



КОД БЕЗОПАСНОСТИ

Средство защиты информации

**vGate R2**

**Руководство администратора**

Быстрый старт



## 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

<b>Список сокращений</b> .....	<b>4</b>
<b>Введение</b> .....	<b>5</b>
<b>Назначение vGate</b> .....	<b>6</b>
<b>Компоненты vGate</b> .....	<b>7</b>
<b>Ввод в эксплуатацию vGate</b> .....	<b>8</b>
<b>Устранение неисправностей</b> .....	<b>9</b>
Распространенные ошибки .....	9
Ответы на вопросы .....	9
<b>Документация</b> .....	<b>10</b>

## Список сокращений

<b>AD</b>	Active Directory — служба каталогов MS Windows
<b>DNS</b>	Domain Name System (система доменных имен)
<b>iSCSI</b>	Internet Small Computer System Interface — протокол для управления системами хранения и передачи данных на основе TCP/IP
<b>vCenter</b>	Централизованное средство управления ESXi-серверами и виртуальными машинами
<b>vCSA</b>	vCenter Server Appliance — виртуальный модуль с установленным сервером vCenter и связанными с ним службами
<b>PSC</b>	Platform Services Controller — компонент, обеспечивающий работу служб виртуальной инфраструктуры VMware
<b>АВИ</b>	Администратор виртуальной инфраструктуры
<b>АИБ</b>	Администратор информационной безопасности
<b>АС</b>	Автоматизированная система
<b>БД</b>	База данных
<b>ВМ</b>	Виртуальная машина (англ. — VM)
<b>Главный АИБ</b>	Главный администратор информационной безопасности
<b>ИБ</b>	Информационная безопасность
<b>НСД</b>	Несанкционированный доступ
<b>ОС</b>	Операционная система
<b>ОЗУ</b>	Оперативное запоминающее устройство
<b>ПО</b>	Программное обеспечение
<b>ПРД</b>	Правила разграничения доступа
<b>СВТ</b>	Средства вычислительной техники
<b>СЗИ</b>	Средство защиты информации
<b>СХД</b>	Система хранения данных (англ. — SAN)
<b>КЦ</b>	Контроль целостности
<b>ЦПУ</b>	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](mailto:vgateinfo@securitycode.ru).

Данное руководство предназначено для администраторов изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся сведения, необходимые для первоначальной настройки и эксплуатации vGate.

Документ предназначен для vGate 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](mailto: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](mailto:education@securitycode.ru).

## Назначение vGate

vGate предназначен для обеспечения безопасности виртуальной инфраструктуры, развернутой с использованием системы виртуализации VMware vSphere.

# Компоненты vGate

При развертывании компоненты vGate располагаются согласно схеме:



Компоненты vGate выполняют следующие функции.

Компонент	Функции
<b>Сервер авторизации</b>	Основной сервер авторизации выполняет следующие функции: <ul style="list-style-type: none"> <li>• Аутентификация пользователей и компьютеров.</li> <li>• Разграничение доступа к средствам управления виртуальной инфраструктурой.</li> <li>• Хранение данных.</li> <li>• Регистрация событий безопасности.</li> <li>• Автоматическое развертывание компонентов защиты vGate на ESXi-серверах.</li> <li>• Репликация данных (при наличии резервного сервера)</li> </ul>
<b>Резервный сервер авторизации</b>	При сбое основного сервера резервный сервер берет на себя все функции сервера авторизации. Осуществляет репликацию данных и хранение информации о пользователях и настройках
<b>Агент аутентификации</b>	Выполняет функцию идентификации и аутентификации пользователей и компьютеров
<b>Компонент защиты ESXi-сервера</b>	Выполняет контроль целостности VM и осуществляет защиту от НСД внутри сети администрирования. Контролирует целостность модулей и настроек vGate
<b>Компонент защиты vCenter</b>	Осуществляет управление фильтрацией входящего трафика и защиту от НСД внутри сети администрирования
<b>Компонент защиты PSC</b>	Осуществляет защиту от НСД внутри сети администрирования
<b>Консоль управления</b>	Осуществляет централизованное управление vGate
<b>Веб-консоль</b>	Осуществляет управление настройками мониторинга и сегментирования через веб-интерфейс
<b>Сервер мониторинга</b>	Выполняет сбор и корреляцию событий виртуальной инфраструктуры
<b>Средство просмотра отчетов</b>	Позволяет формировать отчеты о состоянии параметров безопасности виртуальной инфраструктуры, произошедших событиях и внесенных в конфигурацию изменениях
<b>Служба развертывания vGate</b>	Осуществляет установку агентов vGate на защищаемые ESXi-серверы

# Ввод в эксплуатацию vGate

## Для развертывания и настройки vGate:

1. Ознакомьтесь с ограничениями использования продукта (см. Release Notes).
2. Ознакомьтесь с требованиями к программному и аппаратному обеспечению (см. раздел "Системные требования" в документе [2]).
3. Настройте сеть администрирования, отделив ее от сети защищаемых компьютеров и сети виртуальных машин (см. раздел "Правила конфигурирования локальной сети" в документе [2]).
4. Выберите способ маршрутизации трафика (см. раздел "Настройка маршрутизации между подсетями" в документе [2]):
  - с помощью сервера авторизации;
  - с помощью отдельного маршрутизатора.
5. При необходимости подготовьте резервный сервер авторизации.
6. Выполните установку сервера авторизации vGate, консоли управления и средства просмотра отчетов (см. раздел "Установка и настройка сервера авторизации" в документе [2]).
7. При использовании резервирования выполните установку ПО vGate на резервном сервере авторизации (см. раздел "Установка и настройка сервера авторизации с резервированием" в документе [2]).
8. Установите компонент "Агент аутентификации" на компьютер АИБ.
9. Установите компонент "Агент аутентификации" на рабочем месте АВИ.
10. В консоли управления зарегистрируйте имеющуюся лицензию на использование vGate для защиты ESXi-серверов (см. раздел "Регистрация лицензии" в документе [2]).
11. Добавьте в список защищаемых объектов серверы vCenter и ESXi (см. раздел "Регистрация защищаемых серверов" в документе [2]).
12. Установите компоненты vGate на защищаемые серверы vCenter и ESXi (см. раздел "Развертывание компонентов защиты" в документе [2]).
13. Создайте учетные записи пользователей (см. раздел "Управление учетными записями пользователей" в документе [2]).
14. Настройте метки безопасности (см. раздел "Настройка меток безопасности" в документе [2]) и назначьте их учетным записям и объектам виртуальной инфраструктуры (см. раздел "Настройка полномочного управления доступом к конфиденциальным ресурсам" в документе [2]).
15. Назначьте наборы политик безопасности защищаемым объектам или группам объектов (см. раздел "Настройка политик безопасности" в документе [2]).
16. Настройте правила разграничения доступа к защищаемым серверам (см. раздел "Управление доступом к защищаемым серверам" в документе [2]).



# Устранение неисправностей

## Распространенные ошибки

Список проблем, которые могут возникнуть при работе с ПО vGate, и способы их решения находятся в документе Troubleshooting.html (расположен на установочном диске в папке \Documentation).

Особенности работы vGate и возможные ошибки описаны в документе ReleaseNotes.html (расположен на установочном диске в папке \Documentation\VSphere).

## Ответы на вопросы

Данный раздел содержит список частых вопросов и ответы на них.

Вопрос	Ответ
В vGate 4.3 поддерживается работа с несколькими серверами vCenter?	Да. Для этого необходимо объединить серверы vCenter с помощью режима VMware vCenter Linked Mode
Как переустановить служебные учетные записи vGate 4.3 в Active Directory?	<ol style="list-style-type: none"> <li>1. Удалите служебные учетные записи vGate из Active Directory.</li> <li>2. Запустите программу установки сервера авторизации vGate.</li> <li>3. В диалоге изменения параметров установки нажмите кнопку "Изменить" и следуйте указаниям мастера. Все текущие настройки vGate при этом сохраняются.</li> <li>4. По окончании установки будут созданы новые служебные учетные записи vGate в Active Directory.</li> <li>5. Отключите автоматическую смену паролей для служебных учетных записей</li> </ol>
Почему установка агента аутентификации на компьютере в сети защищаемых серверов завершается ошибкой?	Установка агента аутентификации внутри защищаемого периметра не поддерживается (см. раздел "Конфигурирование локальной сети" в документе [2])

## 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