примечание. Возможность изменения уровня сессии в агенте аутентификации vGate контролируется администратором информационной безопасности. По умолчанию возможность отключена. Подробности в разделе "Включение контроля уровня сессий" в документе [2].

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).

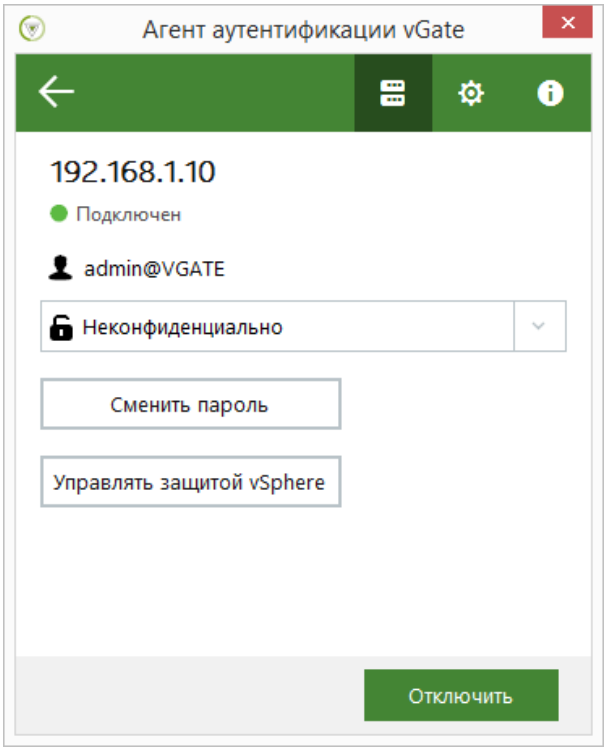
Например, АВИ может запускать ВМ 1 или ВМ 2, выбрав уровень сессии, соответствующий уровню конфиденциальности одной из этих ВМ.



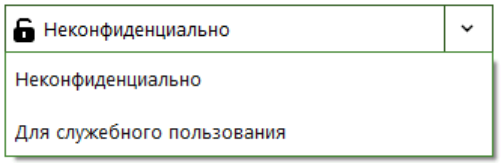
Выбор уровня сессии

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 (ESXi-серверы, хранилища ВМ, физические сетевые адаптеры, виртуальные сети) необходимо проинформировать АИБ об этом и обозначить круг лиц, которым следует предоставить доступ к этим ресурсам.

Надежное удаление ВМ

Внимание! Для выполнения операции надежного удаления ВМ АВИ должен иметь доступ к ESXi-серверу или серверу vCenter (а именно к TCP-портам 902, 443), на котором выполняется удаляемая ВМ, а также иметь привилегию "Операции с файлами в хранилищах".

Для безопасного вывода ВМ из эксплуатации, т. е. удаления ВМ без возможности последующего восстановления, необходимо перед удалением ВМ выполнить очистку дисков ВМ.

Если для удаляемой ВМ задана соответствующая политика безопасности, очистка дисков виртуальных машин выполняется автоматически. Если политика не задана, для этого может использоваться специальная утилита командной строки vmdktool.exe.

Совет. Утилита также может быть полезна в том случае, если ВМ была удалена не полностью, а только какой-либо ее диск.

Перед очисткой диска ВМ необходимо убедиться в отсутствии у виртуальной машины снимков (snapshots[1]), после чего необходимо остановить ВМ.

Примечание. Перед использованием утилиты vmdktool на компьютере необходимо установить компонент Microsoft Visual C++ 2015 Redistributable с обновлением KB2999226.

Формат командной строки утилиты

Командная строка утилиты надежного удаления ВМ имеет следующий формат.

Для удаления ВМ с ESXi-сервера:

```
>vmdktool.exe –s [arg] –u [arg] -p [arg] -m [arg] -v [arg] –d [arg] –t [arg]
```

Для удаления ВМ с сервера vCenter:

```
>vmdktool.exe –s [arg] –u [arg] -p [arg] -m [arg] -v vmPath=[arg] –d [arg] –t [arg]
```

[1] Снимок (Snapshot) — снимок состояния ВМ (содержимое памяти, настройки ВМ, содержимое дисков) в определенный момент времени. Возврат к снимку (revert to snapshot) восстанавливает сохраненное состояние ВМ.

Описание параметров командной строки утилиты приведено в таблице.

Параметр	Описание
-s [arg]	Сетевое имя или IP-адрес сервера ESXi/vCenter
-u [arg]	Имя учетной записи администратора сервера ESXi/vCenter
-p [arg]	Пароль администратора сервера ESXi/vCenter
-m [arg]	Отпечаток SSL сертификата
-v [arg]	Полный путь к файлу конфигурации ВМ (*.vmx)
-d [arg]	Полный путь к диску ВМ (*.vmdk)
-t [arg]	Число, указывающее на код байта, которым заполняется диск ВМ. Значение аргумента: от 0 до 255. Значение по умолчанию: 255

Примечание. Номер порта ESXi-сервера по умолчанию равен 902, сервера vCenter — 443.

Для просмотра справки по утилите используйте следующую команду:

```
>vmdktool.exe –?
```

Пример надежного удаления

Пусть заданы следующие параметры:

Параметр	Значение
Имя ESXi-сервера	esx5.esx.local
Имя администратора ESXi-сервера	root
Имя сервера vCenter	vcenter60.vg.text
Имя администратора сервера vCenter	admin@vsphere.local
Пароль администратора сервера ESXi/vCenter	P@ssw0rd
Отпечаток SSL сертификата	42:1A:39:6E:D3:4D:B6:A9:5F:C4:1F:C4:B0:C3:4E:38:42:6A:1C:71
Полный путь к файлу конфигурации ВМ (*.vmx) для ESXi	"[storage1] vm4/vm4.vmx"
Полный путь к файлу конфигурации ВМ (*.vmx) для vCenter	Datacenter/vm/vm4
Полный путь к диску ВМ (*.vmdk)	[storage1] vm4/vm4.vmdk
Число, указывающее на код байта для заполнения диска	55

Для удаления ВМ с ESXi-сервера в командной строке следует ввести следующую команду:

```
>vmdktool.exe -s esx5.esx.local -u root -p P@ssw0rd -m
42:1A:39:6E:D3:4D:B6:A9:5F:C4:1F:C4:B0:C3:4E:38:42:6A:1C:71
-v "[storage1] vm4/vm4.vmx" -d "[storage1] vm4/vm4.vmdk"
-t 55
```

Для удаления ВМ с сервера vCenter в командной строке следует ввести следующую команду:

```
>vmdktool.exe -s vcenter60.vg.text -u admin@vsphere.local -p
P@ssw0rd -m
42:1A:39:6E:D3:4D:B6:A9:5F:C4:1F:C4:B0:C3:4E:38:42:6A:1C:71
-v vmPath=Datacenter/vm/vm4 -d "[storage1] vm4/vm4.vmdk"
-t 55
```

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 3
Доступ к виртуальной инфраструктуре через веб-интерфейс

Для доступа пользователя к виртуальной инфраструктуре без агента аутентификации администратору информационной безопасности необходимо создать правила разграничения доступа для защищаемых серверов (см. документ [2]).

Внимание!

- Не поддерживается одновременная работа пользователя в двух разных доменах.
- Сессия пользователя через агент аутентификации vGate имеет более высокий приоритет при одновременном использовании агента аутентификации и веб-интерфейса для доступа к виртуальной инфраструктуре.

Примечание. При доступе к виртуальной инфраструктуре через веб-интерфейс может быть недоступна функция скачивания файлов в vSphere Web Client. В этом случае необходимо использовать ESXi Embedded Host Client.

Для выполнения процедуры аутентификации:

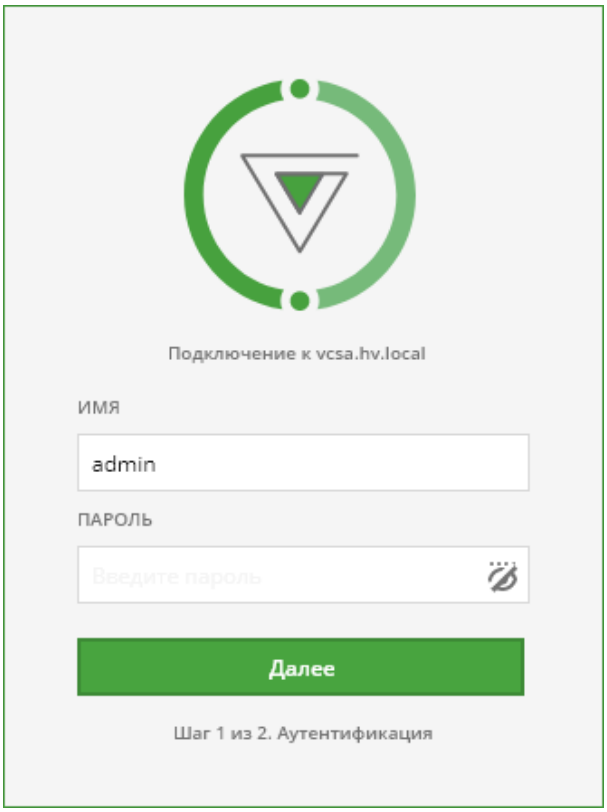
1. Запустите браузер и введите следующий URL-адрес:

   https://<protected_server>

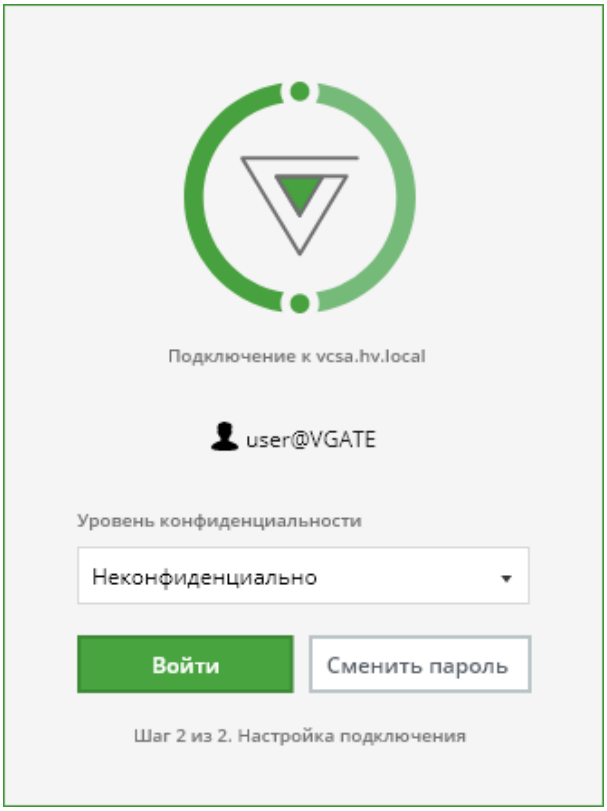
   где <protected_server> — IP-адрес или полное доменное имя (FQDN) защищаемого сервера.

   Примечание. Для доступа к серверу vCenter (vCSA) рекомендуется использовать полное доменное имя сервера. При использовании IP-адреса сервера, авторизация проходит только со второй попытки.

   На экране появится следующий диалог.



2. Введите учетные данные пользователя и нажмите кнопку "Далее".
   Появится следующий диалог.



Примечание. Чтобы изменить пароль пользователя, нажмите кнопку "Сменить пароль". В появившемся окне введите текущий и новый пароль.

3. Выберите уровень конфиденциальности сессии из списка возможных вариантов (см. стр.**16**) и нажмите кнопку "Войти".
   Будет выполнен переход на страницу защищаемого сервера.

Примечание.

- При доступе к виртуальной инфраструктуре без агента аутентификации выбрать уровень конфиденциальности сессии и изменить пароль можно только при аутентификации.
- При бездействии пользователя сессия автоматически прерывается через 15 минут. Принудительный выход пользователя из системы не предусмотрен.

Глава 4
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.**25**).

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. 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