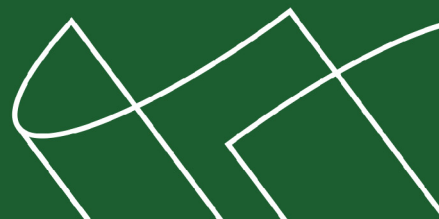


**Код безопасности**  
ГК «Информзащита»

Средство защиты информации

**vGate R2**



## **Руководство пользователя**

Работа в защищенной среде



## Код безопасности

ГК «Информзащита»

© Компания "Код Безопасности", 2011. 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: **127018, г. Москва, ул. Суцеский Вал,  
дом 47, стр. 2, помещение №1**

Телефон: **(495) 980-23-45**

Факс: **(495) 980-23-45**

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

Web: **<http://www.securitycode.ru>**

# Оглавление

<b>Список сокращений .....</b>	<b>4</b>
<b>Введение .....</b>	<b>5</b>
<b>Назначение vGate .....</b>	<b>5</b>
<b>Глава 1. Подготовка к установке vGate.....</b>	<b>6</b>
Подготовка сети к установке vGate .....	6
Создание учетной записи для АИБ .....	6
Подготовка персонального идентификатора .....	7
<b>Глава 2. Работа в защищенной среде .....</b>	<b>8</b>
Подключение к защищенной среде .....	8
Аутентификация пользователя.....	8
Авторизация по персональному идентификатору .....	8
Проверка состояния подключения.....	8
Смена пароля .....	9
Доступ к элементам управления виртуальной инфраструктурой .....	9
Особенности работы с конфиденциальными ресурсами.....	9
Управление уровнем доступа .....	9
Выбор уровня сессии .....	10
Ввод в эксплуатацию нового оборудования .....	10
Надежное удаление VM.....	10
Формат командной строки утилиты.....	11
Пример надежного удаления .....	11
Завершение работы в защищенной среде .....	11
<b>Документация .....</b>	<b>12</b>

## Список сокращений

<b>SAN</b>	Система хранения данных (рус. СХД)
<b>VM</b>	Виртуальная машина (рус. VM)
<b>АВИ</b>	Администратор виртуальной инфраструктуры
<b>АИБ</b>	Администратор информационной безопасности
<b>АС</b>	Автоматизированная система
<b>VM</b>	Виртуальная машина (англ. VM)
<b>НСД</b>	Несанкционированный доступ
<b>ПО</b>	Программное обеспечение
<b>СВТ</b>	Средства вычислительной техники
<b>СЗИ</b>	Средство защиты информации
<b>СХД</b>	Система хранения данных (англ. SAN)

## Введение

Данное руководство предназначено для администраторов виртуальной инфраструктуры<sup>1</sup>, защищаемой продуктом "Средство защиты информации vGate R2" (далее — vGate). В документе содержатся сведения, необходимые для работы в защищенной среде.

### Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) 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.** Некоторые примечания могут и 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.** Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (<http://www.securitycode.ru/>) или связаться с представителями компании по электронной почте ([support@securitycode.ru](mailto:support@securitycode.ru) и [hotline@infosec.ru](mailto:hotline@infosec.ru)). Актуальную версию эксплуатационной документации на программный продукт можно посмотреть на сайте компании по адресу: [http://www.securitycode.ru/products/sn\\_vmware/documentation/](http://www.securitycode.ru/products/sn_vmware/documentation/).

**Учебные курсы.** Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте <http://www.itsecurity.ru/>. Связаться с представителем Учебного центра можно по электронной почте ([edu@infosec.ru](mailto:edu@infosec.ru)).

## Назначение vGate

vGate предназначен для обеспечения безопасности виртуальной инфраструктуры, развернутой с использованием систем VMware vSphere 4, VMware vSphere 4.1 или VMware vSphere 5.

<sup>1</sup> В отношении пользователей vGate принята следующая терминология:

- Пользователь, выполняющий функции администратора информационной безопасности, называется "Администратором".
- "Пользователями" считаются администраторы виртуальной инфраструктуры.

## Глава 1

# Подготовка к установке vGate

## Подготовка сети к установке vGate

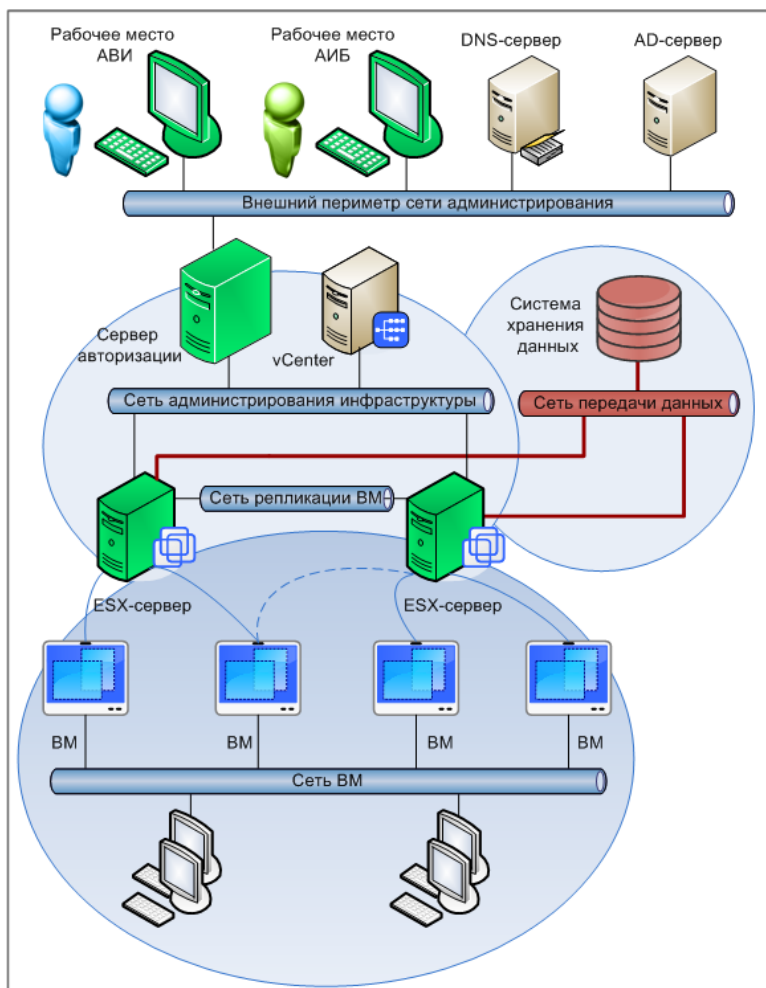
До установки vGate необходимо:

- Подключить необходимое дополнительное оборудование (сервер авторизации, рабочее место АИБ 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 (ESX-серверам, vCenter и т. д.).

Правила конфигурирования сети, требования к оборудованию, а также порядок настройки маршрутизации приведены в документе "Руководство администратора. Установка, обновление и удаление" [ 2 ].

Пример виртуальной инфраструктуры и размещения компонентов vGate представлен на рисунке:



## Создание учетной записи для АИБ

Для доступа к виртуальной инфраструктуре администратору информационной безопасности необходимо создать учетную запись в среде VMware vSphere 4, VMware vSphere 4.1 или VMware vSphere 5. Эта учетная запись должна ограничить полномочия АИБ по управлению виртуальной инфраструктурой только возможностью просмотра конфигурации элементов виртуальной инфраструктуры.

## Подготовка персонального идентификатора

Если на рабочем месте АВИ установлена система Secret Net 5.1, то для аутентификации пользователя возможно использование персонального идентификатора (e-token).

Перед его использованием на рабочем месте необходимо выполнить предварительные настройки:

1. Выполните инициализацию персонального идентификатора в Secret Net 5.1 согласно документации на нее.
2. Подключите персональный идентификатор к ПК.
3. Запустите агент аутентификации (см. стр. 8).
4. Введите имя и пароль пользователя, отметьте поле "Входить в систему автоматически" и нажмите кнопку "Подключиться".

Пароль будет сохранен в персональный идентификатор (e-token).

## Глава 2

# Работа в защищенной среде

## Подключение к защищенной среде

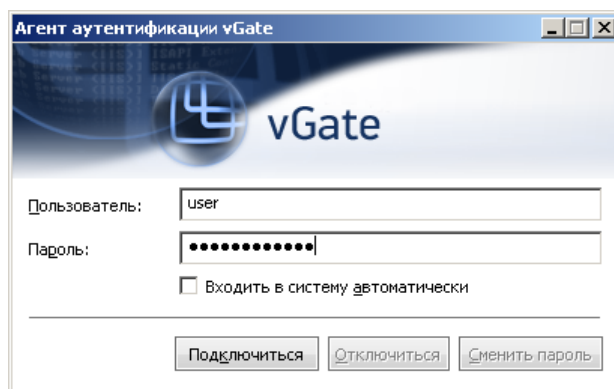
Доступ на управление виртуальной инфраструктурой получают только пользователи, прошедшие аутентификацию. В vGate предусмотрена процедура аутентификации пользователей (администраторов виртуальной инфраструктуры) и компьютеров. Аутентификация компьютеров выполняется автоматически.

### Аутентификация пользователя

**Для выполнения процедуры аутентификации:**

1. Выберите в меню "Пуск" команду "Программы | Код безопасности | vGate | Вход в систему".

На экране появится диалог:



**Примечание.** Если установить отметку в поле "Входить в систему автоматически", то последующие подключения пользователя к защищенной среде будут выполняться автоматически (без запроса пароля).

2. Введите учетные данные (имя пользователя и пароль) и нажмите кнопку "Подключиться".

### Авторизация по персональному идентификатору

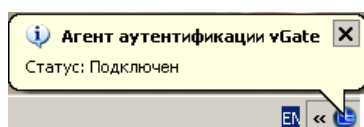
Для авторизации по персональному идентификатору необходимо выполнить предварительную настройку (см. стр. 7). После этого вход пользователя будет осуществляться автоматически после подключения персонального идентификатора к ПК и загрузки операционной системы.



Иногда может потребоваться также ввод PIN-кода персонального идентификатора (если при его инициализации был изменен PIN-код по умолчанию).

### 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:



## Смена пароля



**Важно!** 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 контекстное меню для значка, находящегося в правой части панели задач.
2. В контекстном меню выберите пункт "Сменить пароль...".

На экране появится диалог:

3. Введите старый пароль, дважды укажите новый пароль и нажмите кнопку "OK".

## 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 (ESX-серверы, VM, 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 VM, редактирование параметров VM (в том числе и сетевых), доступ к хранилищу VM, перемещение VM и т. д.

### Управление уровнем доступа

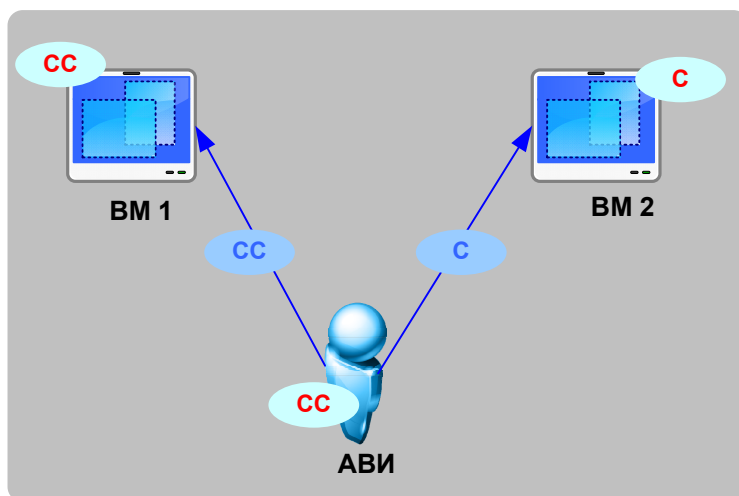
Каждый сеанс работы пользователя при подключении к защищенной среде получает уровень сессии "неконфиденциально". При этом пользователь может выполнять только операции с ресурсами того же уровня конфиденциальности, т. е. "неконфиденциально". Для доступа к ресурсам большего уровня конфиденциальности пользователь может в процессе работы изменить уровень сессии, но не выше собственного уровня конфиденциальности.

Уровень сессии может принимать одно из следующих значений (указаны в порядке возрастания):

- неконфиденциально;
- для служебного пользования;
- секретно;
- совершенно секретно.

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 VM 1 и VM 2, выбрав уровень сессии, соответствующий уровню конфиденциальности VM:



Условные обозначения:

Уровни конфиденциальности:	Уровни сессии:
<b>CC</b> Совершенно секретно	<b>CC</b> Совершенно секретно
<b>C</b> Секретно	<b>C</b> Секретно

## Выбор уровня сессии

Для выбора уровня сессии:



1. Вызовите контекстное меню для значка, находящегося в правой части панели задач.
2. В контекстном меню выберите пункт "Уровень сессии".
3. В появившемся подменю выберите нужный уровень сессии.

## Ввод в эксплуатацию нового оборудования

В случае ввода в эксплуатацию нового оборудования виртуальной инфраструктуры (ESX-серверы, хранилища VM, физические сетевые адаптеры, виртуальные сети) необходимо проинформировать АИБ об этом и обозначить круг лиц, которым следует предоставить доступ к этим ресурсам.

## Надежное удаление VM



**Важно!** Для выполнения операции надежного удаления VM АВИ должен иметь доступ к ESX-серверу (а именно к TCP-портам 902, 903, 443), на котором выполняется удаляемая VM, а также иметь привилегию "разрешено скачивать файлы виртуальных машин".

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

Если для удаляемой VM 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 была удалена не VM полностью, а только какой-то ее диск.

Перед очисткой диска VM необходимо убедиться в отсутствии у виртуальной машины снапшотов<sup>2</sup>, после чего необходимо остановить VM.

## Формат командной строки утилиты

Командная строка утилиты для надежного удаления VM имеет следующий формат:

```
>vmdktool.exe -h [arg] --port [arg] -u [arg] -p [arg] -v [arg] -d [arg] -t [arg]
```

Описание параметров командной строки утилиты приведено в таблице:

Параметры	Описание
-s [arg]	Сетевое имя или IP-адрес ESX-сервера <sup>3</sup>
-h [arg]	Номер порта ESX-сервера. Значение по умолчанию: 902
-u [arg]	Имя учетной записи администратора ESX-сервера
-p [arg]	Пароль администратора ESX-сервера
-v [arg]	Полный путь к файлу конфигурации VM (*.vmx)
-d [arg]	Полный путь к диску VM (*.vmdk)
-t [arg]	Число, которым заполняется диск VM. Значение аргумента: от 0 до 255. Значение по умолчанию: 255

Для просмотра справки по утилите используйте следующую команду:

```
>vmdktool.exe -?
```

## Пример надежного удаления

Пусть заданы следующие параметры:

Имя ESX-сервера	esx4.esx.local
Номер порта ESX-сервера	902
Имя администратора ESX-сервера	root
Пароль администратора ESX-сервера	P@ssw0rd
Полный путь к файлу конфигурации VM (*.vmx)	[storage1] vm4/vm4.vmx"
Полный путь к диску VM (*.vmdk)	[storage1] vm4/vm4.vmdk
Число для заполнения	55

В командной строке указываем:

```
>vmdktool.exe -s esx4.esx.local -u root -p P@ssw0rd -v "[storage1] vm4/vm4.vmx" -d "[storage1] vm4/vm4.vmdk" -t 55
```

## Завершение работы в защищенной среде



### Для завершения работы в защищенной среде:

1. Вызовите контекстное меню для значка, находящегося в правой части панели задач.
2. В контекстном меню выберите пункт "Отключиться".

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

<sup>2</sup> Снапшот (Snapshot) — снимок состояния VM (содержимое памяти, настройки VM, содержимое дисков) в определенный момент времени. Возврат к снапшоту (revert to snapshot) восстанавливает сохраненное состояние VM.

<sup>3</sup> Безопасное удаление VM через vCenter не поддерживается.

## Документация

<b>1</b>	Средство защиты информации vGate R2. Руководство администратора. Общие сведения	RU.88338853.501410.012 91 1
<b>2</b>	Средство защиты информации vGate R2. Руководство администратора. Установка, обновление и удаление	RU.88338853.501410.012 91 2
<b>3</b>	Средство защиты информации vGate R2. Руководство администратора. Настройка и эксплуатация	RU.88338853.501410.012 91 3
<b>4</b>	Средство защиты информации vGate R2. Руководство администратора. Как начать работу	RU.88338853.501410.012 91 4
<b>5</b>	Средство защиты информации vGate R2. Руководство пользователя. Работа в защищенной среде	RU.88338853.501410.012 92