КОД безопасности

Средство защиты информации

vGate R2

Руководство администратора

Установка, настройка и эксплуатация (Hyper-V)

RU.88338853.501410.012 91 2-2

© Компания "Код Безопасности", 2021. 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

AD	Active Directory — служба каталогов MS Windows
DNS	Domain Name System (система доменных имен)
IOPS	Input/output operations per second — количество операций, выполняемых системой хранения данных за одну секунду
iSCSI	Internet Small Computer System Interface — протокол для управления системами хранения и передачи данных на основе TCP/IP
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
БД	База данных
ВМ	Виртуальная машина (англ. — VM)
Главный АИБ	Главный администратор информационной безопасности
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 изделия "Средство защиты информации vGate R2" RU.88338853.501410.012 (далее — vGate). В документе содержатся сведения, необходимые для установки, настройки и эксплуатации vGate.

Документ предназначен для vGate for Hyper-V версии 4.4.

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.

Глава 1
Установка vGate

Требования к оборудованию и программному обеспечению

Системные требования

К компьютерам, на которые устанавливаются компоненты vGate, предъявляются следующие системные требования.

Компонент	Операционная система
Сервер авторизации	• Windows Server 2012 R2 x64 + Update KB2999226. • Windows Server 2016 x64. • Windows Server 2019 x64. Минимальная необходимая пропускная способность канала для сети резервирования — 10 Мбит/с. Для компонента "Сервер авторизации" требуется 10 ГБ на жестком диске. Дополнительно: • Драйверы JaCarta (при использовании персонального идентификатора JaCarta). • Драйверы для Рутокен S, Lite и ЭЦП (при использовании персонального идентификатора Рутокен)
Резервный сервер авторизации	• Windows Server 2012 R2 x64 + Update KB2999226. • Windows Server 2016 x64. • Windows Server 2019 x64. Для компонента "Сервер авторизации" требуется 10 ГБ на жестком диске. Минимальная необходимая пропускная способность канала для сети резервирования — 10 Мбит/с
Агент аутентификации	• Microsoft Windows 8.1 x86/x64. • Microsoft Windows 10 Enterprise. • Microsoft Windows Server 2012 R2 x64 + Update KB2999226. • Microsoft Windows Server 2016 x64. • Microsoft Windows Server 2019 x64. Для компонента "Агент аутентификации" требуется 200 МБ на жестком диске. Дополнительно: • Драйверы JaCarta (при использовании персонального идентификатора JaCarta). • Драйверы для Рутокен S, Lite и ЭЦП (при использовании персонального идентификатора Рутокен)
Консоль управления	• Microsoft Windows 8.1 x86/x64. • Microsoft Windows 10 Enterprise. • Microsoft Windows Server 2012 R2 x64 + Update KB2999226. • Microsoft Windows Server 2016 x64. • Microsoft Windows Server 2019 x64
Модули защиты Hyper-V	• Windows Server 2012 x64 + Update KB2999226. • Windows Server 2012 R2 x64 + Update KB2999226. • Windows Server 2016 x64. • Windows Server 2019 x64. • Microsoft Hyper-V Server 2012 R2. • Microsoft Hyper-V Server 2016. • Microsoft Hyper-V Server 2019. Для компонента защиты Hyper-V требуется 200 МБ на жестком диске

Компонент защиты System Center Virtual Machine Manager (SCVMM)	• Windows Server 2012 R2 x64 + Update KB2999226. • Windows Server 2016 x64. • Windows Server 2019 x64. • Microsoft System Center 2012 R2 Virtual Machine Manager. • Microsoft System Center 2016 Virtual Machine Manager
Сервер мониторинга	Microsoft Hyper-V Server, удовлетворяющий минимальным требованиям: • процессор — 2 ядра CPU; • память — 4 ГБ; • хранилище — 20 ГБ

Требования ПО vGate к аппаратному обеспечению совпадают с требованиями операционных систем.

Внимание! Имеются следующие системные ограничения:
- Установка сервера авторизации и модуля защиты Hyper-V на контроллер домена не поддерживается.
- Не поддерживается протокол IPv6. Поэтому при установке сервера авторизации необходимо отключить протокол IPv6 в свойствах сетевого адаптера.

Внимание! При использовании контроллера домена для хранения учетных записей vGate необходимо выбирать контейнер, имя и полный путь к которому не содержат символов кириллицы.

Внимание! Для корректной установки ПО vGate на компьютеры с ОС Windows необходимо на время установки отключить самозащиту в Kaspersky Endpoint Security.

Примечание.
- Совместное использование персональных идентификаторов JaCarta и Рутокен не поддерживается.
- Не поддерживается использование JaCarta PKI/ГОСТ.

Соответствие размеров виртуальных инфраструктур, защищаемых с помощью vGate 4.4, рекомендуемым системным требованиям указано в таблице ниже.

Количество компонентов защиты vGate	Потоки ЦПУ	ОЗУ (ГБ)	Диск (IOPS)
10	2	2	100
50	4	5	300
100	6	8	550
200	12	15	1050
300	16	22	1550

Требования к аппаратному обеспечению

Требования к конфигурации компьютера, на который устанавливаются компоненты vGate, совпадают с требованиями к ОС, установленной на нем.

Серверы Hyper-V должны быть оборудованы необходимым числом независимых Ethernet-интерфейсов для реализации конфигурирования локальной сети.

На компьютере, предназначенном для сервера авторизации, должно быть не менее одного Ethernet-интерфейса при развертывании vGate с использованием маршрутизатора (см. стр.**15**) и не менее двух Ethernet-интерфейсов при использовании сервера авторизации для маршрутизации трафика (см. стр.**20**).

Внимание! Работа ПО vGate с использованием Fibre Channel не гарантируется.

Внимание! Компьютеры, предназначенные для установки компонентов vGate, должны быть оборудованы необходимым количеством физических Ethernet-интерфейсов. Работа vGate с виртуальными сетевыми адаптерами на физических компьютерах не поддерживается.

Внимание! Допускается установка сервера авторизации на ВМ, но располагать его на защищаемом vGate сервере не рекомендуется.

План установки

Развертывание vGate рекомендуется проводить в следующем порядке:

№	Шаг установки	Особенности	Описание
1	**Конфигурирование локальной сети**		См. стр.**11**
2	**Установка и настройка сервера авторизации**	Выполняется в случае развертывания сервера без резервирования: • Выполняется установка сервера авторизации. • Выполняется первоначальная настройка в процессе установки ПО. • Создается учетная запись главного АИБ в процессе установки ПО	См. стр.**14**
	Установка и настройка сервера авторизации с резервированием	Выполняется в случае развертывания сервера с резервированием (функция доступна только в vGate Enterprise и Enterprise Plus). Основной сервер: • Выполняется установка и первоначальная настройка сервера авторизации. • Создается учетная запись главного АИБ в процессе установки ПО. • Устанавливается компонент "Резервирование конфигурации". Резервный сервер: • Выполняется установка резервного сервера авторизации. • Выполняется первоначальная настройка в процессе установки ПО	См.стр.**26**
4	**Установка компонента защиты соединений Hyper-V**	Компонент защиты соединений устанавливается на сервер Hyper-V, если необходимо обеспечить фильтрацию соединений Hyper-V с помощью vGate	См. стр.**47**
5	**Установка компонентов защиты виртуальной инфраструктуры**	Во время первоначальной настройки vGate в консоли управления выполняется установка компонентов защиты: • на сервер System Center Virtual Machine Manager (SCVMM), если он присутствует в конфигурации; • на серверы Hyper-V	См. стр. стр.**87**
6	**Установка и настройка сервера мониторинга**	Выполняется развертывание компонентов ПО vGate, обеспечивающих работу мониторинга безопасности, в следующем порядке: • выполняется развертывание и настройка сервера мониторинга; • в веб-консоли vGate выполняется настройка подключения к серверу мониторинга	См. стр.**49**
7	**Установка ПО на компьютер АИБ**	• Устанавливаются агент аутентификации и консоль управления Hyper-V. Этот шаг следует пропустить, если рабочее место АИБ на сервере авторизации	См. стр.**46**
8	**Установка ПО на компьютер АВИ**	Устанавливается агент аутентификации	См.стр.**46**

№	Шаг установки	Особенности	Описание
9	**Установка ПО на другие компьютеры из внешнего периметра сети администрирования инфраструктуры**	Устанавливается агент аутентификации на компьютеры, которые располагаются во внешнем периметре сети администрирования, если с них будут осуществляться входящие соединения во внутренний периметр	См. стр.46

Конфигурирование локальной сети

Правила конфигурирования локальной сети

Чтобы обеспечить надежный уровень защиты, необходимо до установки компонентов vGate выполнить конфигурирование сети, руководствуясь следующими правилами:

- Сеть администрирования виртуальной инфраструктуры (защищаемый периметр, в котором размещаются серверы Hyper-V и сервер SCVMM) рекомендуется отделить от сети виртуальных машин и других сетей виртуальной инфраструктуры.
- Если в виртуальной инфраструктуре используются функции динамической миграции (Live Migrations) и репликации, рекомендуется организовать отдельную сеть репликации виртуальных машин, отделив ее от сетей администрирования и сетей виртуальных машин.
- Если данные виртуальных машин хранятся за пределами серверов Hyper-V в отдельной системе хранения, рекомендуется создать сеть передачи данных на основе технологии Ethernet (iSCSI) или SMB 3.0. При необходимости сеть передачи данных и сеть репликации виртуальных машин могут быть совмещены.

Для работы в сети, сконфигурированной таким образом, серверы Hyper-V должны иметь необходимое число независимых Ethernet-интерфейсов.

Внимание! Не рекомендуется использование протокола DHCP для Ethernet-интерфейсов, подключенных к защищаемому периметру и периметру сети администрирования.

Внимание! При использовании режима интеграции с Active Directory, в котором сервер авторизации vGate входит в домен Windows, выполните следующие рекомендации:

- не размещайте контроллер домена в защищаемом периметре сети администрирования виртуальной инфраструктуры;
- сервер авторизации не поддерживает автоматическую смену паролей для служебных учетных записей vGate в домене Windows. Поэтому необходимо создать отдельное организационное подразделение (Organization Unit — OU) для размещения учетных записей компьютеров, на которых установлен сервер авторизации vGate, и отключить для него автоматическую смену паролей. Для этого назначьте данному OU групповую политику, в которой в ветви "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options" присвойте параметру "Domain member: Disable machine account password changes" значение "Enabled" или параметру "Domain member: maximum machine account password age" — значение "999 days". Данное OU выбирается на определенном шаге установки сервера авторизации.

Перед конфигурированием локальной сети рекомендуется ознакомиться с документацией к продукту Microsoft Hyper-V.

Примеры виртуальной инфраструктуры и размещения компонентов vGate представлены на рисунках 1 и 2.

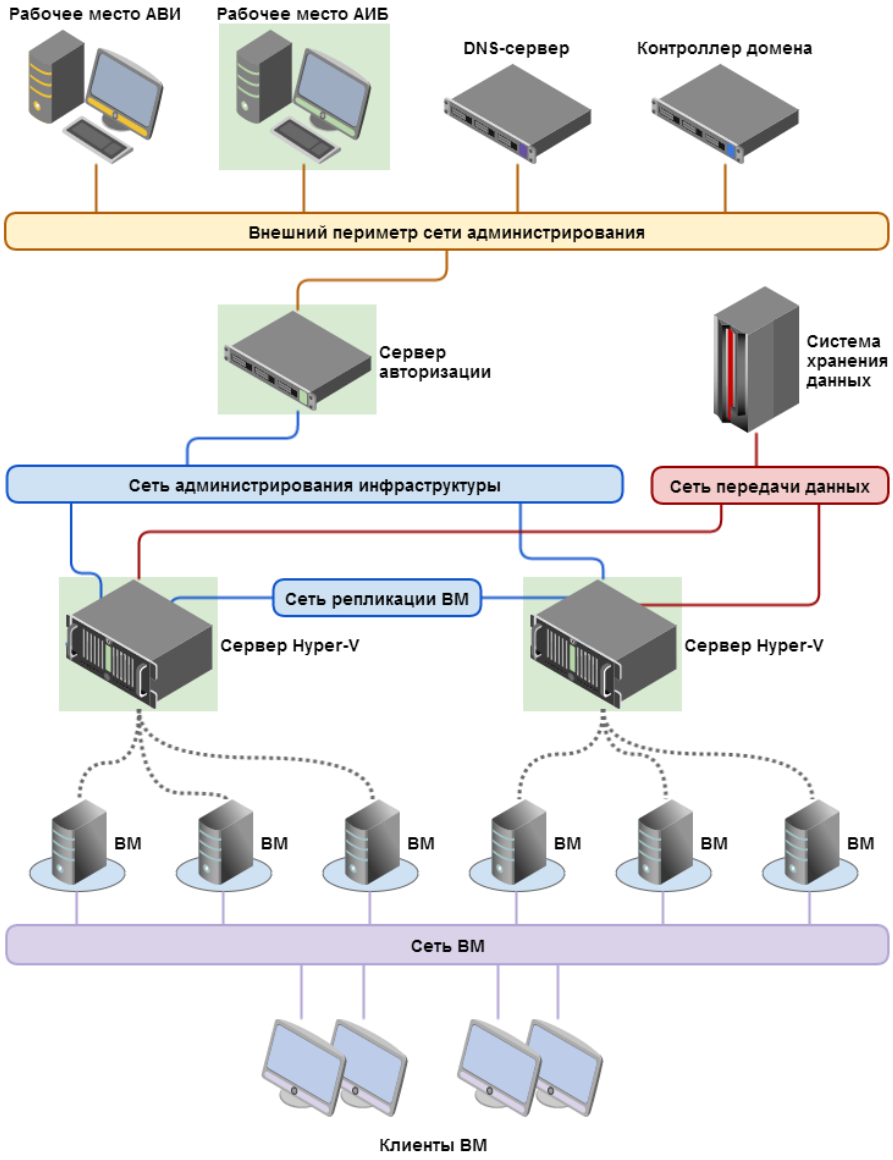


Рис.1 Архитектура сети и размещение компонентов (маршрутизацию трафика выполняет сервер авторизации vGate)

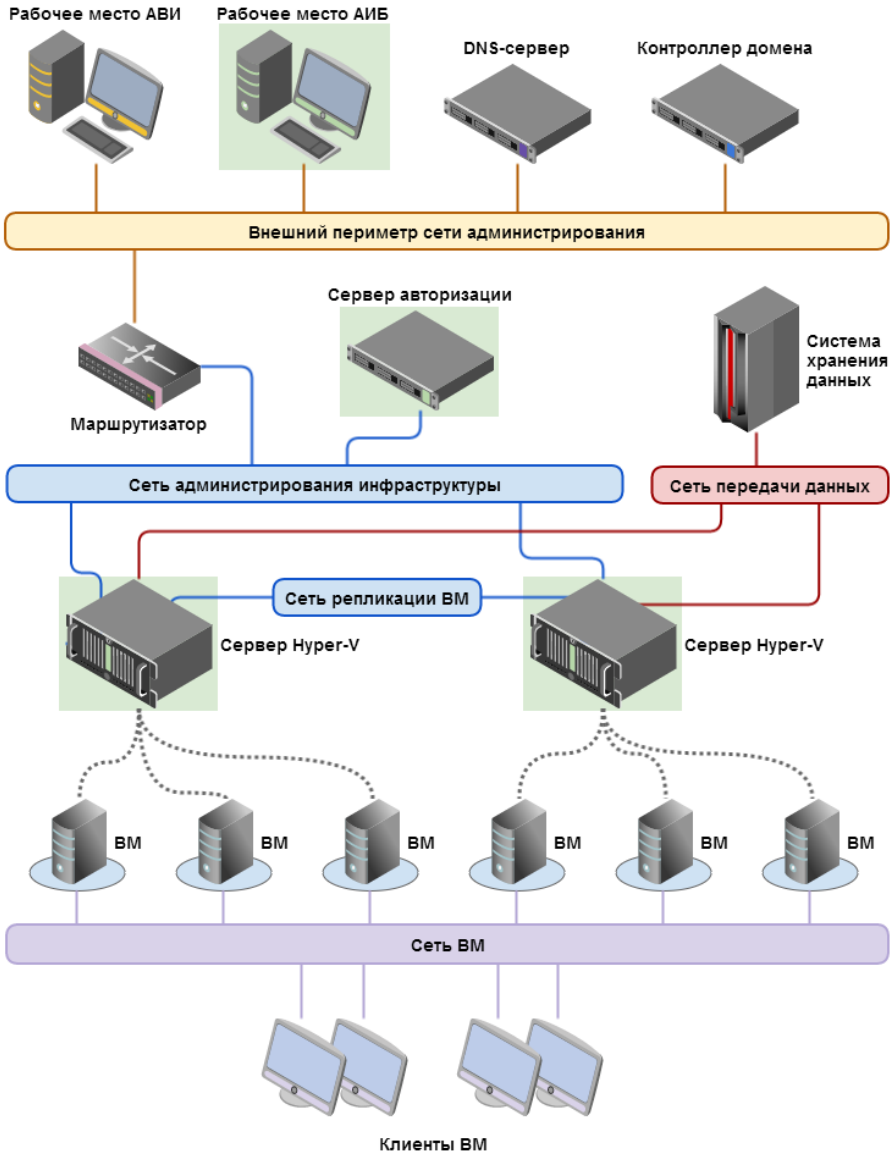


Рис.2 Архитектура сети и размещение компонентов (маршрутизация с помощью существующего маршрутизатора в сети)

Настройка маршрутизации между подсетями

Внимание! После конфигурирования локальной сети обязательно следует настроить маршрутизацию между подсетями, а также убедиться в наличии доступа с рабочих мест АВИ к элементам управления виртуальной инфраструктурой. Только после этого можно приступать к установке и настройке компонентов vGate.

В таблице приведены основные варианты настройки маршрутизации:

Вариант	Особенности настройки
Использование стороннего маршрутизатора	На рабочих местах АВИ в качестве шлюза по умолчанию нужно указать маршрутизатор, уже существующий во внешнем периметре сети администрирования предприятия. Также необходимо запретить прямое сетевое взаимодействие между рабочими местами АВИ и защищаемыми серверами
Использование сервера авторизации в качестве шлюза	На всех рабочих местах АВИ в качестве шлюза по умолчанию следует указать IP-адрес внешнего сетевого адаптера сервера авторизации. На всех компьютерах в защищаемом периметре сети администрирования инфраструктуры (серверы Hyper-V, SCVMM) в качестве шлюза по умолчанию следует указать IP-адрес адаптера защищаемого периметра сервера авторизации
Получение маршрута с сервера авторизации	На всех компьютерах защищаемого периметра сети администрирования (серверы Hyper-V, SCVMM) в качестве шлюза по умолчанию следует указать IP-адрес адаптера защищаемого периметра сервера авторизации. В консоли управления следует настроить получение маршрута к защищенной сети с сервера авторизации (см. стр.**76**). В этом случае на рабочих местах АВИ маршрут к защищенной сети добавляется с сервера авторизации в момент запуска службы аутентификации vGate, после чего маршрут записывается в локальную таблицу маршрутизации ПК

Если предполагается использование конфигурации с резервным сервером авторизации, то DNS-сервер рекомендуется разместить во внешней сети. Кроме того, в DNS необходимо настроить псевдоним (CNAME), указывающий на основной сервер. В этом случае при установке агентов аутентификации необходимо будет указывать псевдоним (CNAME) основного сервера.

Установка и настройка сервера авторизации

Установка и последующая работа сервера авторизации vGate различаются в зависимости от способа маршрутизации управляющего трафика между внешним и защищаемым периметрами сети администрирования:

- С помощью существующего маршрутизатора в сети (см. стр.**15**).

  В этом режиме сервер авторизации размещается в защищаемом периметре сети администрирования инфраструктуры, то есть в той же подсети, в которой размещены защищаемые серверы (см. Рис.2 на стр.**13**). Режим не требует реконфигурации существующей сети и предусматривает наличие во внешней сети администрирования сертифицированного межсетевого экрана (маршрутизатора), фильтрующего сетевой трафик к защищаемым серверам. На маршрутизаторе необходимо закрыть доступ с рабочих мест АВИ и АИБ в защищаемую подсеть или к серверам по отдельности и разрешить доступ к серверу авторизации. Подробнее о настройках маршрутизатора см.стр.**175**.

- С помощью сервера авторизации vGate (см. стр.**20**).

  При выборе этого способа защищаемые серверы должны быть расположены в отдельной подсети. На всех компьютерах защищаемого периметра сети администрирования (серверы Hyper-V и SCVMM) в качестве шлюза по умолчанию следует указать IP-адрес адаптера защищаемого периметра сервера авторизации. На всех рабочих местах АВИ в качестве шлюза по умолчанию

следует указать IP-адрес сетевого адаптера сервера авторизации во внешней сети администрирования.

При выборе данного режима не требуется дополнительная настройка маршрутизатора.

Внимание!

- Если предполагается использование Active Directory, необходимо ввести компьютер, предназначенный для сервера vGate, в домен.
- Если компьютер сервера авторизации был добавлен в домен после установки ПО vGate, необходимо добавить этот домен в список доверенных доменов в консоли управления vGate (см. стр.77).

Установка при использовании стороннего маршрутизатора

Подготовка компьютера:

Настройте на компьютере, предназначенном для сервера авторизации, одно соединение локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.2**

Для установки сервера авторизации:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков.

   Если программа установки не запустилась автоматически, запустите на исполнение файл autorun.exe, находящийся в папке \autorun.

   На экране появится стартовый диалог программы установки.
3. Активируйте ссылку "Сервер авторизации" в секции "Для защиты Microsoft Hyper-V" стартового диалога программы установки.

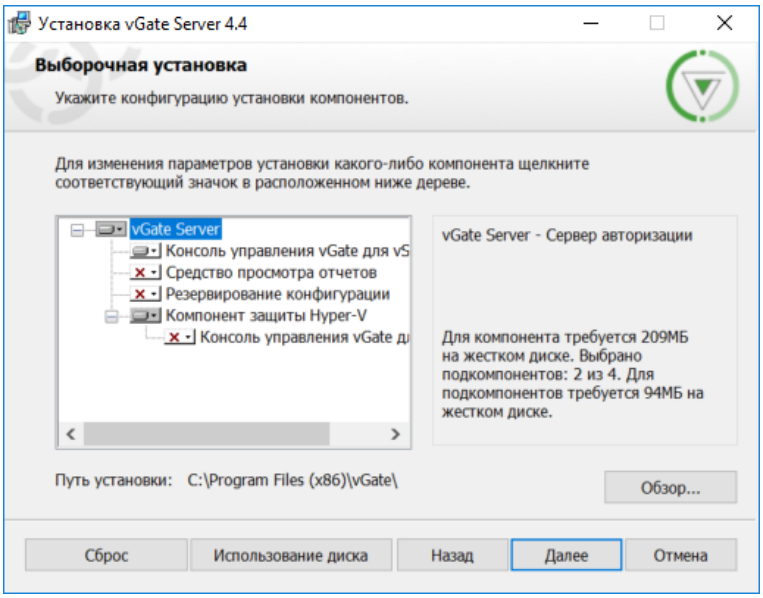
   Совет. Для установки этого продукта можно также запустить на исполнение файл \vGate\vGateServer.msi, находящийся на установочном диске.

   Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.
4. Нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

   Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора устанавливаемых компонентов.



6. Выберите компоненты, которые следует установить.

Пояснение.

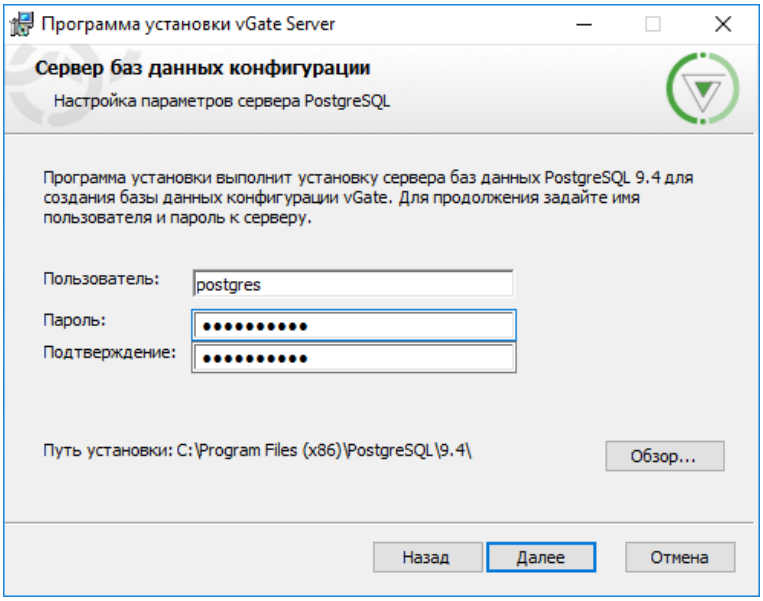
- Для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V установите "Компонент защиты Hyper-V". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Выберите для установки консоль управления vGate. Для этого раскройте пункт "Компонент защиты Hyper-V" и выберите компонент "Консоль управления vGate для Hyper-V".
- Компонент "Резервирование конфигурации" по умолчанию не устанавливается. Если предполагается использовать резервирование конфигурации (см. стр. 26), выберите этот компонент для установки. Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".

В диалоге также имеются следующие кнопки:

Кнопка	Действие
Обзор	Открывает диалог для изменения пути к каталогу установки
Использование диска	Открывает диалог с информацией о размере свободного места на дисках компьютера
Сброс	Возвращает состояние компонентов установки по умолчанию

7. Нажмите кнопку "Далее".

На экране появится следующий диалог.

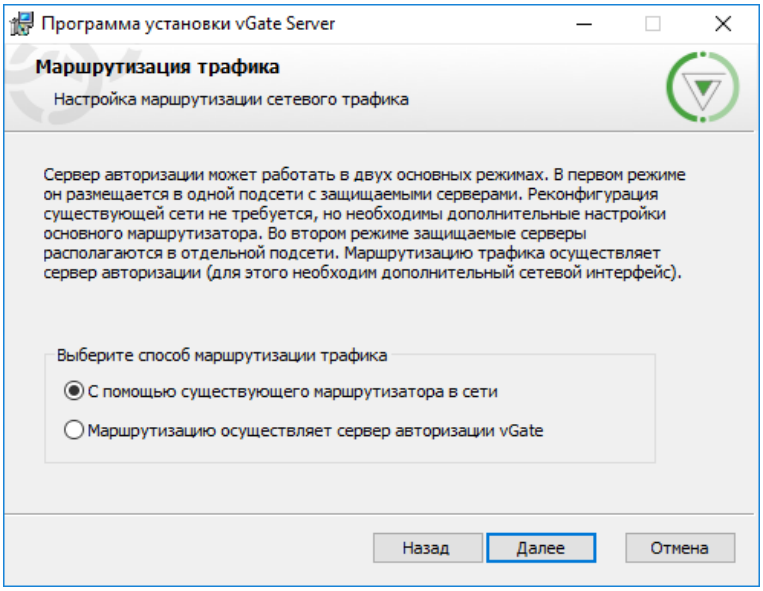


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

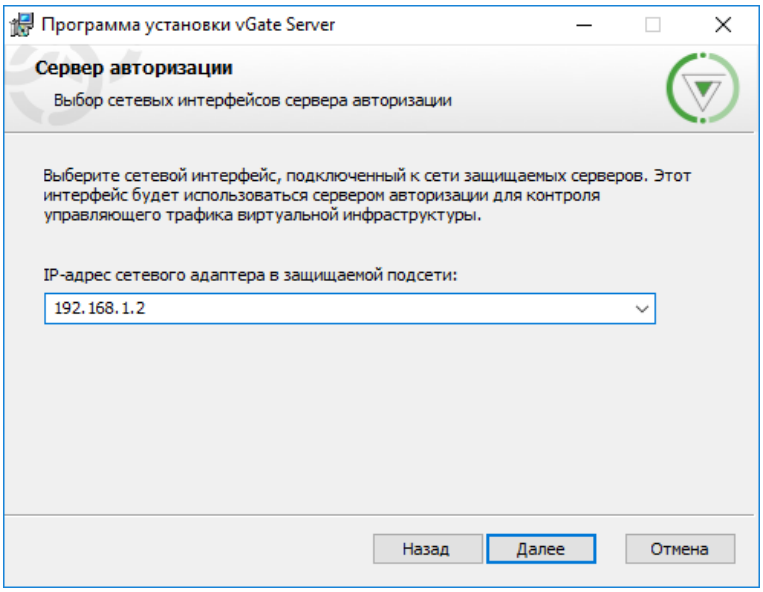
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для vGate версии 4.0 и выше по умолчанию используется порт базы данных PostgreSQL 5432. Значение данного порта можно изменить только при отдельной установке PostgreSQL (до установки ПО vGate). Порты базы данных PostgreSQL для основного и резервного серверов должны совпадать.

На экране появится следующий диалог.



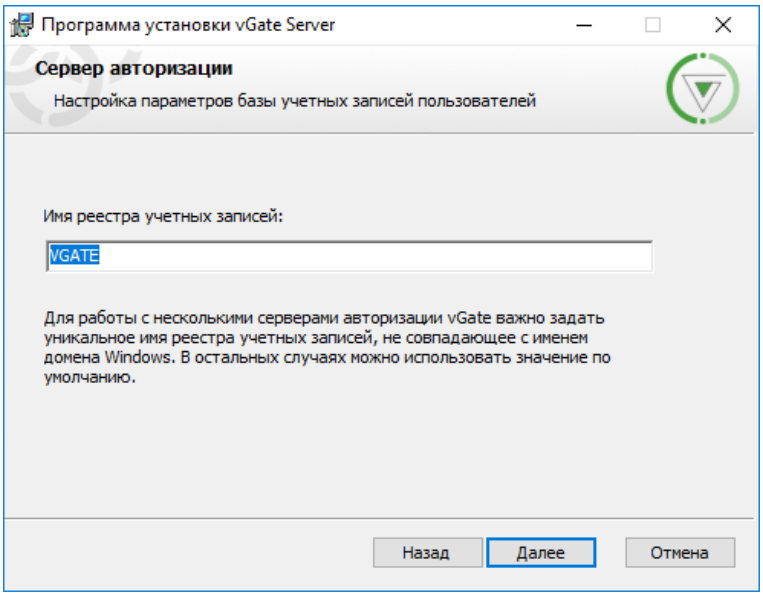
9. Выберите способ маршрутизации трафика "С помощью существующего маршрутизатора в сети" и нажмите кнопку "Далее".

На экране появится следующий диалог.



10. Укажите IP-адрес адаптера 1 сервера авторизации, через который будут проходить маршруты в защищаемый периметр сети администрирования инфраструктуры и из него, и нажмите кнопку "Далее".

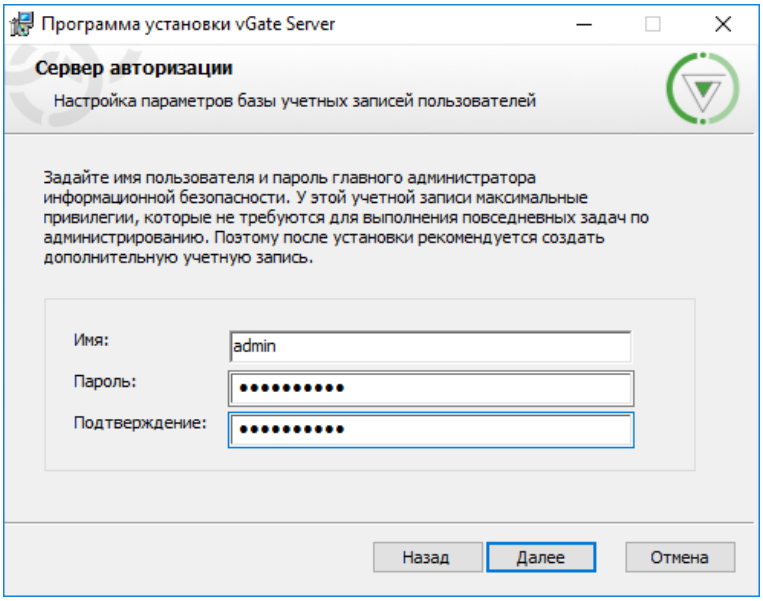
На экране появится следующий диалог.



Примечание. Если в сети планируется использовать несколько серверов авторизации, то при установке каждого сервера авторизации следует указывать уникальное имя реестра учетных записей vGate.

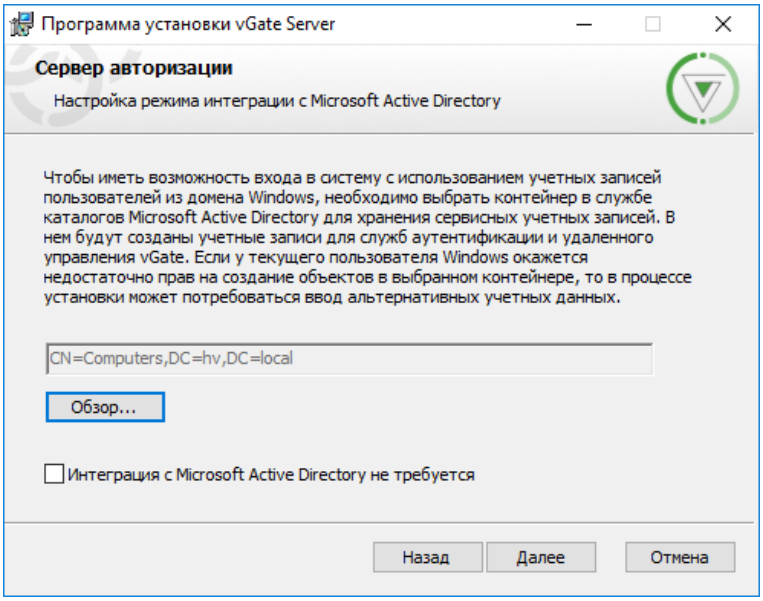
11. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

На экране появится следующий диалог.



12. Укажите учетные данные главного администратора информационной безопасности и нажмите кнопку "Далее".

Если учетная запись данного компьютера входит в домен Windows, на экране появится следующий диалог.



Примечание. Если используется учетная запись локального администратора, на экране появится сообщение об ошибке "Не удалось подключиться к службе каталогов". Поле выбора контейнера для учетных записей vGate будет пустым, а кнопка "Обзор" недоступна.

13. Укажите организационное подразделение (OU), созданное при конфигурировании локальной сети (см. стр.**11**) для хранения служебных учетных записей vGate, и нажмите кнопку "Далее".

Совет. Отметьте пункт "Интеграция с Microsoft Active Directory не требуется", если не планируется аутентификация в vGate с указанием учетных данных пользователей из домена Windows.

Примечание. Если учетная запись администратора не обладает правами группы Account Operators, то в процессе установки будет предложено ввести данные учетной записи, обладающей такими правами. В противном случае установка будет прекращена.

На экране появится диалог с сообщением о готовности к установке.

14. Нажмите кнопку "Установить".

Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

15. Нажмите кнопку "Готово".

> **Примечание.** В некоторых случаях на экране может появиться сообщение о необходимости перезагрузить компьютер. Выполните перезагрузку, нажав кнопку "Да" в окне сообщения.

Установка для работы без отдельного маршрутизатора

Подготовка компьютера:

Настройте на компьютере, предназначенном для сервера авторизации, два соединения локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес из диапазона адресов защищаемого периметра, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.2**
Адаптер 2	Сеть внешнего периметра администрирования	IP-адрес из диапазона адресов внешней сети, используемый для соединения с рабочими местами АВИ и АИБ. В примерах используется IP-адрес **192.168.2.3**

Для установки сервера авторизации:

1. Войдите в систему с правами администратора компьютера.

2. Поместите установочный диск в устройство чтения компакт-дисков.

> Если программа установки не запустилась автоматически, запустите на исполнение файл autorun.exe, находящийся в папке \autorun.

На экране появится стартовый диалог программы установки.

3. Активируйте ссылку "Сервер авторизации" в секции "Для защиты Microsoft Hyper-V" стартового диалога программы установки.

> **Совет.** Для установки этого продукта можно также запустить на исполнение файл \vGate\vGateServer.msi, находящийся на установочном диске.

Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.

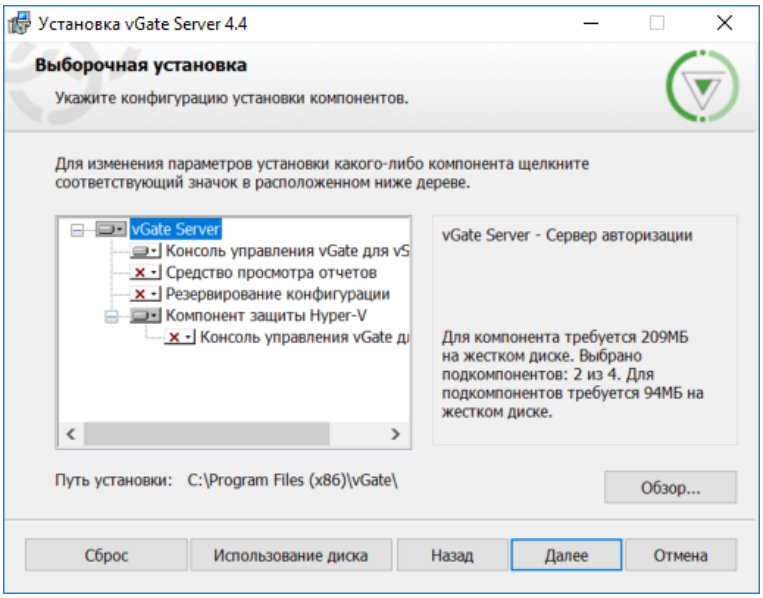
4. Нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

> **Совет.** Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора устанавливаемых компонентов.



6. Выберите компоненты, которые следует установить.

Пояснение.

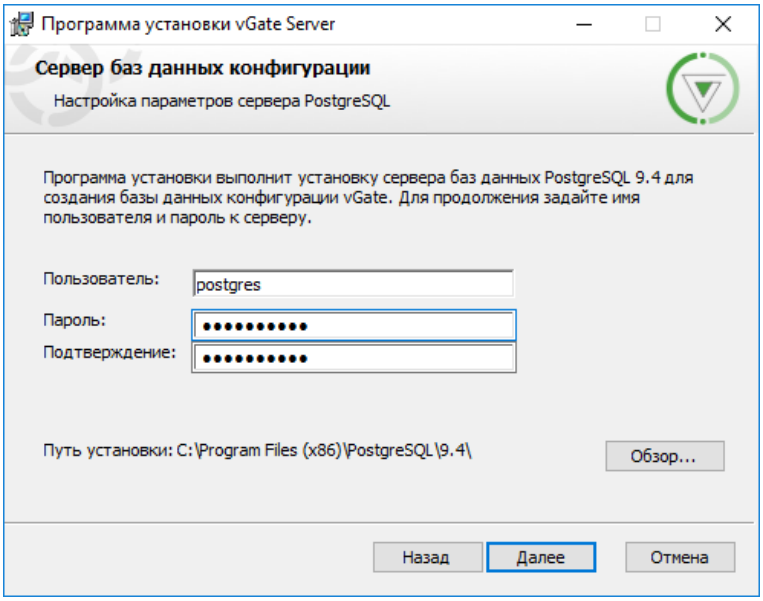
- Для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V установите "Компонент защиты Hyper-V". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Выберите для установки консоль управления vGate. Для этого раскройте пункт "Компонент защиты Hyper-V" и выберите компонент "Консоль управления vGate для Hyper-V".
- Компонент "Резервирование конфигурации" по умолчанию не устанавливается. Если предполагается использовать резервирование конфигурации (см. стр. 26), выберите этот компонент для установки. Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".

В диалоге также имеются следующие кнопки:

Кнопка	Действие
Обзор	Открывает диалог для изменения пути к каталогу установки
Использование диска	Открывает диалог с информацией о размере свободного места на дисках компьютера
Сброс	Возвращает состояние компонентов установки по умолчанию

7. Нажмите кнопку "Далее".

На экране появится следующий диалог.

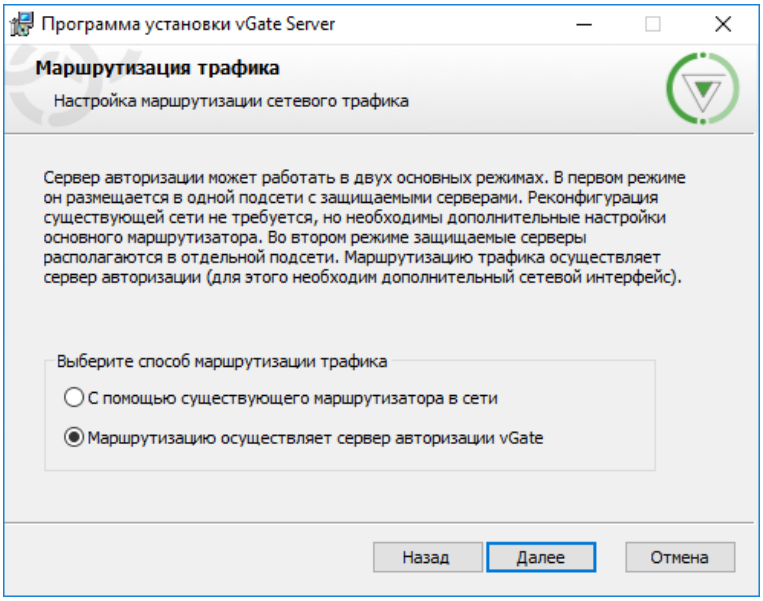


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

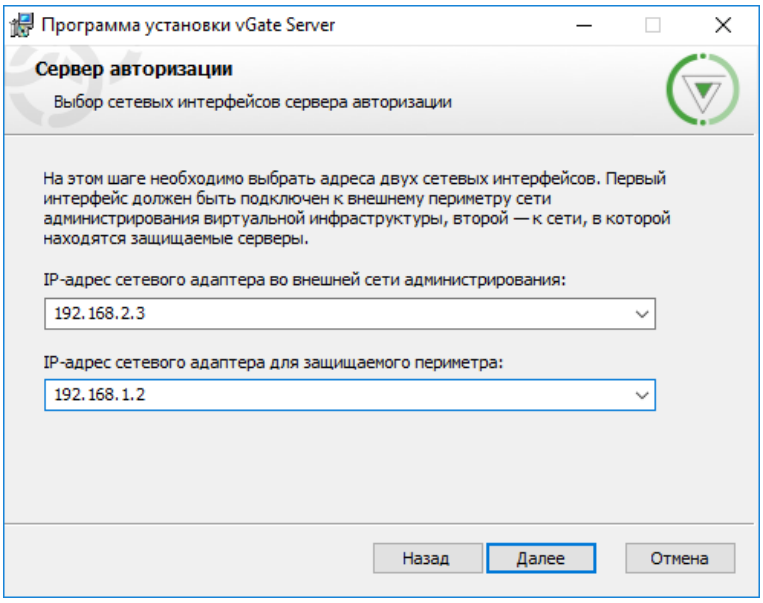
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для vGate версии 4.0 и выше по умолчанию используется порт базы данных PostgreSQL 5432. Значение данного порта можно изменить только при отдельной установке PostgreSQL (до установки ПО vGate). Порты базы данных PostgreSQL для основного и резервного серверов должны совпадать.

На экране появится следующий диалог.



9. Выберите способ маршрутизации трафика "Маршрутизацию осуществляет сервер авторизации vGate" и нажмите кнопку "Далее".

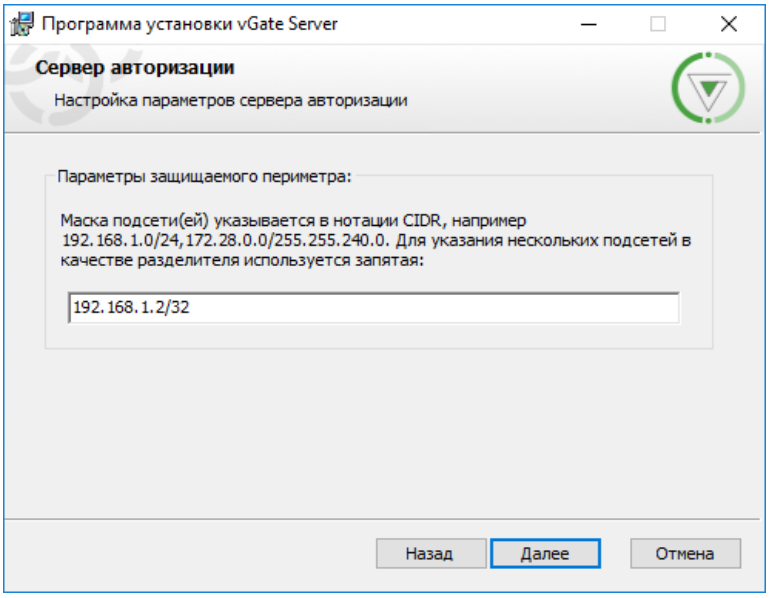
На экране появится следующий диалог.



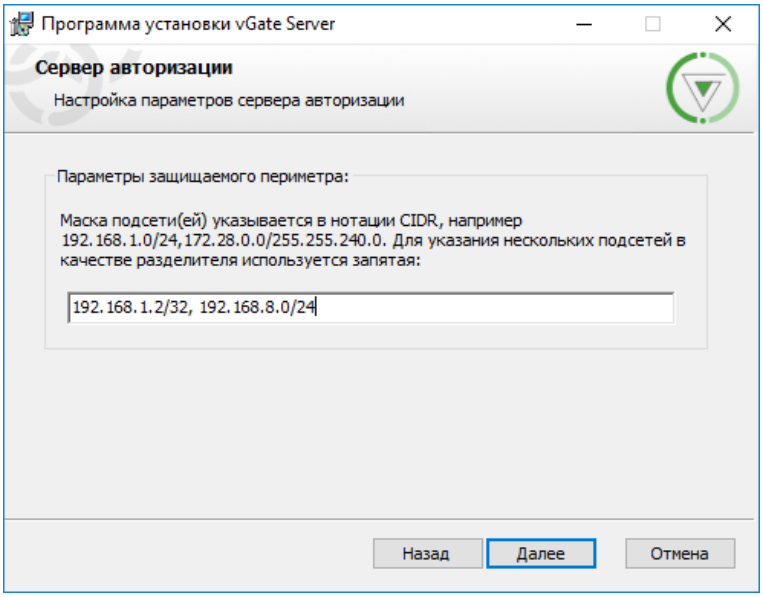
10. Укажите сетевые параметры сервера авторизации и нажмите кнопку "Далее".

Параметр	Описание
IP-адрес сетевого адаптера во внешней сети администрирования	IP-адрес сервера во внешнем периметре сети администрирования инфраструктуры (подсети, в которой размещены рабочие места АИБ и АВИ)
IP-адрес сетевого адаптера для защищаемого периметра	IP-адрес сервера в защищаемом периметре сети администрирования инфраструктуры (подсети, в которой размещены защищаемые серверы виртуальной инфраструктуры)

На экране появится следующий диалог.



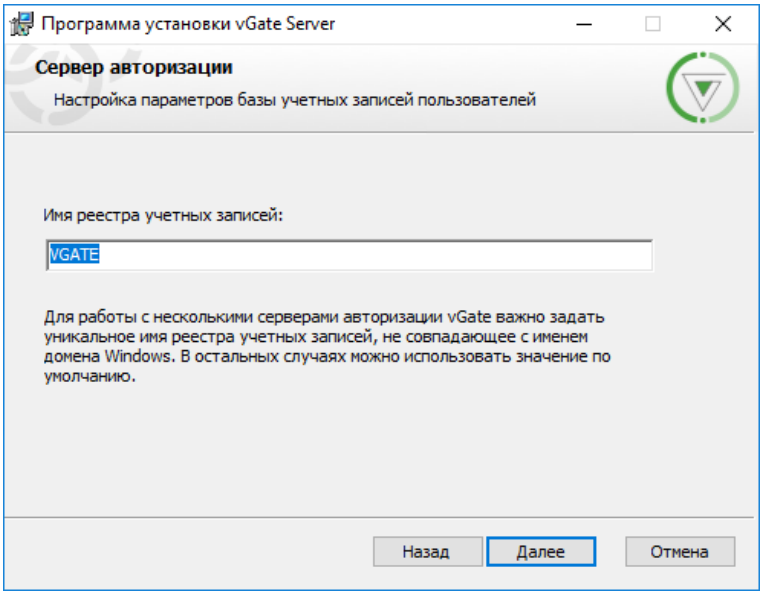
11. Если защищаемый периметр сети администрирования состоит из нескольких сетей, укажите их IP-адреса в текстовом поле, используя запятую в качестве разделителя.



Таким образом, передача данных внутрь защищаемого периметра будет разрешена только в том случае, если IP-адрес назначения соответствует одной из указанных подсетей.

12. Проверьте корректность IP-адресов подсетей, в которых размещаются защищаемые серверы Hyper-V, и нажмите кнопку "Далее".

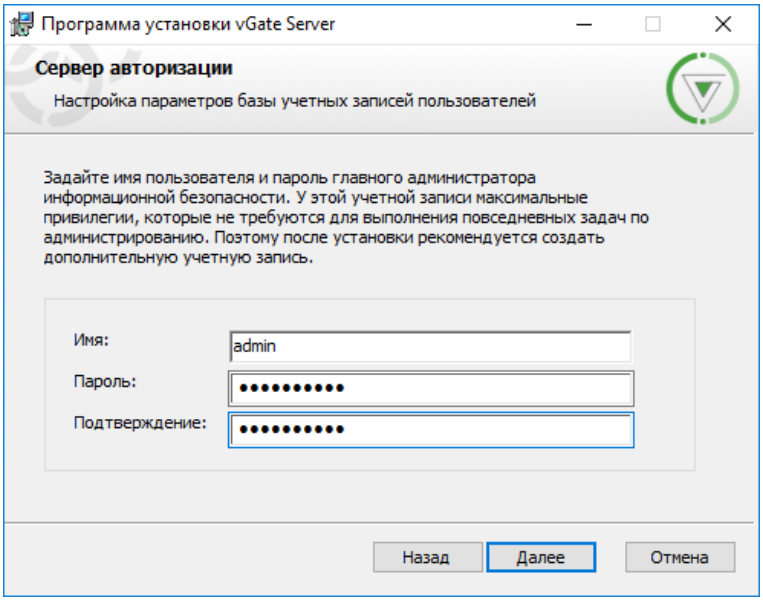
На экране появится следующий диалог.



Примечание. Если в сети планируется использовать несколько серверов авторизации, то при установке каждого сервера авторизации следует указывать уникальное имя реестра учетных записей vGate.

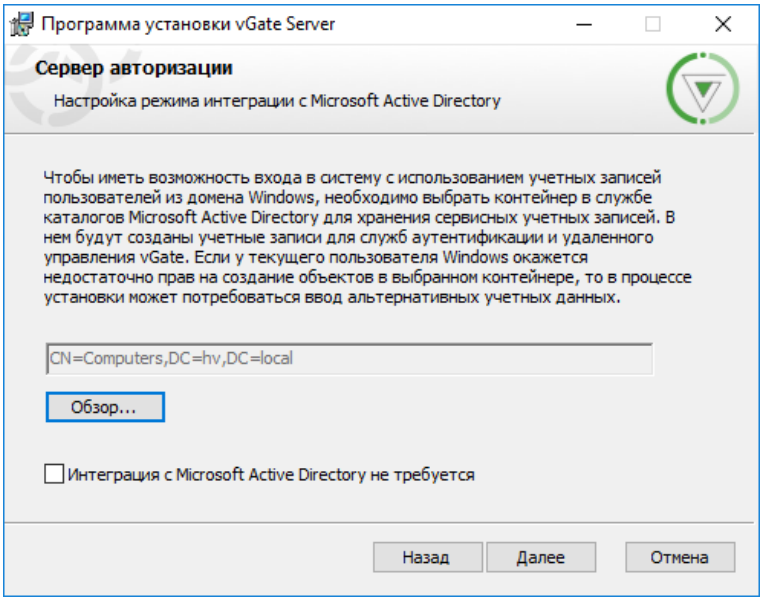
13. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

На экране появится следующий диалог.



14. Укажите учетные данные главного администратора информационной безопасности и нажмите кнопку "Далее".

Если учетная запись данного компьютера входит в домен Windows, на экране появится следующий диалог.



Примечание. Если используется учетная запись локального администратора, на экране появится сообщение об ошибке "Не удалось подключиться к службе каталогов". Поле выбора контейнера для учетных записей vGate будет пустым, а кнопка "Обзор" недоступна.

15. Укажите организационное подразделение (OU), созданное при конфигурировании локальной сети (см. стр.**11**) для хранения служебных учетных записей vGate, и нажмите кнопку "Далее".

Совет. Отметьте пункт "Интеграция с Microsoft Active Directory не требуется", если не планируется аутентификация в vGate с указанием учетных данных пользователей из домена Windows.

Примечание. Если учетная запись администратора не обладает правами группы Account Operators, то в процессе установки будет предложено ввести данные учетной записи, обладающей такими правами. В противном случае установка будет прекращена.

На экране появится диалог с сообщением о готовности к установке.

16. Нажмите кнопку "Установить".

    Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

    После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

17. Нажмите кнопку "Готово".

> **Примечание.** В некоторых случаях на экране может появиться сообщение о необходимости перезагрузить компьютер. Выполните перезагрузку, нажав кнопку "Да" в окне сообщения.

Установка и настройка сервера авторизации с резервированием

Функция резервирования сервера авторизации доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

vGate предоставляет возможность резервирования сервера авторизации. Для этого необходимо произвести установку двух серверов авторизации — основного и резервного — и настроить репликацию данных между ними. В случае сбоя основного сервера управление может быть переведено на резервный сервер авторизации вручную или автоматически (если настроена функция горячего резервирования, см. стр.**69**).

> **Внимание!** До установки ПО резервного сервера авторизации vGate необходимо зарегистрировать лицензию для демонстрационной версии vGate, лицензию на использование vGate Enterprise или Enterprise Plus в консоли управления vGate R2 на основном сервере авторизации.

Установка и последующая работа сервера авторизации vGate с резервированием возможна в двух режимах в зависимости от способа маршрутизации трафика между внешним и защищаемым периметрами сети администрирования:

- С помощью существующего маршрутизатора в сети (см. стр.**27**).

  В этом режиме сервер авторизации размещается в защищаемом периметре сети администрирования инфраструктуры, то есть в той же подсети, в которой размещены защищаемые серверы (см. Рис.2 на стр.**13**). Режим не требует реконфигурации существующей сети и предусматривает наличие во внешней сети администрирования сертифицированного межсетевого экрана (маршрутизатора), фильтрующего сетевой трафик к защищаемым серверам. На маршрутизаторе необходимо закрыть доступ с рабочих мест АВИ и АИБ в защищаемую подсеть или к серверам по отдельности и разрешить доступ к серверу авторизации. Подробнее о настройках маршрутизатора см.стр.**175**.

- С помощью сервера авторизации vGate (см. стр.**36**).

  При выборе этого способа защищаемые серверы должны быть расположены в отдельной подсети. На всех компьютерах защищаемого периметра сети администрирования (серверы Hyper-V и SCVMM) в качестве шлюза по умолчанию следует указать IP-адрес адаптера защищаемого периметра сервера авторизации. На всех рабочих местах АВИ в качестве шлюза по умолчанию следует указать IP-адрес сетевого адаптера сервера авторизации во внешней сети администрирования.

  При выборе данного режима не требуется дополнительная настройка маршрутизатора.

> **Внимание!**
> - Если предполагается использование Active Directory, необходимо ввести компьютеры, предназначенные для основного и резервного серверов авторизации vGate, в один домен.
> - Если компьютер сервера авторизации был добавлен в домен после установки ПО vGate, необходимо добавить этот домен в список доверенных доменов в консоли управления vGate (см. стр.**77**).

Установка при использовании стороннего маршрутизатора

Подготовка компьютеров:

Настройте на компьютере, предназначенном для основного сервера авторизации, два соединения локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	• Основной IP-адрес, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.2**. • Дополнительный IP-адрес, используемый при сбое сервера. В примерах используется IP-адрес **192.168.1.12**
Адаптер 2	Сеть резервирования	IP-адрес из диапазона адресов сети резервирования, по которому будет осуществляться репликация данных между основным и резервным серверами авторизации. В примерах используется IP-адрес **192.168.3.2**

Примечание. IP-адрес для резервирования не должен принадлежать сети администрирования инфраструктуры.

Настройте на компьютере, предназначенном для резервного сервера авторизации, два соединения локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.22**
Адаптер 2	Сеть резервирования	IP-адрес из диапазона адресов сети резервирования, используемый для соединения с основным сервером авторизации. В примерах используется IP-адрес **192.168.3.22**

Примечание. IP-адрес для резервирования не должен принадлежать сети администрирования инфраструктуры.

Для установки основного сервера авторизации:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков.

   Если программа установки не запустилась автоматически, запустите на исполнение файл autorun.exe, находящийся в папке \autorun.

   На экране появится стартовый диалог программы установки.
3. Активируйте ссылку "Сервер авторизации" в секции "Для защиты Microsoft Hyper-V" стартового диалога программы установки.

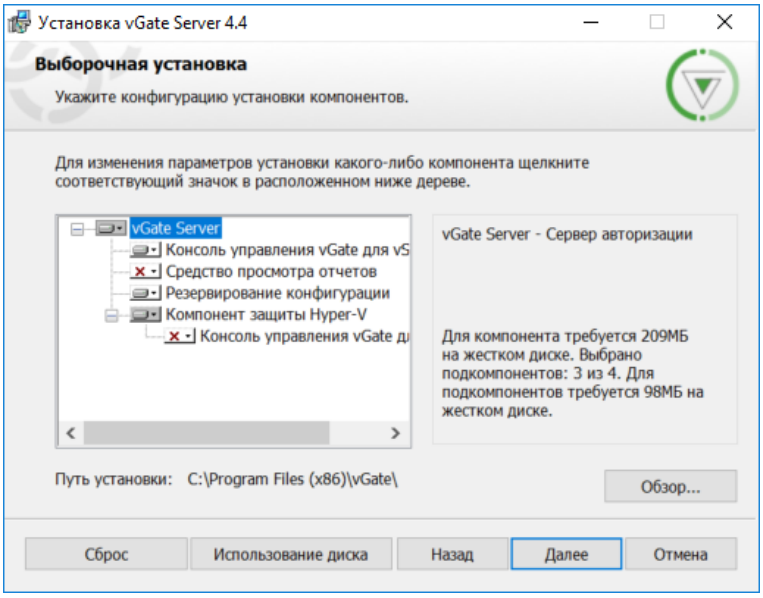
   Совет. Для установки этого продукта можно также запустить на исполнение файл \vGate\vGateServer.msi, находящийся на установочном диске.

   Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.
4. Нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

   Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

   На экране появится диалог для выбора устанавливаемых компонентов.



6. Выберите компоненты, которые следует установить.

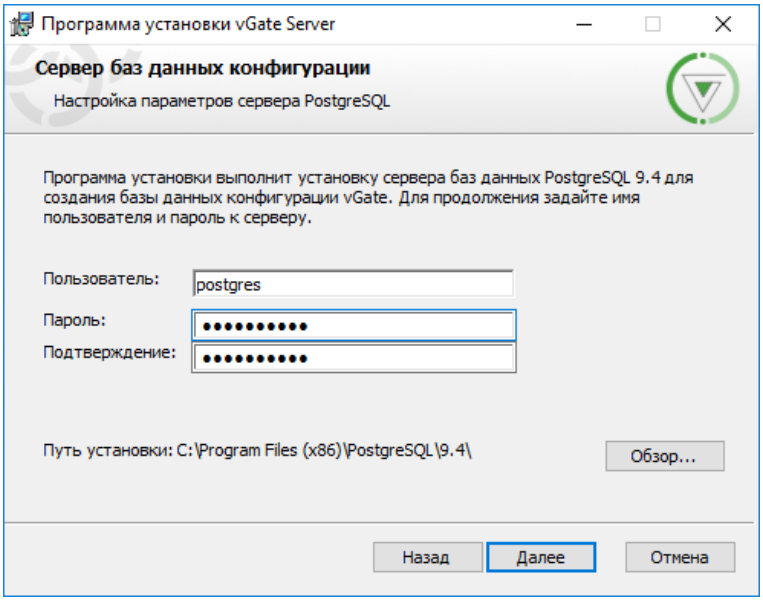
   Пояснение.
   - Для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V установите "Компонент защиты Hyper-V". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
   - Выберите для установки консоль управления vGate. Для этого раскройте пункт "Компонент защиты Hyper-V" и выберите компонент "Консоль управления vGate для Hyper-V".
   - Выберите для установки компонент "Резервирование конфигурации".

В диалоге также имеются следующие кнопки:

Кнопка	Действие
Обзор	Открывает диалог для изменения пути к каталогу установки
Использование диска	Открывает диалог с информацией о размере свободного места на дисках компьютера
Сброс	Возвращает состояние компонентов установки по умолчанию

7. Нажмите кнопку "Далее".

На экране появится следующий диалог.

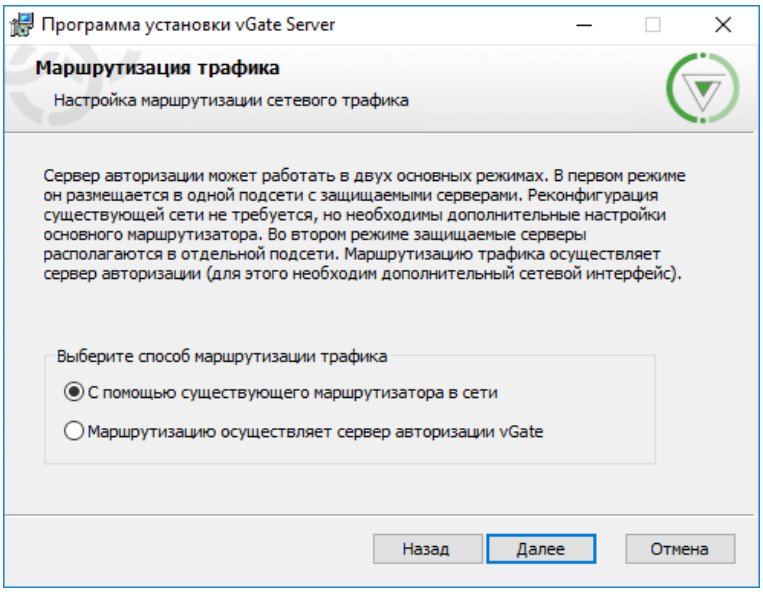


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

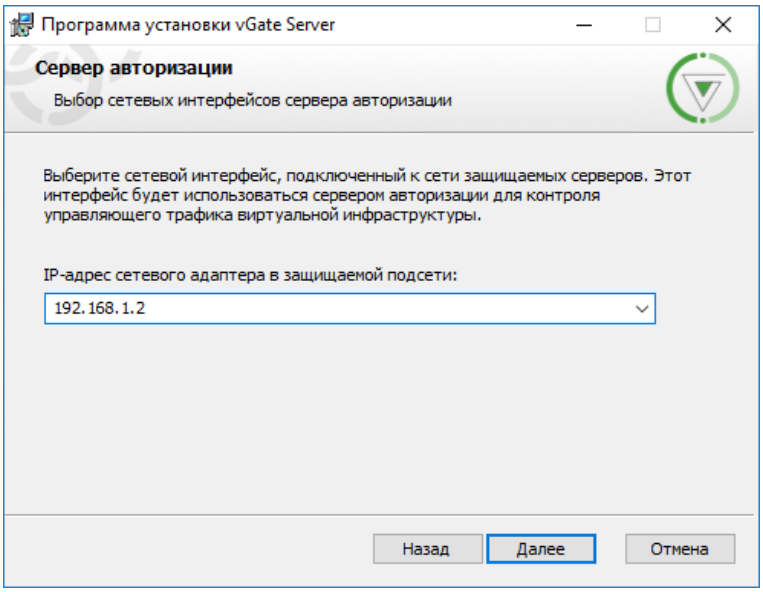
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для vGate версии 4.0 и выше по умолчанию используется порт базы данных PostgreSQL 5432. Значение данного порта можно изменить только при отдельной установке PostgreSQL (до установки ПО vGate). Порты базы данных PostgreSQL для основного и резервного серверов должны совпадать.

На экране появится следующий диалог.



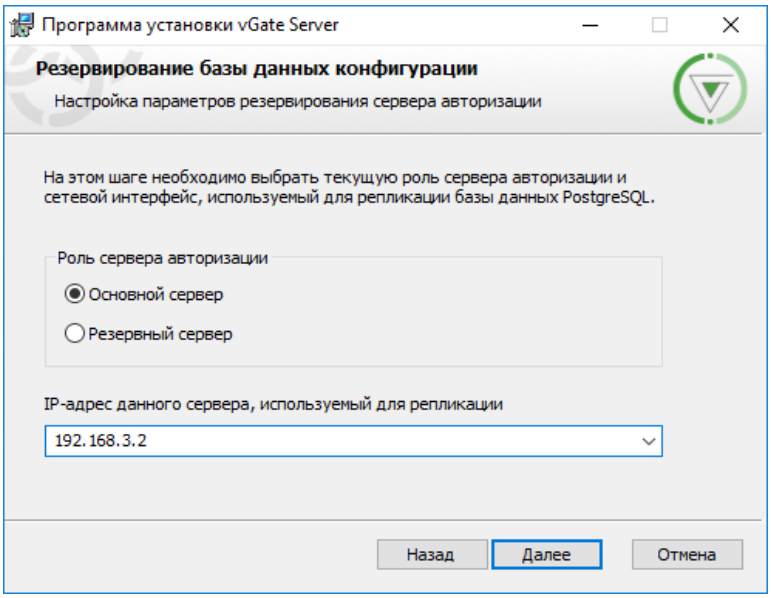
9. Выберите способ маршрутизации трафика "С помощью существующего маршрутизатора в сети" и нажмите кнопку "Далее".

На экране появится следующий диалог.



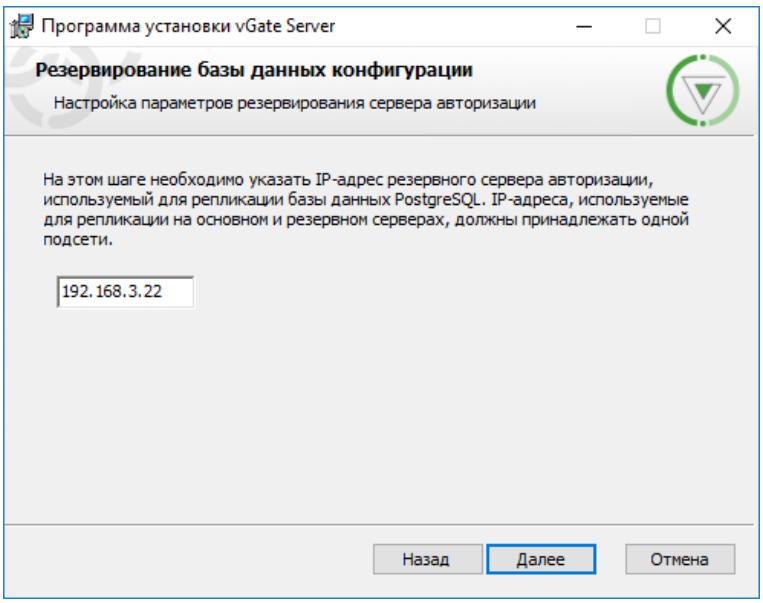
10. Укажите IP-адрес адаптера 1 сервера авторизации, через который будут проходить маршруты в защищаемый периметр сети администрирования инфраструктуры и из него, и нажмите кнопку "Далее".

Так как для установки был выбран компонент "Резервирование конфигурации", на экране появится диалог настройки параметров репликации.



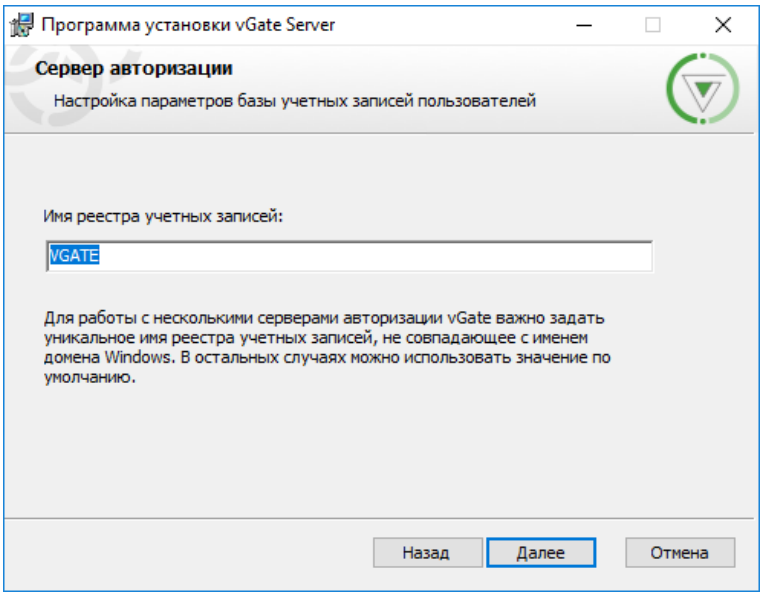
11. Выберите роль сервера авторизации "Основной сервер", укажите IP-адрес этого сервера, используемый для репликации данных между основным и резервным серверами авторизации в сети резервирования, и нажмите кнопку "Далее".

На экране появится диалог настройки параметров резервного сервера.



12. Укажите IP-адрес резервного сервера авторизации в сети резервирования, используемый для репликации, и нажмите кнопку "Далее".

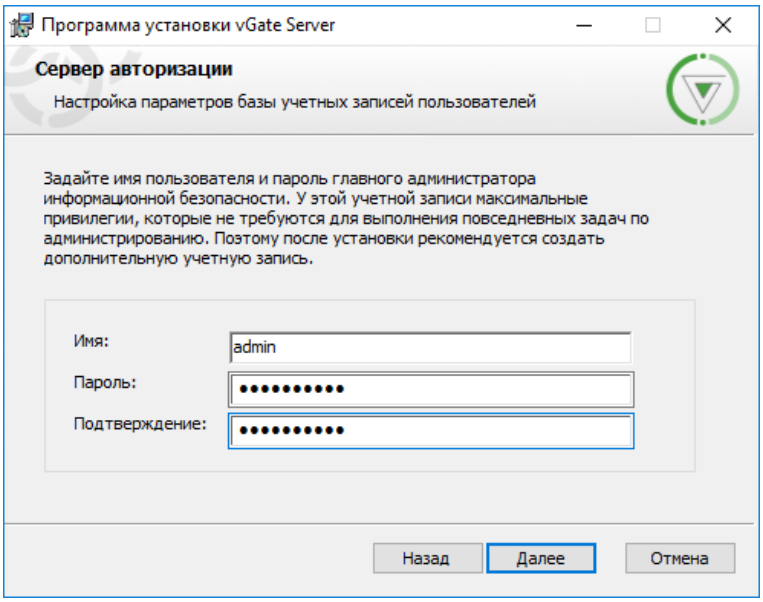
На экране появится следующий диалог.



Примечание. Если в сети планируется использовать несколько серверов авторизации, то при установке каждого сервера авторизации следует указывать уникальное имя реестра учетных записей vGate.

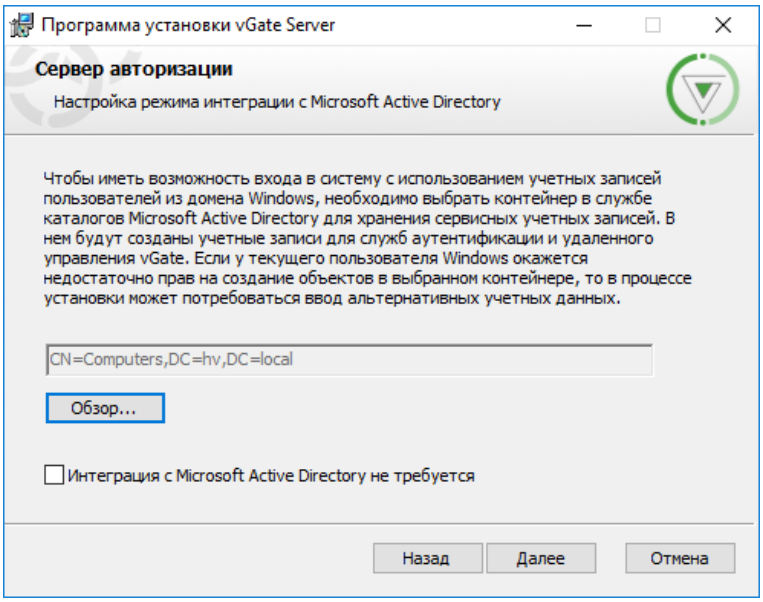
13. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

На экране появится следующий диалог.



14. Укажите учетные данные главного администратора информационной безопасности и нажмите кнопку "Далее".

    Если учетная запись данного компьютера входит в домен Windows, на экране появится следующий диалог.



> **Примечание.** Если используется учетная запись локального администратора, на экране появится сообщение об ошибке "Не удалось подключиться к службе каталогов". Поле выбора контейнера для учетных записей vGate будет пустым, а кнопка "Обзор" недоступна.

15. Укажите организационное подразделение (OU), созданное при конфигурировании локальной сети (см. стр.**11**) для хранения служебных учетных записей vGate, и нажмите кнопку "Далее".

> **Совет.** Отметьте пункт "Интеграция с Microsoft Active Directory не требуется", если не планируется аутентификация в vGate с указанием учетных данных пользователей из домена Windows.

> **Примечание.** Если учетная запись администратора не обладает правами группы Account Operators, то в процессе установки будет предложено ввести данные учетной записи, обладающей такими правами. В противном случае установка будет прекращена.

    На экране появится диалог с сообщением о готовности к установке.

16. Нажмите кнопку "Установить".

    Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

    После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

17. Нажмите кнопку "Готово".

> **Примечание.** В некоторых случаях на экране может появиться сообщение о необходимости перезагрузить компьютер. Выполните перезагрузку, нажав кнопку "Да" в окне сообщения.

Для установки резервного сервера авторизации:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков.

> Если программа установки не запустилась автоматически, запустите на исполнение файл autorun.exe, находящийся в папке \autorun.

    На экране появится стартовый диалог программы установки.

3. В стартовом диалоге программы установки активируйте ссылку "Сервер авторизации".

> **Совет.** Для выполнения установки этого продукта можно также запустить на исполнение файл \vGate\vGateServer.msi, находящийся на установочном диске.

Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.

4. Нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

> **Совет.** Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора устанавливаемых компонентов.

6. Нажмите мышью на значок слева от названия компонента "Резервирование конфигурации" и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск". Нажмите кнопку "Далее".

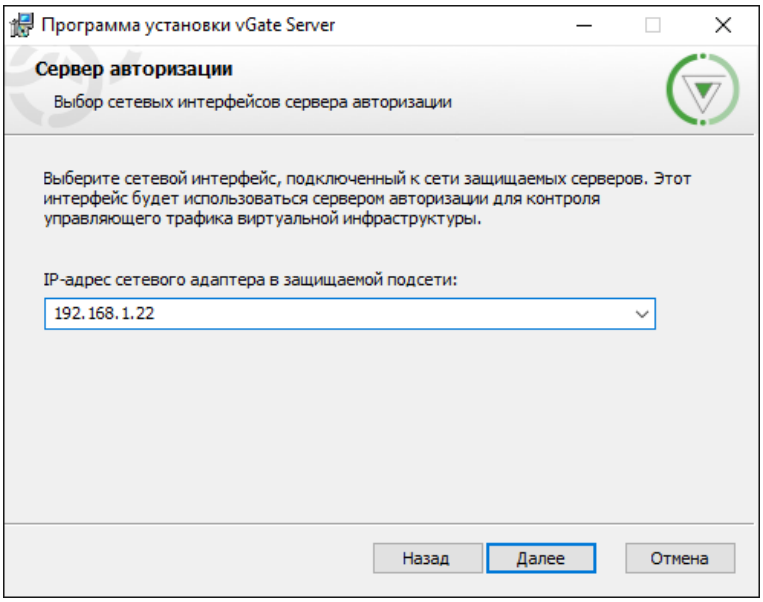
На экране появится диалог установки сервера баз данных PostgreSQL.

7. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее".

На экране появится диалог выбора способа маршрутизации трафика.

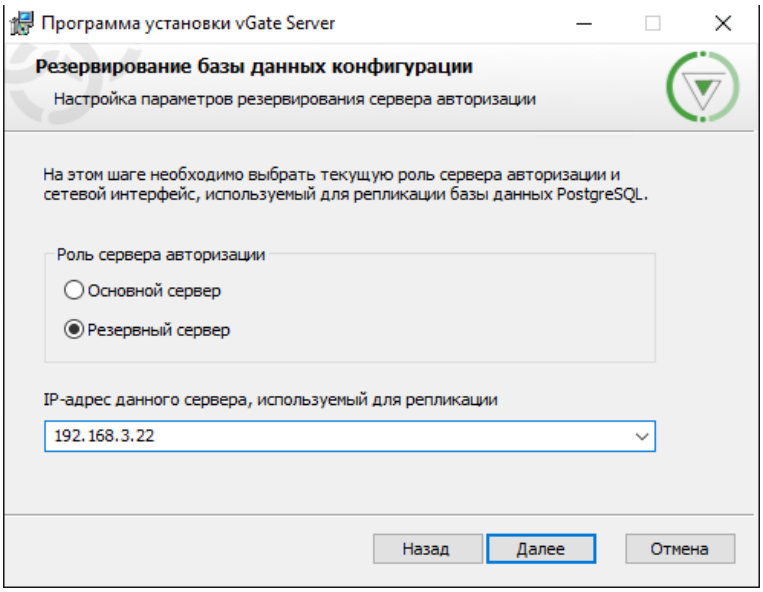
8. Выберите способ маршрутизации трафика "С помощью основного маршрутизатора" и нажмите кнопку "Далее".

На экране появится диалог настройки сетевых параметров.



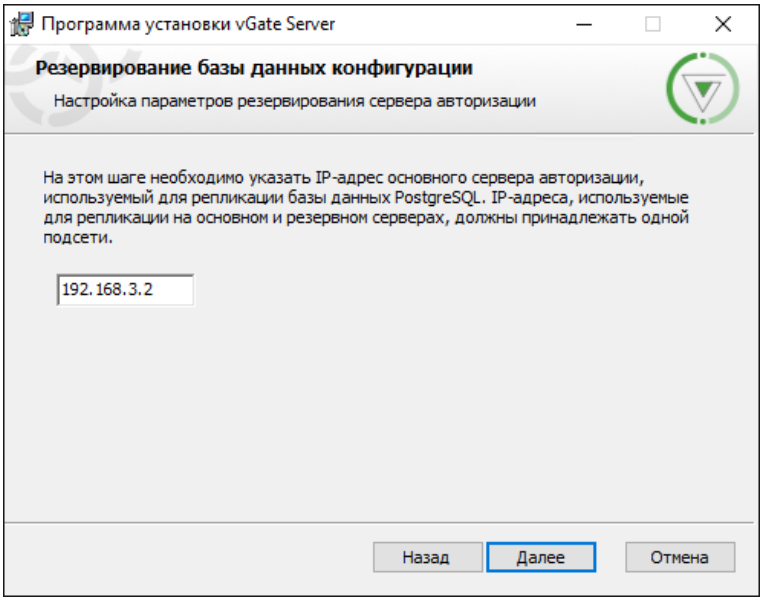
9. Укажите IP-адрес сетевого адаптера резервного сервера авторизации и нажмите кнопку "Далее".

   На экране появится диалог настройки параметров репликации.



10. Выберите роль сервера авторизации "Резервный сервер", укажите IP-адрес этого сервера, используемый для репликации данных между основным и резервным серверами авторизации в сети резервирования, и нажмите кнопку "Далее".

    На экране появится диалог настройки параметров основного сервера.



11. Укажите IP-адрес основного сервера авторизации в сети резервирования, используемый для репликации, и нажмите кнопку "Далее".

    На экране появится диалог с сообщением о готовности к установке.

12. Нажмите кнопку "Установить".

    Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

    После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

13. Нажмите кнопку "Готово".

> **Примечание.** В некоторых случаях на экране может появиться сообщение о необходимости перезагрузить компьютер. Выполните перезагрузку, нажав кнопку "Да" в окне сообщения.

О настройке репликации между основным и резервным серверами читайте на стр.**55**.

Установка для работы без отдельного маршрутизатора

Рассматривается установка сервера авторизации vGate с резервированием в режиме маршрутизации трафика через сервер авторизации.

Подготовка компьютеров:

Настройте на компьютере, предназначенном для основного сервера авторизации, три соединения локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	• Основной IP-адрес из диапазона адресов защищаемого периметра, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.2**. • Дополнительный IP-адрес, используемый при сбое сервера. В примерах используется IP-адрес **192.168.1.12**
Адаптер 2	Сеть внешнего периметра администрирования	IP-адрес из диапазона адресов внешней сети, используемый для соединения с рабочими местами АВИ и АИБ. В примерах используется IP-адрес **192.168.2.3**
Адаптер 3	Сеть резервирования	IP-адрес из диапазона адресов сети резервирования, по которому будет осуществляться репликация данных между основным и резервным серверами авторизации. В примерах используется IP-адрес **192.168.3.2**

> **Примечание.** IP-адрес для резервирования не должен принадлежать сети администрирования инфраструктуры.

Настройте на компьютере, предназначенном для резервного сервера авторизации, три соединения локальной сети.

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	IP-адрес из диапазона адресов защищаемого периметра, используемый серверами Hyper-V для конфигурации и аудита. В примерах используется IP-адрес **192.168.1.22**
Адаптер 2	Сеть внешнего периметра администрирования	IP-адрес из диапазона адресов внешней сети, используемый для связи с рабочими местами АВИ и АИБ. В примерах используется IP-адрес **192.168.2.4**
Адаптер 3	Сеть резервирования	IP-адрес из диапазона адресов сети резервирования, используемый для соединения с основным сервером авторизации. В примерах используется IP-адрес **192.168.3.22**

> **Примечание.** IP-адрес для резервирования не должен принадлежать сети администрирования инфраструктуры.

Для установки основного сервера авторизации:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков.

Если программа установки не запустилась автоматически, запустите на исполнение файл autorun.exe, находящийся в папке \autorun.

На экране появится стартовый диалог программы установки.

3. Активируйте ссылку "Сервер авторизации" в секции "Для защиты Microsoft Hyper-V" стартового диалога программы установки.

Совет. Для установки этого продукта можно также запустить на исполнение файл \vGate\vGateServer.msi, находящийся на установочном диске.

Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.

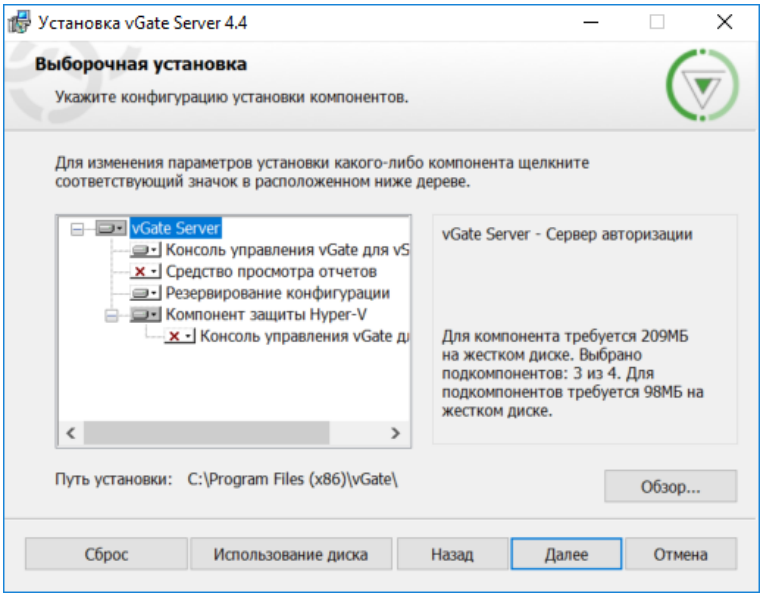
4. Нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора устанавливаемых компонентов.



6. Выберите компоненты, которые следует установить.

Пояснение.

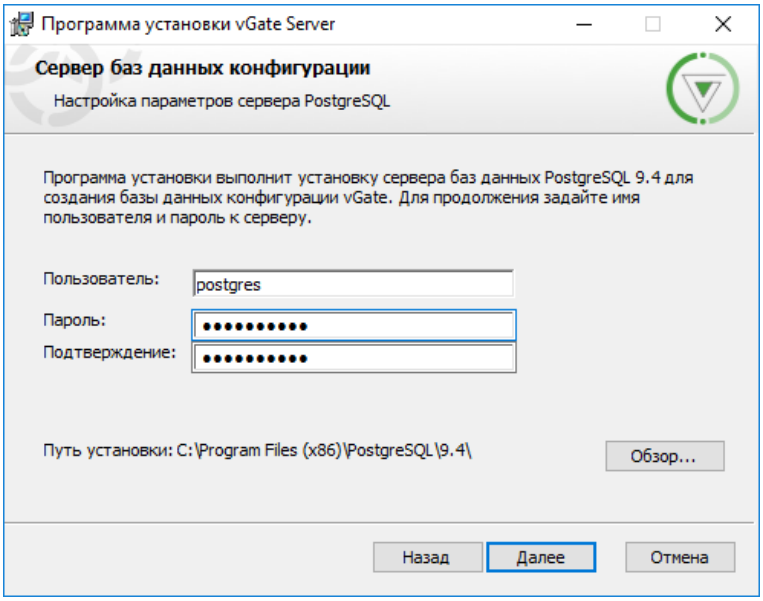
- Для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V установите "Компонент защиты Hyper-V". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Выберите для установки консоль управления vGate. Для этого раскройте пункт "Компонент защиты Hyper-V" и выберите компонент "Консоль управления vGate для Hyper-V".
- Выберите для установки компонент "Резервирование конфигурации".

В диалоге также имеются следующие кнопки:

Кнопка	Действие
Обзор	Открывает диалог для изменения пути к каталогу установки
Использование диска	Открывает диалог с информацией о размере свободного места на дисках компьютера
Сброс	Возвращает состояние компонентов установки по умолчанию

7. Нажмите кнопку "Далее".

На экране появится следующий диалог.

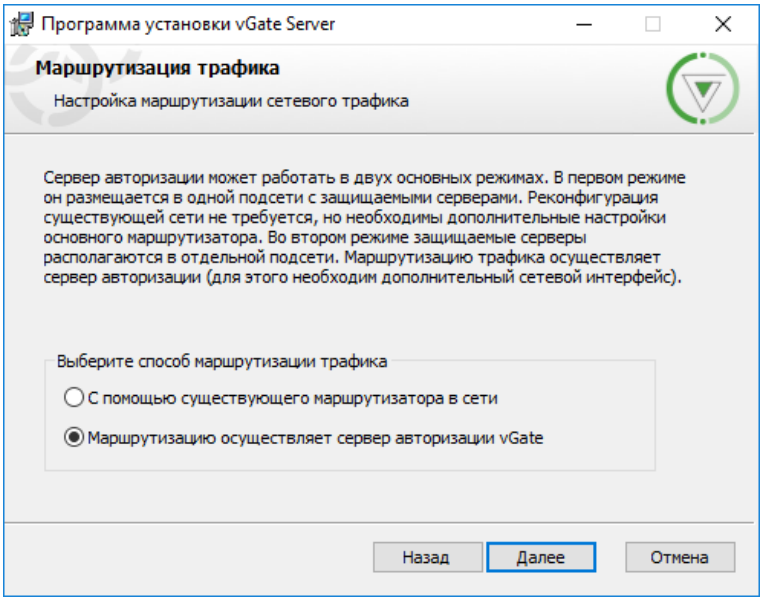


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

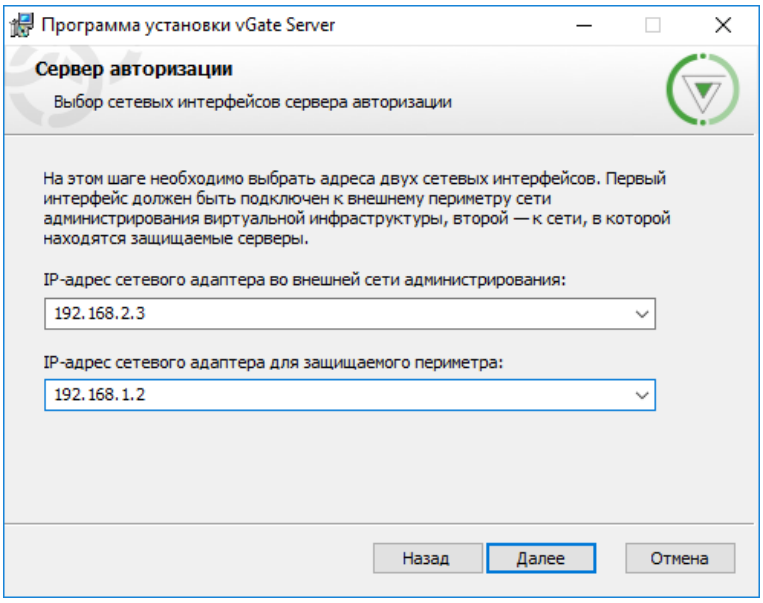
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для vGate версии 4.0 и выше по умолчанию используется порт базы данных PostgreSQL 5432. Значение данного порта можно изменить только при отдельной установке PostgreSQL (до установки ПО vGate). Порты базы данных PostgreSQL для основного и резервного серверов должны совпадать.

На экране появится следующий диалог.



9. Выберите способ маршрутизации трафика "Маршрутизацию осуществляет сервер авторизации vGate" и нажмите кнопку "Далее".

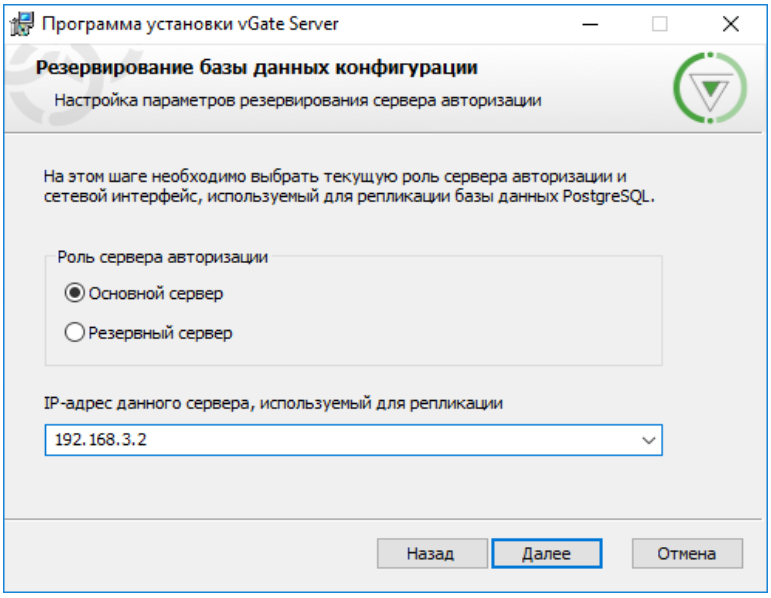
На экране появится следующий диалог.



10. Укажите сетевые параметры сервера авторизации и нажмите кнопку "Далее".

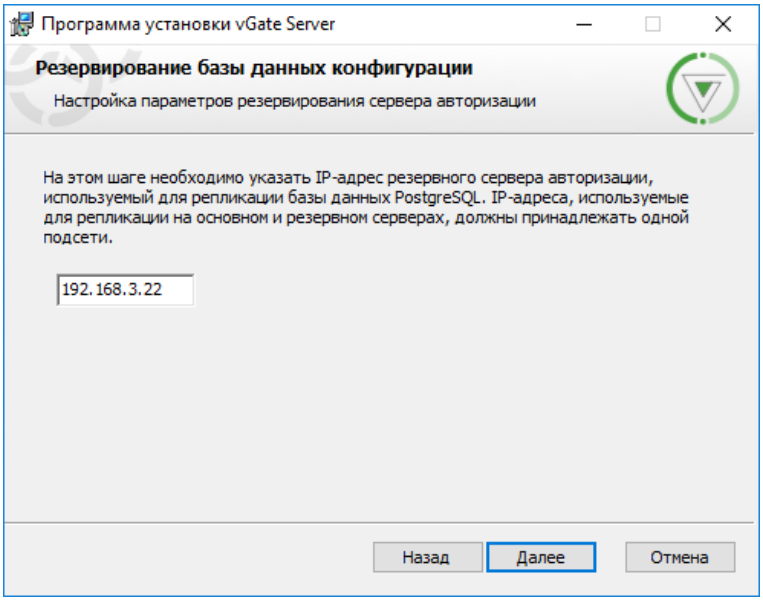
Параметр	Описание
IP-адрес сетевого адаптера во внешней сети администрирования	IP-адрес сервера во внешнем периметре сети администрирования инфраструктуры (подсети, в которой размещены рабочие места АИБ и АВИ)
IP-адрес сетевого адаптера для защищаемого периметра	IP-адрес сервера в защищаемом периметре сети администрирования инфраструктуры (подсети, в которой размещены защищаемые серверы виртуальной инфраструктуры)

Так как для установки был выбран компонент "Резервирование конфигурации", на экране появится диалог настройки параметров репликации.



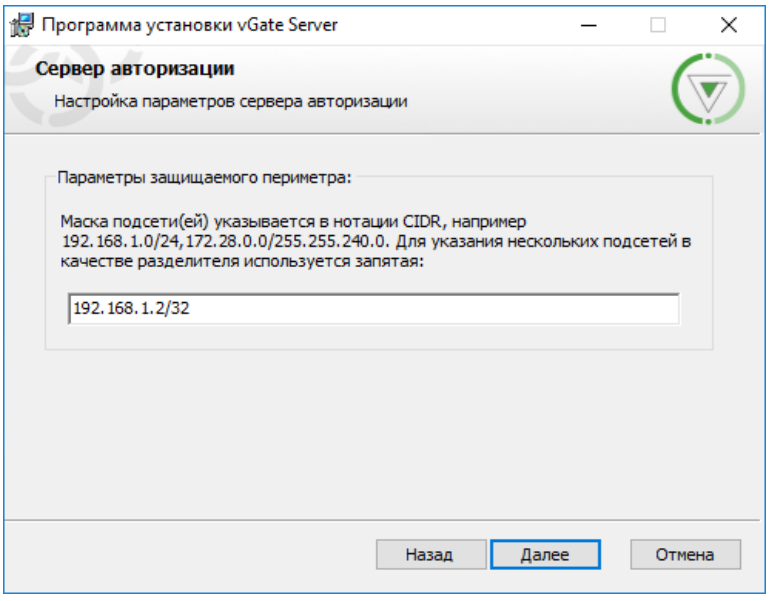
11. Выберите роль сервера авторизации "Основной сервер", укажите IP-адрес этого сервера, используемый для репликации данных между основным и резервным серверами авторизации в сети резервирования, и нажмите кнопку "Далее".

На экране появится диалог настройки параметров резервного сервера.

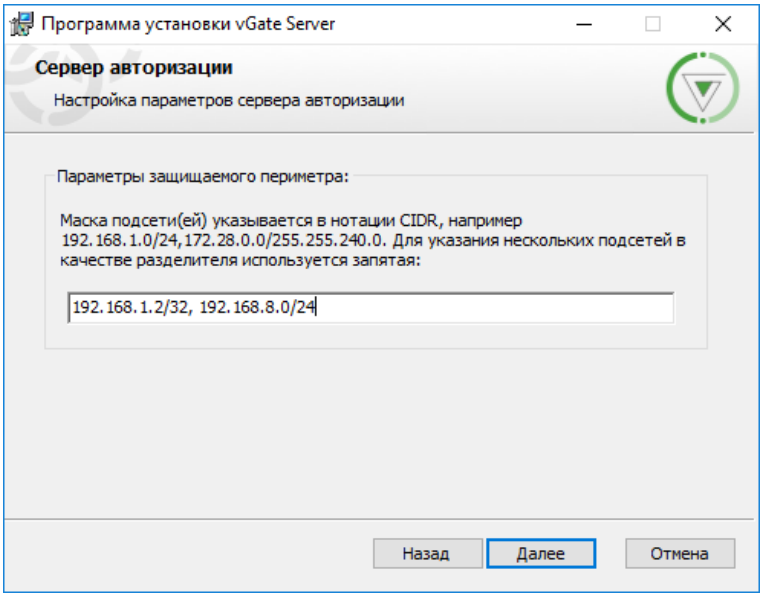


12. Укажите IP-адрес резервного сервера авторизации в сети резервирования, используемый для репликации, и нажмите кнопку "Далее".

На экране появится следующий диалог.



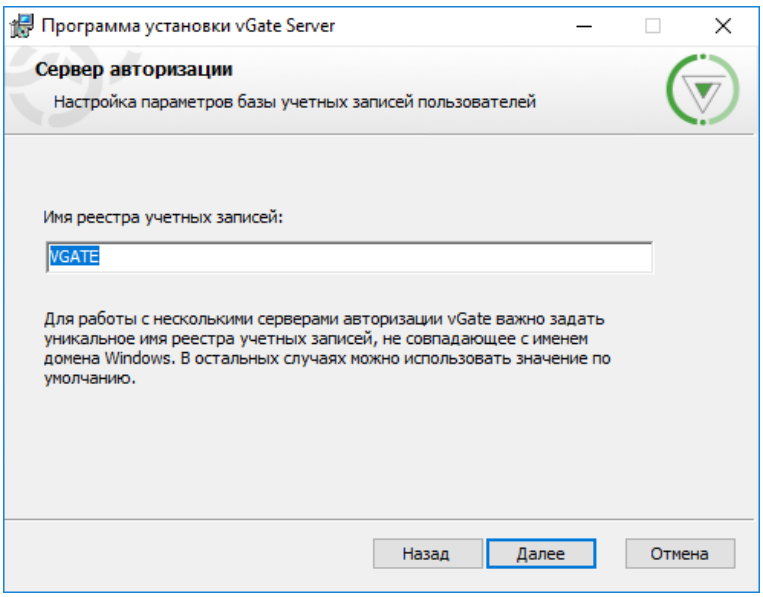
13. Если защищаемый периметр сети администрирования состоит из нескольких сетей, укажите их IP-адреса в текстовом поле, используя запятую в качестве разделителя.



Таким образом, передача данных внутрь защищаемого периметра будет разрешена только в том случае, если IP-адрес назначения соответствует одной из указанных подсетей.

14. Проверьте корректность IP-адресов подсетей, в которых размещаются защищаемые серверы Hyper-V, и нажмите кнопку "Далее".

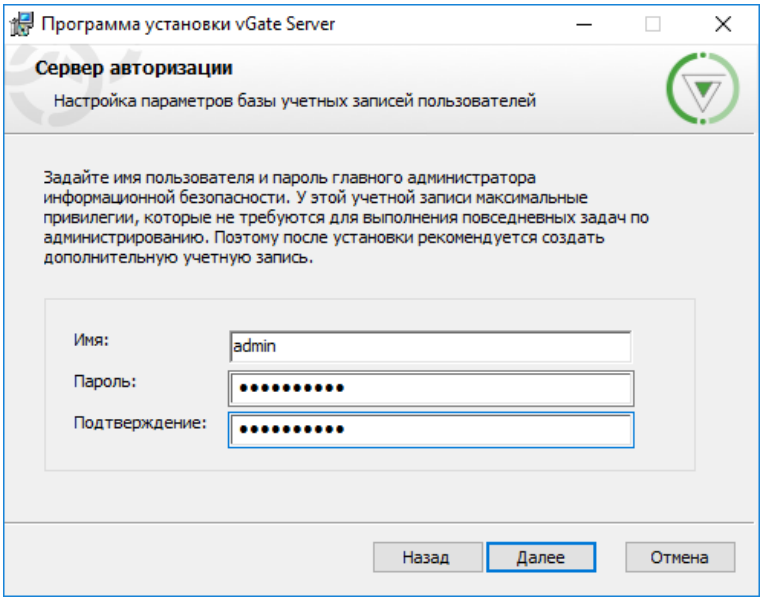
На экране появится следующий диалог.



Примечание. Если в сети планируется использовать несколько серверов авторизации, то при установке каждого сервера авторизации следует указывать уникальное имя реестра учетных записей vGate.

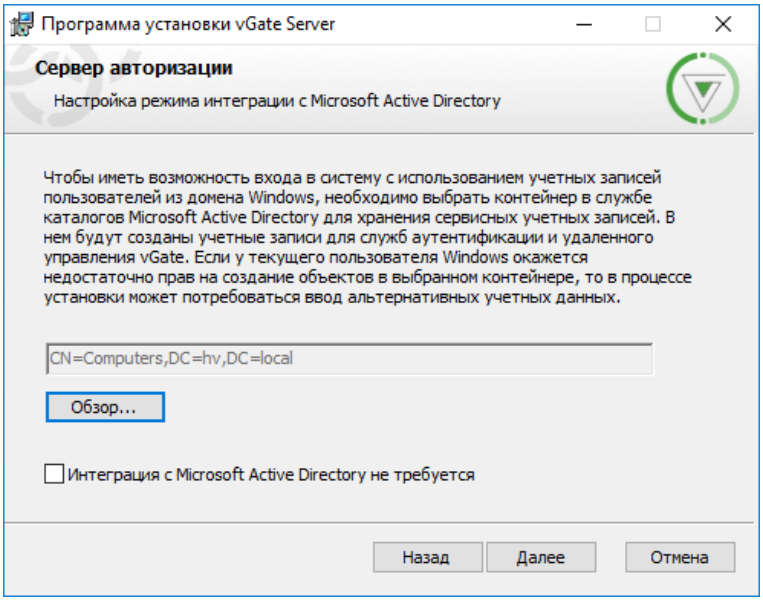
15. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

На экране появится следующий диалог.



16. Укажите учетные данные главного администратора информационной безопасности и нажмите кнопку "Далее".

Если учетная запись данного компьютера входит в домен Windows, на экране появится следующий диалог.



Примечание. Если используется учетная запись локального администратора, на экране появится сообщение об ошибке "Не удалось подключиться к службе каталогов". Поле выбора контейнера для учетных записей vGate будет пустым, а кнопка "Обзор" недоступна.

17. Укажите организационное подразделение (OU), созданное при конфигурировании локальной сети (см. стр.**11**) для хранения служебных учетных записей vGate, и нажмите кнопку "Далее".

Совет. Отметьте пункт "Интеграция с Microsoft Active Directory не требуется", если не планируется аутентификация в vGate с указанием учетных данных пользователей из домена Windows.

Примечание. Если учетная запись администратора не обладает правами группы Account Operators, то в процессе установки будет предложено ввести данные учетной записи, обладающей такими правами. В противном случае установка будет прекращена.

На экране появится диалог с сообщением о готовности к установке.

18. Нажмите кнопку "Установить".

Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

19. Нажмите кнопку "Готово".

> **Примечание.** В некоторых случаях на экране может появиться сообщение о необходимости перезагрузить компьютер. Выполните перезагрузку, нажав кнопку "Да" в окне сообщения.

Для установки резервного сервера авторизации:

1. Войдите в систему с правами администратора компьютера.

2. Поместите установочный диск в устройство чтения компакт-дисков.

> Если программа установки не запустилась автоматически, запустите на исполнение файл autorun.exe, находящийся в папке \autorun.

На экране появится стартовый диалог программы установки.

3. В стартовом диалоге программы установки активируйте ссылку "Сервер авторизации".

> **Совет.** Для выполнения установки этого продукта можно также запустить на исполнение файл \vGate\vGateServer.msi, находящийся на установочном диске.

Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.

4. Нажмите кнопку "Далее".

На экране появится диалог принятия лицензионного соглашения.

5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

> **Совет.** Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора устанавливаемых компонентов.

6. Нажмите мышью на значок слева от названия компонента "Резервирование конфигурации" и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск". Нажмите кнопку "Далее".

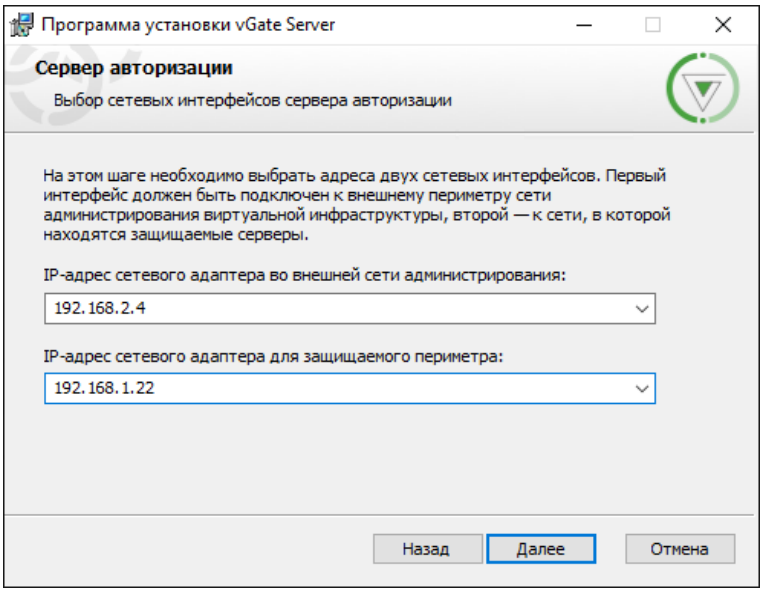
На экране появится диалог установки сервера баз данных PostgreSQL.

7. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее".

На экране появится диалог выбора способа маршрутизации трафика.

8. Выберите способ маршрутизации трафика "Маршрутизацию осуществляет сервер авторизации" и нажмите кнопку "Далее".

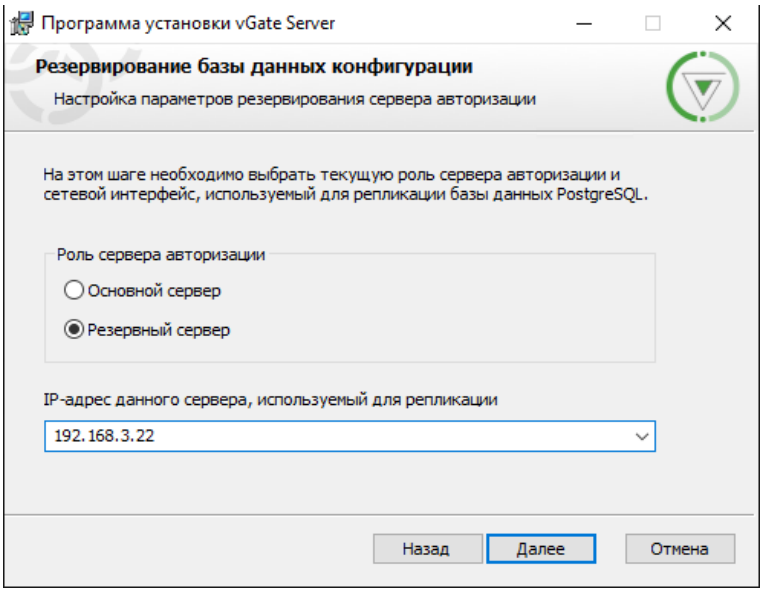
На экране появится диалог настройки сетевых параметров.



9. Укажите сетевые параметры резервного сервера авторизации и нажмите кнопку "Далее".

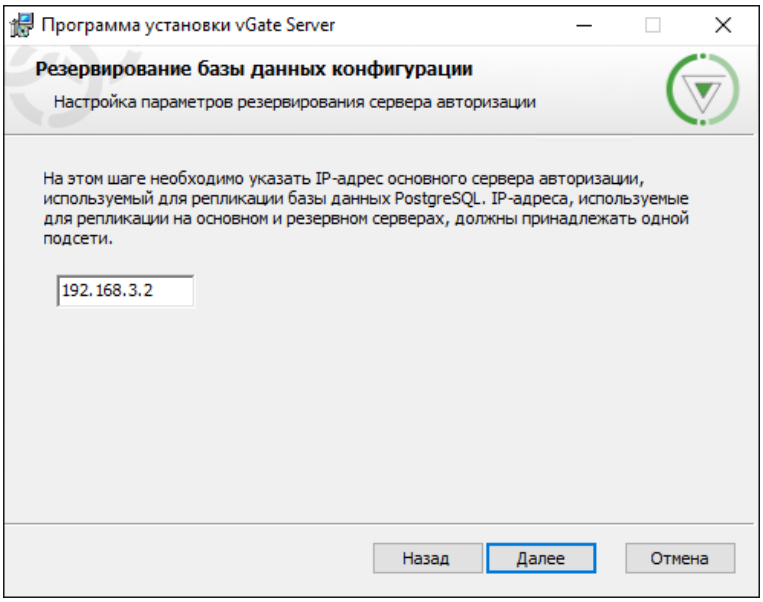
Параметр	Описание
IP-адрес сетевого адаптера во внешней сети администрирования	IP-адрес резервного сервера во внешнем периметре сети администрирования инфраструктуры
IP-адрес сетевого адаптера для защищаемого периметра	IP-адрес резервного сервера в сети администрирования инфраструктуры

На экране появится диалог настройки параметров репликации.



10. Выберите роль сервера авторизации "Резервный сервер", укажите IP-адрес этого сервера, используемый для репликации данных между основным и резервным серверами авторизации в сети резервирования, и нажмите кнопку "Далее".

На экране появится диалог настройки параметров основного сервера.



11. Укажите IP-адрес основного сервера авторизации в сети резервирования, используемый для репликации, и нажмите кнопку "Далее".

На экране появится диалог с сообщением о готовности к установке.

12. Нажмите кнопку "Установить".

Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

13. Нажмите кнопку "Готово".

Примечание. В некоторых случаях на экране может появиться сообщение о необходимости перезагрузить компьютер. Выполните перезагрузку, нажав кнопку "Да" в окне сообщения.

О настройке репликации между основным и резервным серверами читайте на стр.**55**.

Установка сервера авторизации на ВМ

Внимание! Допускается установка сервера авторизации на ВМ, но располагать его на защищаемом vGate сервере не рекомендуется.

При отсутствии свободного физического сервера сервер авторизации (как основной, так и резервный) может быть развернут на ВМ.

Перед установкой основного или резервного сервера авторизации на виртуальную машину необходимо подготовить сервер Hyper-V, удовлетворяющий следующим требованиям:

- наличие не менее двух физических сетевых адаптеров;
- размер ОЗУ и свободное место на диске, достаточные для запуска одной виртуальной машины под управлением Windows Server 2012 R2/2016/2019.

После этого на сервере Hyper-V следует создать виртуальную машину с одной из следующих ОС:

- Windows Server 2012 R2 x64 + Update KB2999226;
- Windows Server 2016 x64;
- Windows Server 2019 x64.

Порядок установки основного или резервного сервера авторизации на ВМ аналогичен порядку установки на выделенный компьютер (см. стр.**14** и стр.**26**).

Подготовка сервера виртуализации к установке vGate с резервированием

При использовании маршрутизатора:

1. Создайте на сервере Hyper-V внешний виртуальный коммутатор (vSwitch1) с привязкой к физическому сетевому адаптеру (vmnic0), подключенному к физической сети, которая используется как сеть защищаемых серверов.
2. Создайте на сервере Hyper-V внешний виртуальный коммутатор (vSwitch2) с привязкой к физическому сетевому адаптеру (vmnic1), подключенному к физической сети, которая используется как сеть резервирования.
3. Создайте на сервере Hyper-V две виртуальные машины (VM1 и VM2) и добавьте каждой из них два виртуальных сетевых адаптера, подключенных к ранее созданным виртуальным коммутаторам (vSwitch1 и vSwitch2).
4. Установите на обе ВМ гостевую операционную систему из списка поддерживаемых сервером авторизации vGate.
5. В гостевых операционных системах ВМ настройте сетевые адаптеры и выполните установку сервера авторизации vGate с резервированием (см. стр.**26**).

При маршрутизации трафика с использованием сервера авторизации:

1. Создайте на сервере Hyper-V внешний виртуальный коммутатор (vSwitch1) с привязкой к физическому сетевому адаптеру (vmnic0), подключенному к физической сети, которая используется как сеть администрирования инфраструктуры.
2. Создайте на сервере Hyper-V внешний виртуальный коммутатор (vSwitch2) с привязкой к физическому сетевому адаптеру (vmnic1), подключенному к физической сети, которая используется как сеть резервирования.
3. Создайте на сервере Hyper-V внешний виртуальный коммутатор (vSwitch3) с привязкой к физическому сетевому адаптеру (vmnic2), подключенному к физической сети, которая используется как сеть внешнего периметра администрирования (в которой размещены рабочие места АИБ и АВИ).
4. Создайте две ВМ (VM1, VM2) и добавьте каждой из них три виртуальных сетевых адаптера, подключенных к ранее созданным виртуальным коммутаторам (vSwitch1, vSwitch2 и vSwitch3).
5. Установите на обе ВМ гостевую операционную систему из списка поддерживаемых сервером авторизации vGate.
6. В гостевых операционных системах ВМ настройте сетевые адаптеры и выполните установку сервера авторизации vGate с резервированием

   (см. стр.**26**).

Установка агента аутентификации на ОС Windows

При установке агента аутентификации на компьютер, учетная запись которого находится в домене, добавленном в список доверенных доменов на сервере авторизации vGate, ввод учетных данных АИБ не требуется. В противном случае необходимо указать данные учетной записи АИБ, имеющей права оператора учетных записей (см. стр.**90**).

Для установки агента аутентификации:

1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков. Если программа установки не запустилась автоматически, запустите на исполнение файл autorun\autorun.exe, находящийся на этом диске.

   На экране появится диалог с перечнем программного обеспечения, содержащегося на установочном диске.
3. Активируйте ссылку "Агент аутентификации".

Совет. Для выполнения установки этого продукта можно также запустить на исполнение файл \vGate\vGateClient.msi, находящийся на установочном диске.

Программа установки выполнит подготовительные действия и выведет на экран диалог приветствия.

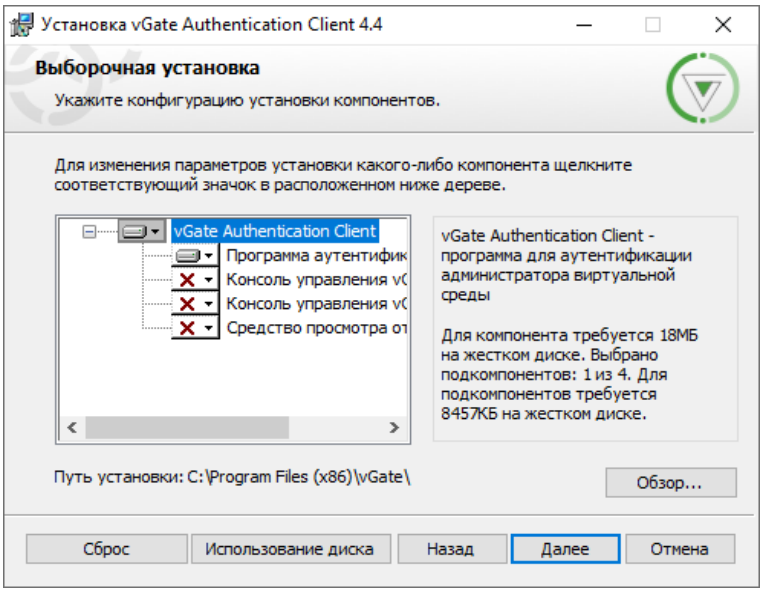
4. Нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.

5. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора устанавливаемых компонентов.



6. Выберите компоненты для установки и нажмите кнопку "Далее".

Пояснение. По умолчанию устанавливаются только компоненты ПО агента аутентификации. Если агент аутентификации устанавливается на рабочее место АИБ во внешнем периметре сети администрирования инфраструктуры, то на данный компьютер также необходимо установить консоль управления vGate для Hyper-V.

Возможно управление несколькими серверами авторизации с одного рабочего места АВИ или АИБ (см. раздел "Аутентификация пользователя" в документе [4]).

На экране появится диалог с сообщением о готовности к установке.

7. Нажмите кнопку "Установить".

   Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

   После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

8. Нажмите кнопку "Готово".

Примечание. После установки агента аутентификации рекомендуется перезагрузить компьютер.

Установка компонента защиты соединений сервера Hyper-V

Установка компонента защиты соединений сервера Hyper-V выполняется в случае, если необходимо осуществлять фильтрацию сетевых соединений сервера с помощью vGate.

Для установки компонента защиты:

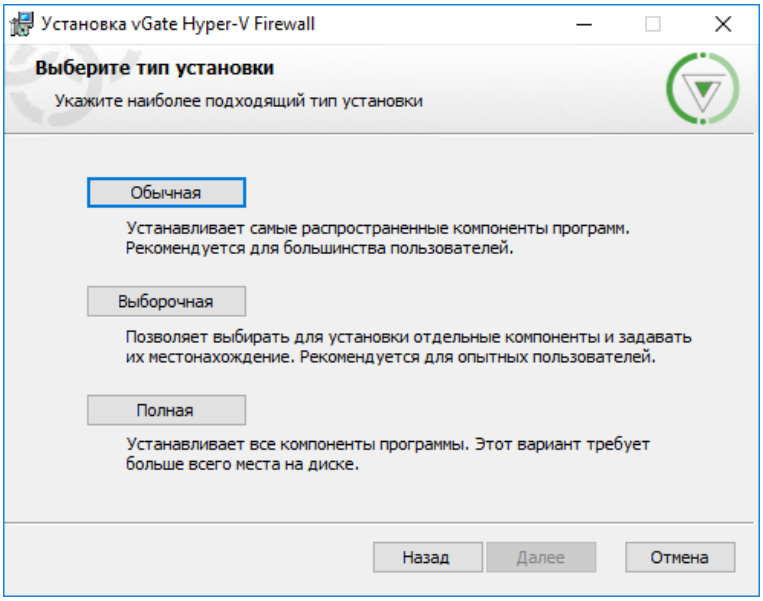
1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков и запустите на исполнение файл \vGateHyperVFirewall.msi.

   Программа установки выполнит подготовительные действия и выведет на экран диалог приветствия.
3. Нажмите кнопку "Далее".

   На экране появится диалог принятия лицензионного соглашения.
4. Ознакомьтесь с содержанием лицензионного соглашения, прочитав его до конца, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее".

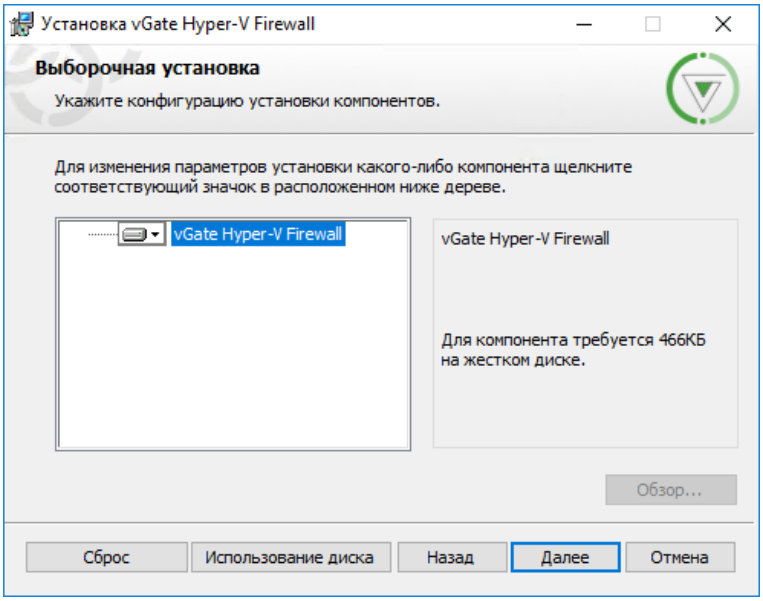
Совет. Для получения бумажной копии лицензионного соглашения нажмите кнопку "Печать".

На экране появится диалог для выбора типа установки.



5. Выберите тип установки и нажмите кнопку "Далее".

   На экране появится диалог для выбора устанавливаемых компонентов.



6. Выберите компонент для установки и нажмите кнопку "Далее".

   На экране появится диалог с сообщением о готовности к установке.

7. Нажмите кнопку "Установить".

   Начнется процесс копирования файлов на жесткий диск и настройки устанавливаемых компонентов. Ход этого процесса отображается в диалоге программы установки полосой прогресса.

   После успешной установки и настройки компонентов на экране появится диалог с сообщением об успешном завершении установки.

8. Нажмите кнопку "Готово".

Установка и настройка сервера мониторинга

Для работы функции мониторинга безопасности (см. стр.**144**) необходимо развернуть в сети сервер мониторинга.

Для развертывания сервера мониторинга:

1. В диспетчере Hyper-V создайте виртуальную машину, удовлетворяющую следующим требованиям:
   - процессор — 2 ГГц;
   - память — 4 ГБ;
   - сеть — LAN.
2. Подключите к созданной ВМ виртуальный жесткий диск (в формате VHD), расположенный на установочном диске vGate в архиве \monitoring\Monitoring-1.zip.
3. После запуска ВМ введите следующие учетные данные:

   Monitoring login: administrator

   Password: qwe

4. Выполните команду:

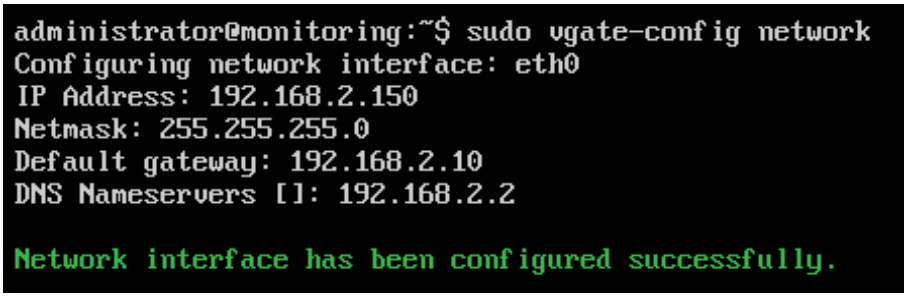
```
sudo vgate-config
```

На экране появится список доступных команд:

5. Для настройки сетевого интерфейса выполните команду:

```
sudo vgate-config network
```

6. Укажите IP-адрес сервера мониторинга, маску подсети, сетевой шлюз и DNS-сервер.



Совет. Можно пропустить настройку DNS-сервера, нажав клавишу Enter.

7. Создайте учетную запись пользователя для подключения к серверу мониторинга.

Для этого выполните команду и задайте имя и пароль пользователя:

```
sudo vgate-config users create
```

По окончании настройки выполните подключение к серверу мониторинга в веб-консоли vGate (см. стр.**144**).

Глава 2
Обновление vGate 4.2 и 4.3 на vGate 4.4

План обновления

Обновление компонентов vGate следует производить в следующем порядке:

№	Шаг установки	Особенности	Описание
1	**Резервное копирование конфигурации**		См. стр.**51**
2	**Экспорт конфигурации vGate**	Экспорт конфигурации vGate версий 4.2 и 4.3 производится в консоли управления vGate	См. стр.**79**
3	**Удаление ПО vGate 4.2 и 4.3**	Выполняется удаление ПО сервера авторизации vGate, агента аутентификации, модуля защиты Hyper-V и консоли управления vGate для Hyper-V, а также PostgreSQL 9.4 (x86). При использовании функции мониторинга безопасности необходимо выполнить удаление сервера мониторинга	См. стр.**53**
4	**Установка ПО vGate 4.4**	Выполняется установка ПО сервера авторизации vGate, агента аутентификации, модуля защиты Hyper-V и консоли управления vGate для Hyper-V. При использовании функции мониторинга безопасности необходимо также выполнить установку и настройку сервера мониторинга	См. стр.**10**
5	**Импорт конфигурации vGate**	В консоли управления выполняется импорт конфигурации vGate, полученной на шаге 2	См. стр.**79**

Примечание. Если до обновления использовалась функция горячего резервирования, в консоли управления на основном сервере авторизации перейдите на вкладку "Конфигурация | Сервер авторизации" и выполните настройку горячего резервирования (см. стр.**69**).

Резервное копирование конфигурации

Перед установкой новой версии vGate необходимо выполнить резервное копирование базы данных конфигурации vGate с помощью вспомогательной утилиты db-util.exe. Утилита располагается в папке, в которую был установлен компонент "Сервер авторизации".

Для создания резервной копии базы данных конфигурации vGate:

1. На основном сервере авторизации создайте папку, в которую будет записана копия конфигурации.
2. Откройте редактор командной строки и выполните следующую команду:

   ```
   db-util.exe -b c:\Backup
   ```

   где
   - db-util.exe — путь к исполняемому файлу утилиты;
   - c:\Backup — путь к созданной папке для хранения резервной копии конфигурации.
3. Убедитесь, что указанная папка содержит копию конфигурации.

Восстановление сервера авторизации

В случае если обновление сервера авторизации завершилось неудачно, для восстановления установленной ранее версии vGate необходимо выполнить следующие действия.

Для восстановления сервера авторизации:

1. Удалите ПО основного сервера авторизации vGate (см. стр.**54**).
2. Удалите ПО PostgreSQL на основном сервере авторизации. После завершения удаления PostgreSQL удалите оставшиеся на компьютере папки установки vGate и ПО PostgreSQL.
3. Установите ПО сервера авторизации vGate той версии, которая была установлена ранее.
4. Выполните восстановление конфигурации vGate из резервной копии с помощью утилиты db_util (см. ниже).

Восстановление резервной копии конфигурации

Для восстановления резервной копии конфигурации:

1. Остановите все службы vGate (иначе восстановление не будет произведено).

   Примечание. Дополнительно необходимо отключить функцию горячего резервирования в консоли управления на основном сервере авторизации vGate (см. стр.**69**), если данная функция используется.

2. Откройте редактор командной строки и выполните следующую команду:

   ```
   db-util.exe -r c:\Backup
   ```

   где

   - db-util.exe — путь к исполняемому файлу утилиты;
   - c:\Backup — путь к созданной папке для хранения резервной копии конфигурации.

   Совет. При необходимости вы также можете использовать следующие аргументы:
   - -f [--force] – команда восстановления конфигурации -r [--restore] не будет запрашивать подтверждение на операцию;
   - -v [--verbose] – операции резервирования и восстановления будут иметь подробный вывод.

   Пример: db-util.exe -v -r c:\Backup -f.

3. Из каталога установки vGate\Kerberos удалите следующие файлы:
   - krb5kt;
   - .k5.VGATE, где VGATE — имя реестра учетных записей vGate.
4. Запустите остановленные службы vGate. При необходимости включите функцию горячего резервирования vGate (см. стр.**69**).

   Примечание. Если в конфигурации vGate использовалась интеграция с Active Directory, то после восстановления необходимо добавить домен, в который входит сервер авторизации, в список доверенных доменов в консоли управления vGate.

   Примечание. После восстановления резервной копии конфигурации возможно отключение репликации из-за переполнения журнала WAL. Для возобновления репликации используйте команду db-util.exe –recreate-replica (см. стр.**172**).

Глава 3
Переустановка и удаление vGate

Программы установки сервера авторизации vGate, агента аутентификации, модуля защиты Hyper-V и консоли управления vGate для Hyper-V позволяют изменить параметры установки и перечень установленных компонентов, а также удалить установленное ПО с компьютера.

Перед тем как приступить к выполнению этих действий, завершите работу консоли управления и агента аутентификации.

Для запуска программы установки:

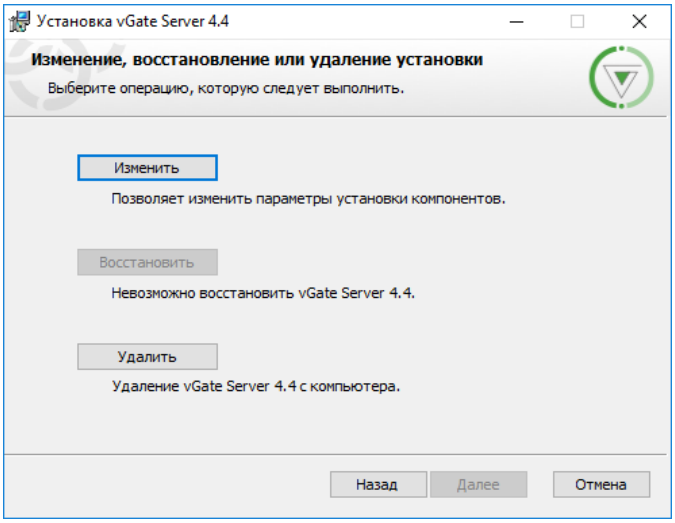
1. Запустите соответствующую программу установки.

   Совет. Это можно сделать двумя способами:
   - Запустите на исполнение файл vGateServer.msi или vGateClient.msi из каталога \vGate\ либо файл vGateHyperVAgent.msi из каталога \vGate\Hyper-V на установочном диске.
   - Активируйте в Панели управления компонент "Программы и компоненты". Выберите в списке установленных программ элемент "vGate Server 4.4", "vGate Authentication Client 4.4" или "vGate Hyper-V Agent 4.4" и нажмите кнопку "Изменить".

   Программа выполнит подготовительные действия и выведет на экран диалог приветствия.

2. Нажмите кнопку "Далее".

   На экране появится диалог "Изменение, восстановление или удаление установки".



Изменение параметров установки

В этом режиме работы программа установки позволяет изменить перечень установленных компонентов, например, добавить или удалить компонент "Резервирование конфигурации" на сервере авторизации.

Для изменения параметров установки:

1. Нажмите кнопку "Изменить".
2. Измените параметры, следуя инструкциям мастера установки.

Переустановка компонентов резервирования

Для переустановки компонентов резервирования:

1. Удалите ПО резервного сервера авторизации. Для этого воспользуйтесь программой установки компонента "Сервер авторизации" (см. стр.**54**) или средствами ОС Windows "Установка и удаление программ". По завершении процедуры удаления перегрузите компьютер.
2. Удалите компонент "Резервирование конфигурации" на основном сервере авторизации. Для этого воспользуйтесь программой установки компонента "Сервер авторизации" (см. стр.**54**) или средствами ОС Windows "Установка и удаление программ". По завершении процедуры удаления перегрузите компьютер.
3. Выполните установку компонентов "Резервирование конфигурации" на основном сервере авторизации, а затем на резервном сервере (см. стр.**26**).

Удаление

Внимание!

- Перед удалением сервера авторизации vGate необходимо удалить компоненты защиты со всех серверов Hyper-V и SCVMM с помощью консоли управления (см. стр.**89**).
- Удаление агента аутентификации следует выполнять перед удалением сервера авторизации.

Для удаления программного обеспечения:

1. Нажмите кнопку "Удалить" в диалоге "Изменение, восстановление или удаление установки".

   На экране появится диалог с сообщением о готовности к удалению.
2. Нажмите кнопку "Удалить".

   Начнется удаление установленных компонентов. По окончании процесса удаления на экране появится диалог об успешном завершении операции.
3. Нажмите кнопку "Готово".

Глава 4
Резервирование

Для обеспечения отказоустойчивости основного сервера авторизации используется функция резервирования, которая предусматривает ввод в эксплуатацию дополнительного (резервного) сервера авторизации.

Функция резервирования сервера авторизации доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Ввод в эксплуатацию резервного сервера авторизации

План ввода

Ввод в эксплуатацию резервного сервера авторизации выполняется в следующем порядке:

№	Шаг	Особенности	Описание
1.	**Предварительная настройка**		См. ниже
2.	**Установка ПО резервного сервера авторизации и консоли управления**	Выполняется на резервном сервере	См. стр.**33** или стр.**43** (в зависимости от выбранного способа маршрутизации трафика)

Внимание! До установки ПО резервного сервера авторизации vGate необходимо зарегистрировать лицензию для демонстрационной версии vGate, лицензию на использование vGate Enterprise или Enterprise Plus в консоли управления vGate R2 на основном сервере авторизации.

Предварительная настройка

Внимание! Если предполагается использование конфигурации с резервным сервером авторизации, в локальной сети должен присутствовать DNS-сервер. Рекомендуется поместить его во внешней сети.

Перед вводом в эксплуатацию резервного сервера:

1. Выполните настройку сетевых соединений основного и резервного серверов так, как описано на стр.**27** (при использовании стороннего маршрутизатора) или на стр.**36** (без использования отдельного маршрутизатора).
2. На основной сервер установите компонент "Резервирование конфигурации". На резервный сервер установите ПО резервного сервера авторизации. Процедура установки приведена на стр.**33** (при использовании маршрутизатора) или на стр.**43** (без использования отдельного маршрутизатора).
3. В DNS настройте псевдоним (CName), указывающий на полное доменное имя (FQDN) основного сервера.
4. При установке агентов аутентификации на рабочие места пользователей и компьютеры в качестве сервера авторизации укажите полное доменное имя (FQDN) псевдонима. Процедура установки агента аутентификации представлена на стр.**46**.

В качестве примера в настоящей главе будут использованы серверы, имеющие следующие настройки.

Основной сервер

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	• IP-адрес, используемый серверами Hyper-V для конфигурации и аудита: **192.168.1.2** • Дополнительный IP-адрес, используемый при сбое основного сервера и его замене резервным: **192.168.1.12**
Адаптер 2	Сеть внешнего периметра администрирования	• IP-адрес из диапазона адресов внешней сети, используемый для соединения с рабочими местами АВИ и АИБ: **192.168.2.3**
Адаптер 3	Сеть резервирования	• IP-адрес из диапазона адресов сети резервирования, по которому будет осуществляться репликация данных между основным и резервным серверами авторизации: **192.168.3.2**

Резервный сервер

Адаптер	Подсеть	Настройки локальной сети
Адаптер 1	Сеть администрирования инфраструктуры	• IP-адрес, используемый серверами Hyper-V для конфигурации и аудита: **192.168.1.22**
Адаптер 2	Сеть внешнего периметра администрирования	• IP-адрес, используемый для связи с рабочими местами АВИ и АИБ: **192.168.2.4**
Адаптер 3	Сеть резервирования	• IP-адрес из диапазона адресов сети резервирования, используемый для соединения с основным сервером авторизации: **192.168.3.22**

В примере маршрутизацию трафика между внешним периметром сети администрирования и сетью защищаемых серверов выполняет сервер авторизации. При использовании маршрутизатора обеспечение отказоустойчивости происходит аналогично.

Автоматическое переключение на резервный сервер

Резервирование в vGate включает в себя возможность автоматического переключения на резервный сервер авторизации в случае сбоя основного сервера (см. стр.**69**).

Для реализации этой функциональности на основном и резервном серверах авторизации запущена служба резервирования сервера авторизации vGate (fmsvc.exe), которая осуществляет мониторинг состояния второго узла кластера серверов авторизации.

Резервный сервер авторизации осуществляет попытки подключения к основному серверу авторизации через заданный интервал времени (см. стр.**69**). Ниже описаны два варианта развития событий, которые приводят к автоматическому переключению управления с основного сервера на резервный.

Соединение между резервным и основным серверами авторизации отсутствует

Если соединение между резервным и основным серверами отсутствует, проверяются следующие условия:

1. На резервном сервере авторизации установлено соединение хотя бы с одним из защищаемых серверов (на которых установлен компонент защиты vGate).
2. После заданного количества неудачных попыток соединения со службами (см. стр.**69**) ситуация не меняется.

Если данные условия выполнены, происходит автоматическое переключение управления на резервный сервер авторизации vGate. На бывшем основном сервере при этом выполняются следующие действия:

1. Из настроек сетевого адаптера удаляется основной IP-адрес (192.168.1.2).
2. Выполняется остановка службы аутентификации vGate (aupa.exe) и службы проксирования трафика vGate (vcp.exe).
3. Выполняется включение анонимного правила для доступа к данному серверу по протоколу RDP.

Автоматическое восстановление репликации

Если после смены ролей серверов авторизации соединение между ними было восстановлено, возможно автоматическое восстановление репликации. Данная опция включена по умолчанию.

Установка ПО резервного сервера на новом сервере

После смены ролей серверов авторизации можно выполнить установку ПО резервного сервера vGate на новом сервере.

Примечание. На новом резервном сервере необходимо использовать такой же IP-адрес в сети резервирования, какой был у предыдущего резервного сервера. Если нужно указать другой IP-адрес, выполните переустановку компонента резервирования на новом основном сервере, указав новый IP-адрес резервного сервера.

Примечание. Доступ к бывшему основному серверу авторизации можно получить локально или по протоколу RDP (данная функция должна быть активна в настройках ОС).

Для установки ПО резервного сервера:

1. Удалите ПО vGate, ПО сервера баз данных PostgreSQL и каталоги установки данного ПО.
2. Установите ПО vGate с компонентом "Резервирование конфигурации" (см. стр.**26**).

Соединение между резервным и основным серверами авторизации установлено

Если соединение между резервным и основным серверами авторизации установлено, проверяются следующие условия:

1. Хотя бы одна из служб aupa.exe, inchd.exe, julius.exe, krb5kdcd, rhuid.exe, hvrhuid.exe, vcp.exe, vgate.webapp на основном сервере не работает.
2. После заданного количества неудачных попыток соединения со службами (см. стр.**69**) ситуация не меняется.

Если данные условия выполнены, происходит смена ролей серверов авторизации. В случае если эта операция завершается с ошибкой, выполняется принудительное переключение управления на резервный сервер авторизации. На бывшем основном сервере выполняются действия, описанные выше.

Мониторинг состояния резервирования

В Failover Monitor есть функция мониторинга состояния резервирования, которая управляет сообщениями об изменении состояния репликации.

Сообщение о сбое/восстановлении репликации записывается в журнал событий сервера, отправившего запрос, в журнал vGate и в лог-файл Failover Monitor.

Основные причины отказа репликации:

- отставание резервного сервера авторизации vGate от основного при большой нагрузке на базу данных;
- отказ одного из серверов авторизации;
- нарушение связи между основным и резервным серверами авторизации по сети репликации.

Замена основного сервера при сбое

Если в консоли управления vGate не настроена функция автоматического переключения на резервный сервер авторизации, то в случае выхода из строя основного сервера необходимо вручную сделать резервный сервер основным до тех пор, пока основной сервер не будет восстановлен или заменен.

Пояснение. В качестве примеров в процедурах данного раздела используются IP-адреса основного и резервного серверов авторизации, указанные в таблице (см. стр.**56**).

Передача управления резервному серверу авторизации

1. Отключите питание на основном сервере.
2. Запустите консоль управления vGate на резервном сервере от имени администратора (см. стр.**61**), перейдите в раздел "Конфигурация", откройте группу параметров "Сервер авторизации" и нажмите кнопку-ссылку "Назначить основным". В появившемся окне нажмите кнопку "Сменить роль".

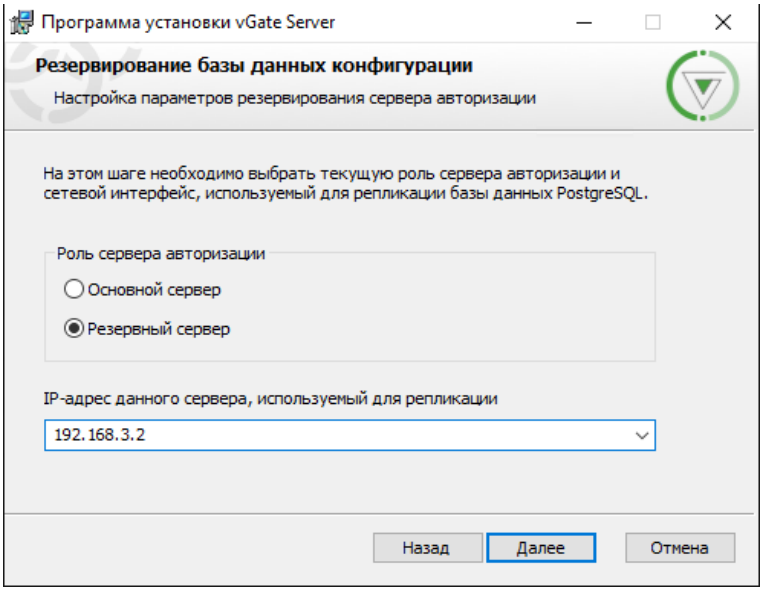
   Резервному серверу будет назначен основной IP-адрес основного сервера (192.168.1.2), а его собственный IP-адрес (192.168.1.22) станет дополнительным.
3. В DNS измените настройки псевдонима, настроив ссылку на полное доменное имя (FQDN) резервного сервера.
4. Если маршрутизацию трафика выполняют серверы авторизации, измените настройки маршрута в защищаемый периметр для всех компьютеров во внешней сети, на которых не был установлен агент аутентификации vGate, с учетом нового внешнего IP-адреса сервера авторизации (192.168.2.4).

   Если на внешнем компьютере установлен агент аутентификации vGate, то маршрут будет изменен автоматически при выполнении следующих условий:
   - в конфигурации vGate включена опция "Добавлять на клиенте маршрут к защищенной сети";
   - внешний компьютер и сервер авторизации vGate находятся в одной подсети.

Ввод в эксплуатацию нового сервера

Для ввода в эксплуатацию нового сервера:

1. Настройте на новом сервере соединения локальной сети по схеме резервного сервера (см. стр.**27** или стр.**36** в зависимости от выбранного способа маршрутизации трафика). В качестве IP-адреса в сети администрирования инфраструктуры укажите 192.168.1.12, а в качестве IP- адреса внешнего периметра — 192.168.2.3.
2. Выполните установку ПО резервного сервера авторизации (см. стр.**33** или стр.**43** в зависимости от выбранного способа маршрутизации трафика). На шаге **6** установки в качестве IP-адресов основного и резервного серверов из сети резервирования укажите адреса 192.168.3.22 и 192.168.3.2 соответственно.



Если вместо ввода в эксплуатацию нового основного сервера был восстановлен после сбоя прежний основной сервер, удалите из настроек адаптера 1 основной IP-адрес сервера (192.168.1.2). У сервера-1 должен остаться только один IP-адрес из сети администрирования инфраструктуры (192.168.1.12). Затем полностью удалите ПО vGate и ПО сервера баз данных PostgreSQL на этом сервере и выполните установку резервного сервера авторизации vGate.

Смена ролей серверов авторизации

В случае проведения регламентных работ на основном сервере авторизации можно временно изменить роль сервера.

Для изменения ролей серверов авторизации:

1. На основном сервере в разделе "Конфигурация" откройте группу параметров "Сервер авторизации" и нажмите кнопку-ссылку "Назначить резервным". В появившемся на экране диалоге нажмите кнопку "Сменить роль".
2. Откройте консоль управления на резервном сервере (новый основной сервер).
3. В DNS измените настройки псевдонима, настроив ссылку на новый основной сервер.
4. Если маршрутизацию трафика выполняют серверы авторизации, измените настройки маршрута в защищаемый периметр для всех внешних компьютеров, на которых не был установлен агент аутентификации vGate, с учетом нового IP-адреса сервера авторизации во внешнем периметре сети администрирования (192.168.2.3).

По окончании регламентных работ на основном сервере авторизации необходимо провести обратную процедуру изменения ролей серверов vGate.

Если на внешнем компьютере установлен агент аутентификации vGate, то маршрут будет изменен автоматически при выполнении следующих условий:

- в конфигурации vGate включена опция "Добавлять на клиенте маршрут к защищенной сети";
- внешний компьютер и сервер авторизации vGate находятся в одной подсети.

Переустановка сервера авторизации

Переустановка резервного сервера авторизации

При плановой или аварийной замене резервного сервера vGate необходимо выполнить его переустановку.

Примечание. На новом резервном сервере необходимо использовать такой же IP-адрес в сети резервирования, какой был у прежнего резервного сервера. Если нужно указать другой IP-адрес, выполните переустановку компонента резервирования на новом основном сервере, указав новый IP-адрес резервного сервера.

Для переустановки резервного сервера:

1. Если необходимо, удалите ПО vGate и ПО сервера баз данных PostgreSQL с компьютера, предназначенного для установки резервного сервера авторизации.

   После удаления ПО PostgreSQL необходимо удалить каталог установки данного ПО.

2. На основном сервере авторизации выполните переустановку компонента "Резервирование конфигурации" и настройте репликацию данных между резервным и основным серверами авторизации vGate.
3. Установите ПО vGate R2 на компьютере, предназначенном для резервного сервера авторизации (см. стр.**26**).

Переустановка основного сервера авторизации

Для переустановки основного сервера авторизации рекомендуется выполнить те же действия, что при замене основного сервера при сбое (см. стр.**58**).

Глава 5
Настройка конфигурации

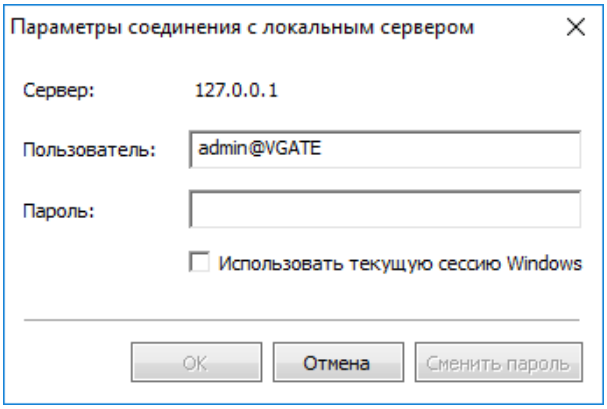
Консоль управления

Для запуска консоли управления:

1. Выберите в меню "Пуск" команду "Приложения | Код Безопасности | vGate | Консоль управления vGate для Hyper-V".

В ОС Windows более ранней версии, чем Windows 8 или Windows Server 2012, следует выбрать команду "Программы | Код Безопасности | vGate | Консоль управления vGate для Hyper-V".

Если консоль запущена на сервере авторизации, появится диалог соединения с сервером.



Пояснение. Если консоль управления запущена на рабочем месте АИБ, расположенном на отдельном компьютере, то будут использованы данные сервера авторизации и учетные данные администратора, указанные при подключении к защищенной среде в агенте аутентификации.

2. Укажите параметры соединения с сервером авторизации и нажмите кнопку "OK".

Параметр	Описание
Сервер	Полное доменное имя или IP-адрес сервера авторизации. Поле заполняется автоматически
Пользователь	Имя учетной записи главного администратора информационной безопасности
Пароль	Пароль главного администратора информационной безопасности
Использовать текущую сессию Windows	Отметьте это поле, чтобы использовать учетные данные пользователя Windows (если сервер авторизации vGate входит в домен)

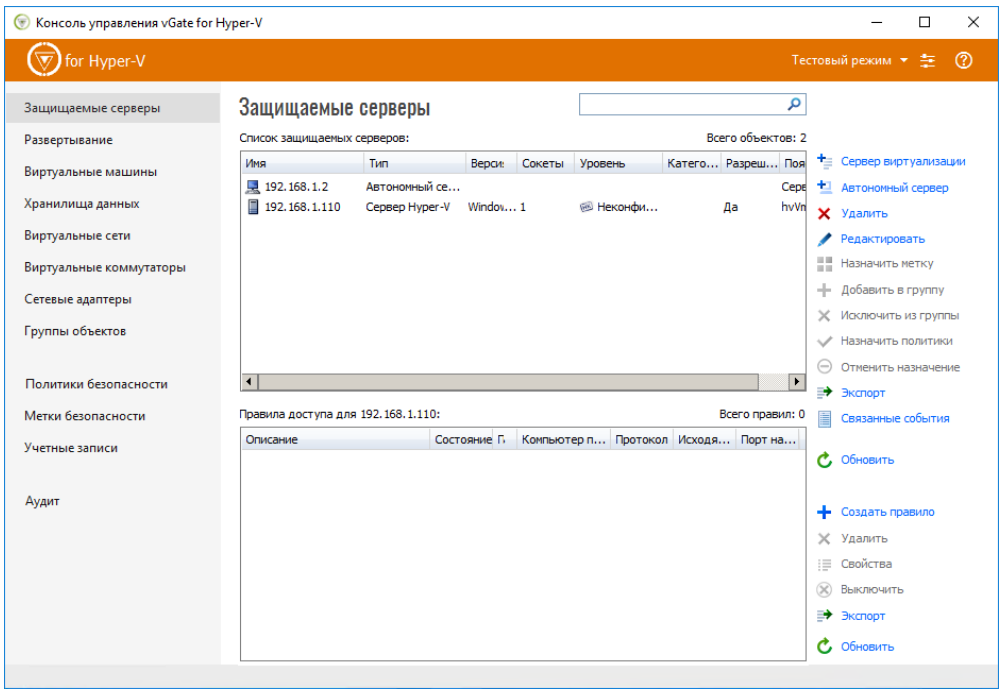
Совет. Для изменения пароля АИБ нажмите кнопку "Сменить пароль".

На экране появится консоль управления vGate.

Примечание. Во время первого запуска консоли управления на экране появится мастер первоначальной настройки (см. стр.62).

Окно консоли управления имеет три рабочие области:

- главное меню (верхняя панель);
- область функций (левая панель);
- область параметров (центральная часть окна).

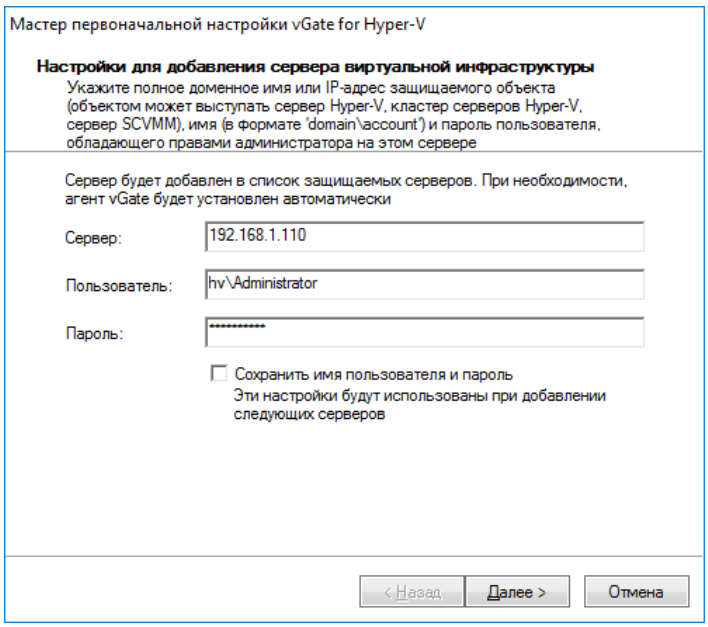


В области параметров отображаются объекты, связанные с выбранной функцией. Для выполнения доступных операций в правой части области параметров находятся кнопки-ссылки. Для поиска объектов по названию в верхней части окна располагается форма поиска.

Главное меню содержит служебные инструменты для выбора режима работы, настройки конфигурации vGate, а также просмотра информации о программе и управления лицензиями.

Мастер первоначальной настройки

Во время первого запуска консоли управления vGate на экране появится мастер первоначальной настройки.



Мастер первоначальной настройки позволяет задать параметры соединения с сервером виртуальной инфраструктуры, указать защищаемые серверы в сети администрирования инфраструктуры и добавить учетные записи пользователей vGate.

Чтобы пропустить какой-либо шаг настройки мастера, нажмите "Далее". Чтобы вернуться к предыдущему шагу, нажмите кнопку "Назад".
Чтобы закрыть мастер первоначальной настройки, нажмите кнопку "Отмена". Вы сможете настроить все необходимые для работы параметры позже (см. стр.65).

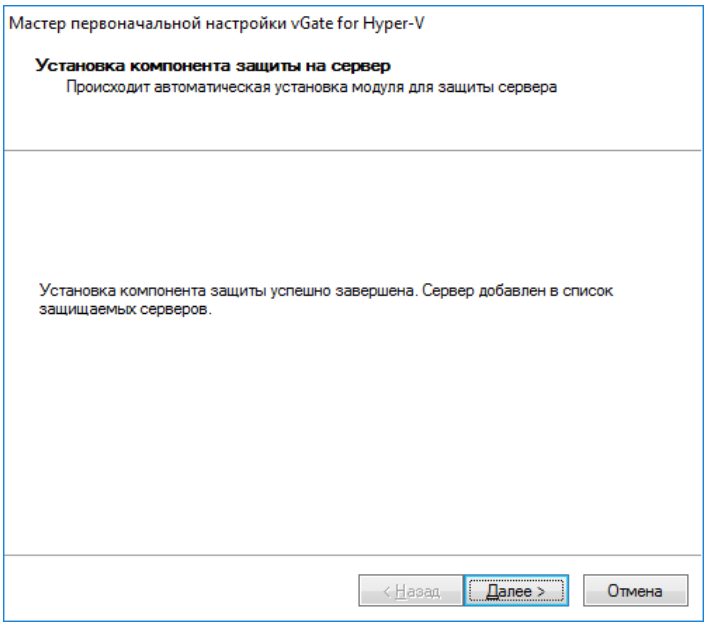
Для первоначальной настройки vGate:

1. Укажите полное доменное имя либо IP-адрес сервера Hyper-V, кластера серверов или сервера SCVMM, а также имя и пароль администратора для данного сервера и нажмите кнопку "Далее".

   Совет. Отметьте поле "Сохранить имя пользователя и пароль", чтобы использовать введенные данные в качестве данных общей учетной записи (см. стр.70).

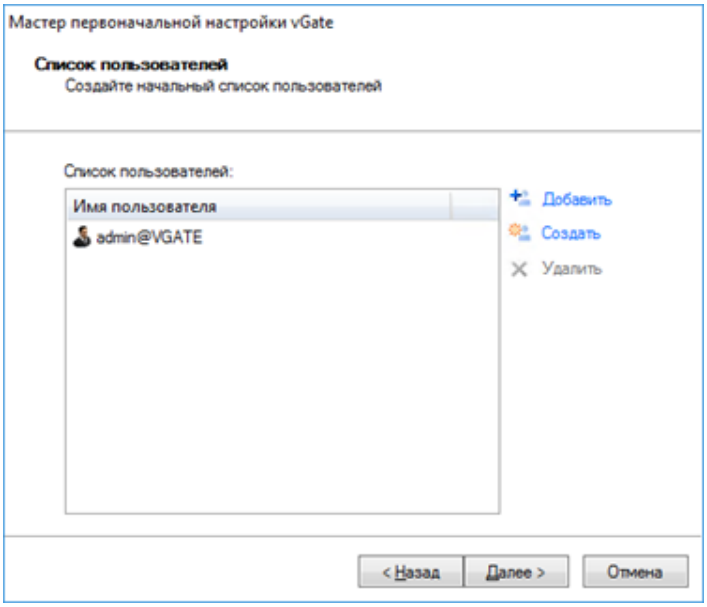
   На указанный сервер будет автоматически установлен агент защиты сервера Hyper-V, и он будет добавлен в список защищаемых объектов. На экране появится сообщение об успешном завершении операции.

   При добавлении кластера серверов в список защищаемых объектов также необходимо добавить все входящие в него серверы Hyper-V. Установка компонента защиты на кластер серверов не производится.



2. Нажмите кнопку "Далее".

   На экране появится диалог добавления учетных записей пользователей.

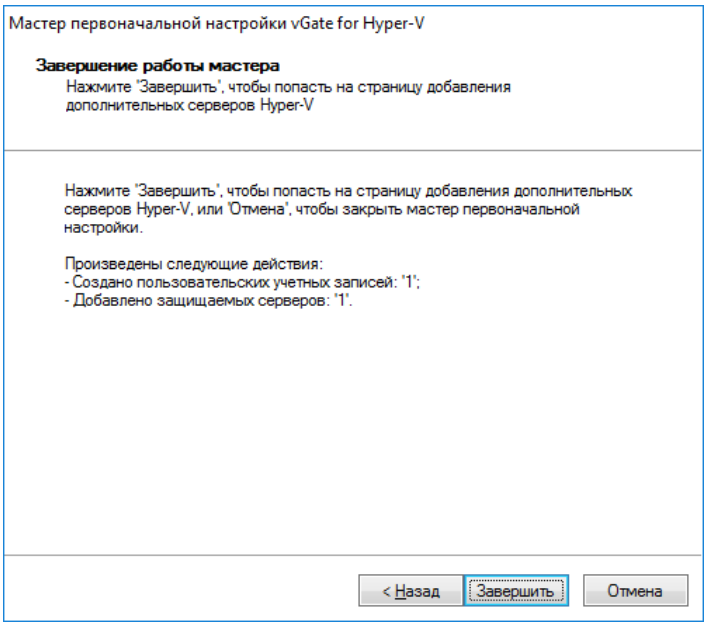


   По умолчанию список пользователей уже содержит учетную запись главного АИБ (см. стр.**90**).

3. Чтобы добавить пользователя из Active Directory, нажмите кнопку-ссылку "Добавить" и зарегистрируйте существующую учетную запись (см. стр.**90**). Для создания нового пользователя нажмите кнопку-ссылку "Создать" (см. стр.**92**).

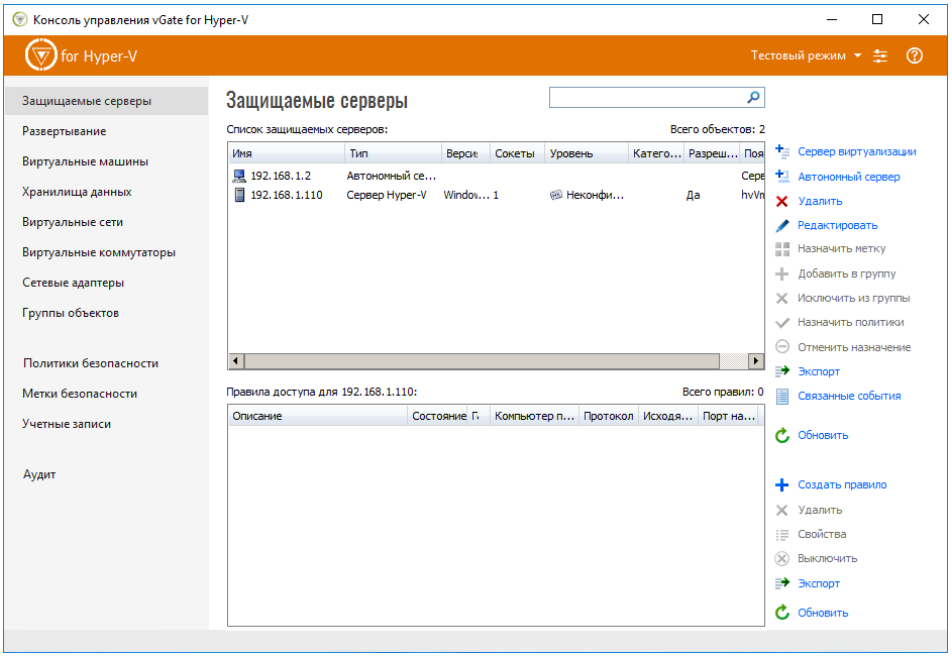
4. Нажмите кнопку "Далее".

   На последнем шаге мастер отобразит сведения о совершенных действиях.



5. Чтобы завершить работу мастера, нажмите "Завершить".

   На экране появится окно управления защищаемыми серверами.



Общий порядок настройки

План настройки конфигурации

1. Нажмите кнопку в области главного меню консоли управления и зарегистрируйте имеющуюся лицензию на использование vGate для защиты серверов Hyper-V (см. стр.**66**).
2. Нажмите кнопку в области главного меню. Если для соединения с защищаемыми серверами используется общая учетная запись, настройте параметры соединения с серверами Hyper-V (см. стр.**70**).
3. Выберите функцию "Защищаемые серверы" и добавьте серверы Hyper-V в список защищаемых серверов. Для этого используйте кнопку "Сервер виртуализации" (см. стр.**88**).

   Пояснение. На экране появится мастер добавления нового защищаемого сервера (см. стр.**88**). Если на шаге **2** были заданы параметры общей учетной записи, они будут указаны в окне мастера. При добавлении серверов Hyper-V в список защищаемых серверов на них автоматически устанавливается компонент защиты vGate.

4. Добавьте сервер SCVMM, если он присутствует в конфигурации, в список защищаемых серверов. Для этого используйте кнопку "Сервер виртуализации" (см. стр.**88**).

   Пояснение. При добавлении сервера SCVMM в список защищаемых серверов на него будет автоматически установлен компонент защиты vGate.

5. Если серверы Hyper-V объединены в кластер и для управления кластером используется Failover Cluster Manager (FCM), добавьте в список защищаемых серверов точку доступа к кластеру и все серверы, входящие в кластер. Для этого используйте кнопку "Сервер виртуализации" (см. стр. **88**). Агент аутентификации будет установлен только на серверах Hyper-V.

   Примечание. Если в сети администрирования виртуальной инфраструктуры кроме серверов SCVMM и Hyper-V имеются другие серверы и устройства, требующие управления (например, система хранения данных и т. д.), их также нужно добавить в список защищаемых серверов, используя кнопку "Автономный сервер".

6. Повторите действия **3**, **5** для всех защищаемых серверов Hyper-V и кластеров серверов.
7. Выберите функцию "Учетные записи" и создайте учетные записи для пользователей vGate. Если сервер авторизации vGate входит в домен, добавьте учетные записи пользователей и компьютеров из Active Directory, которым следует предоставить доступ к защищаемым объектам (см. стр.**90**).
8. Выберите функцию "Защищаемые серверы" и настройте для каждого пользователя необходимые правила доступа к компонентам управления виртуальной инфраструктурой (см. стр.**115**).

Внимание! После предоставления пользователям доступа к защищаемым серверам необходимо перевести vGate из тестового в штатный режим работы (см. стр.**85**).

9. Настройте остальные функции при необходимости.

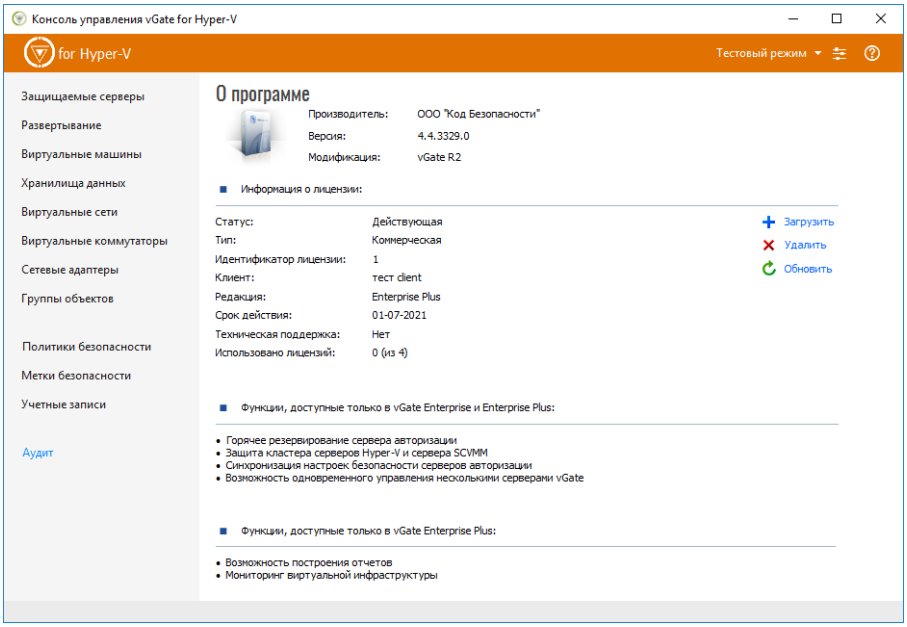
Регистрация лицензии

Для ознакомления с ПО vGate в демонстрационном режиме необходим ключ активации (см. раздел "Правила использования лицензий" в документе [1]). Демонстрационный режим работы vGate поддерживает выполнение всех функций, доступных в редакции Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]) без ограничений. Для полноценной работы vGate по истечении демонстрационного периода следует приобрести лицензию и зарегистрировать полученный ключ активации. Подробнее о правилах использования лицензий см. в документе [1].

Для регистрации лицензии:

1. Нажмите кнопку  в области главного меню консоли управления.

   На экране будет отображена информация о действующей лицензии.



2. Чтобы зарегистрировать лицензию, необходимо загрузить ключ активации. Для этого нажмите кнопку-ссылку "Загрузить" и выберите нужный файл.

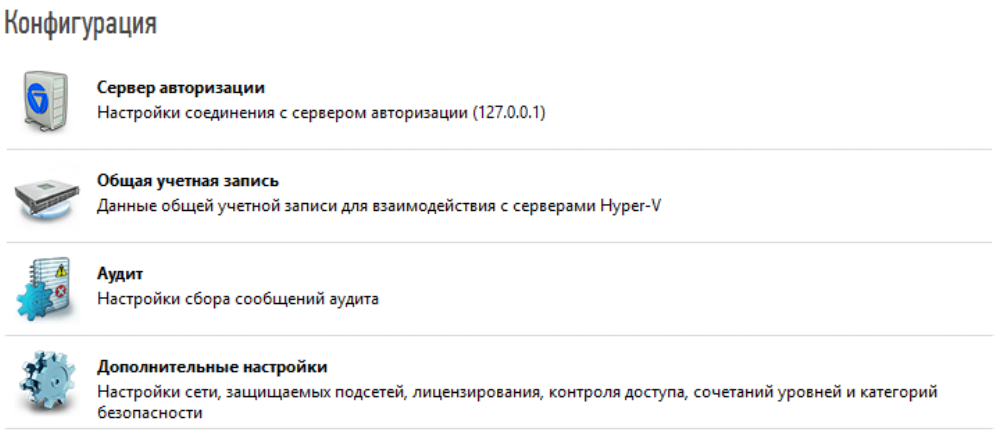
Примечание. Чтобы обновить информацию о лицензии, нажмите кнопку-ссылку "Обновить". Для удаления лицензионного ключа используется кнопка-ссылка "Удалить".

Настройка конфигурации

В области главного меню консоли управления нажмите кнопку .

В области параметров будут отображены заголовки и краткое описание групп параметров конфигурации.

Совет. Нажмите на заголовок, чтобы открыть группу. Для редактирования значений параметров используйте ссылки-заголовки подразделов или кнопки-ссылки в правой части области параметров.



Изменить некоторые параметры сетевой конфигурации сервера авторизации, в том числе адрес внешнего сетевого адаптера, средствами консоли управления нельзя. Для этого нужно выполнить переустановку сервера в режиме изменения (см. стр.**53**).

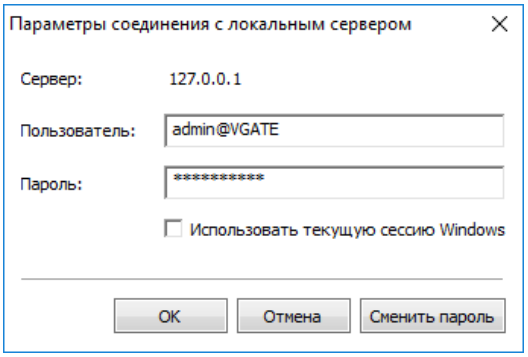
Повторное подключение к серверу авторизации

В случае появления на экране сообщений о потере связи с сервером авторизации или принудительном разрыве соединения рекомендуется выполнить повторное подключение к серверу авторизации. Повторное подключение к серверу авторизации может также потребоваться в случае необходимости изменить параметры соединения с сервером авторизации.

Для повторного подключения к серверу авторизации:

1. В разделе "Конфигурация" откройте группу параметров "Сервер авторизации".
2. В области параметров нажмите кнопку-ссылку "Переподключение".

   На экране появится диалог для ввода параметров соединения.



3. Укажите пароль администратора информационной безопасности, при необходимости измените остальные параметры соединения и нажмите кнопку "ОК".

Параметр	Описание
Пользователь	Имя учетной записи администратора информационной безопасности
Пароль	Пароль администратора информационной безопасности
Использовать текущую сессию Windows	Отметьте это поле, чтобы использовать учетные данные пользователя Windows (если сервер авторизации vGate входит в домен)

Совет. Для изменения пароля АИБ нажмите кнопку "Сменить пароль".

Изменение роли сервера

Если необходимо назначить сервер авторизации резервным, а резервный сервер основным (например, при сбое основного сервера), можно произвести смену ролей серверов из консоли управления, установленной на сервере авторизации.

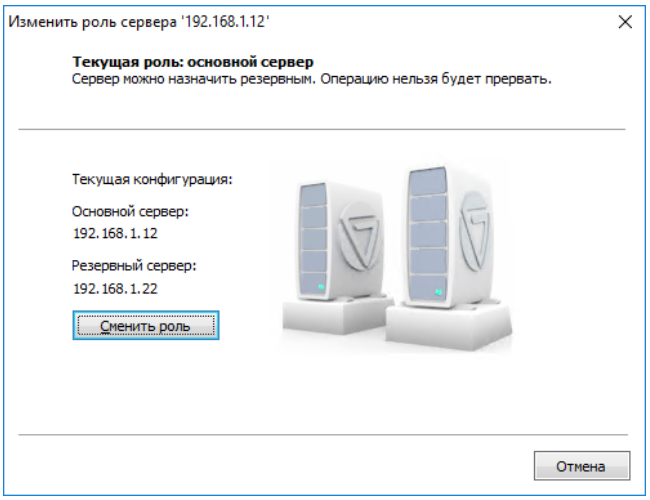
Функция резервирования сервера авторизации доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Внимание! Для выполнения смены ролей серверов необходимо, чтобы консоль управления была установлена на основном и резервном серверах авторизации. Операция недоступна для выполнения с помощью консоли управления, установленной на отдельном рабочем месте АИБ.

Для изменения роли сервера:

1. В разделе "Конфигурация" откройте группу параметров "Сервер авторизации".
2. В области параметров нажмите кнопку-ссылку "Назначить резервным".

   Откроется окно с информацией о текущей конфигурации.



3. Нажмите кнопку "Сменить роль", а затем кнопку "ОК" в появившемся окне.
4. Для завершения операции запустите консоль управления на резервном сервере авторизации.

   Роли серверов будут изменены (см. стр.**55**).

Настройка горячего резервирования

Резервирование в vGate включает в себя возможность автоматического переключения на резервный сервер авторизации в случае сбоя основного сервера.

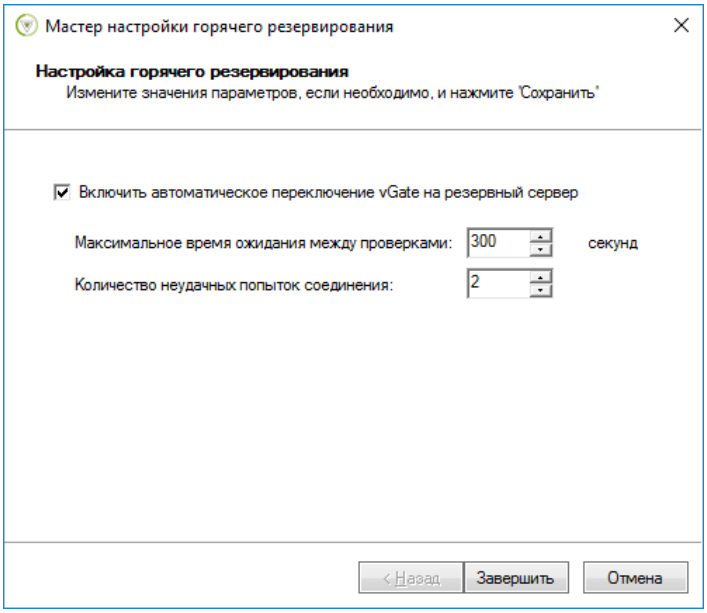
Функция резервирования сервера авторизации доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Внимание! Для доступа к функции горячего резервирования необходимо ввести в эксплуатацию резервный сервер авторизации (см. стр.55).

Для настройки горячего резервирования:

1. В разделе "Конфигурация" откройте группу параметров "Сервер авторизации".
2. В области параметров нажмите кнопку-ссылку "Настройка".

   Откроется окно мастера настройки горячего резервирования.



3. Настройте параметры горячего резервирования и нажмите "Сохранить".

Параметр	Описание
Включить автоматическое переключение vGate на резервный сервер	Отметьте данный пункт, чтобы включить опцию автоматического переключения управления на резервный сервер авторизации в случае сбоя основного сервера
Максимальное время ожидания между проверками (секунд)	Укажите интервал времени для проверки связи между серверами авторизации. Минимальное время — 120 секунд
Количество неудачных попыток соединения	Укажите количество неудачных попыток соединения между серверами авторизации, после которого производится автоматический перевод управления на резервный сервер

4. Настройки горячего резервирования будут сохранены.

   Функция автоматического переключения будет работать только в случае, если в списке защищаемых серверов на основном сервере авторизации есть серверы виртуализации.

Изменение параметров соединения с сервером виртуализации

- Если для управления виртуальной инфраструктурой используется SCVMM, то указываются параметры соединения с ним.
- Если в виртуальной инфраструктуре используется несколько серверов Hyper-V, то для того, чтобы установить на них агент защиты сервера Hyper-V и добавить их в список защищаемых серверов, потребуется последовательно выполнить соединение с каждым из серверов (см. стр.**65**). Если для соединения с серверами используется одна и та же учетная запись пользователя домена, ее данные можно сохранить в параметре "Общая учетная запись". В этом случае при установлении соединения с каждым новым сервером Hyper-V не потребуется повторно вводить учетные данные.
- Если серверы Hyper-V объединены в кластер и для управления кластером используется Failover Cluster Manager, то в список защищаемых серверов нужно добавить кластер серверов, а затем серверы Hyper-V.

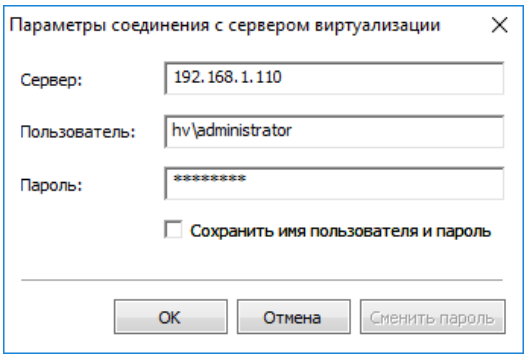
Примечание. Если серверы Hyper-V не включены в домен Active Directory и для соединения с ними нельзя использовать общую учетную запись доменного пользователя, то на каждом сервере Hyper-V можно создать специальную учетную запись пользователя с одинаковыми для всех серверов Hyper-V именем и паролем. Данную учетную запись следует добавить в группу локальных администраторов на каждом сервере Hyper-V и указать при настройке параметров соединения с сервером виртуализации.

Внимание! Данный механизм неприменим в случае, если на сервере Hyper-V включен контроль учетных записей (UAC, User Account Control). Необходимо отключить контроль учетных записей на сервере Hyper-V либо использовать для соединения с ним учетную запись локального администратора, используемую по умолчанию.

Для изменения параметров соединения:

1. В разделе "Конфигурация" откройте группу параметров "Общая учетная запись".
2. В области параметров нажмите кнопку-ссылку "Изменить".

   На экране появится диалог изменения параметров соединения.



3. Укажите полное доменное имя или IP-адрес сервера Hyper-V или SCVMM, а также имя и пароль администратора данного сервера.

   Совет. Отметьте поле "Сохранить имя пользователя и пароль", чтобы сохранить параметры общей учетной записи. Эти параметры будут использоваться в дальнейшем при запуске консоли управления текущим пользователем на данном компьютере. В противном случае введенные учетные данные будут использованы только в рамках текущей сессии работы в консоли управления. При повторном запуске консоли управления будет действовать учетная запись, параметры которой были сохранены ранее.

4. Нажмите кнопку "ОК" в окне редактирования параметров соединения.

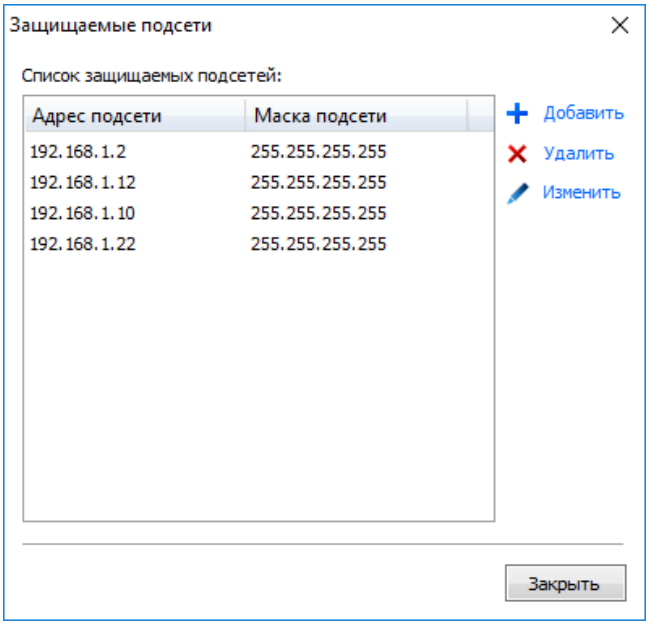
Добавление защищаемых подсетей

Если маршрутизацию трафика в сети выполняет сервер авторизации vGate, то в случае появления в конфигурации сети новых подсетей необходимо добавить их в список защищаемых.

Для добавления подсети:

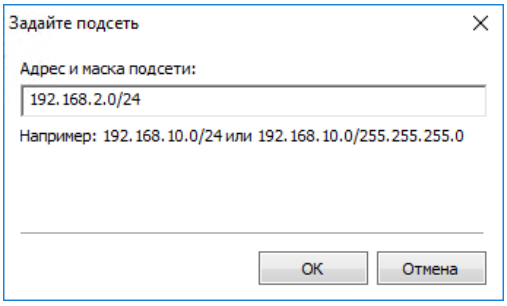
1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Защищаемые подсети".

   На экране появится следующий диалог.



3. Нажмите кнопку-ссылку "Добавить".

   Откроется диалог для добавления защищаемых подсетей.



4. Укажите подсеть и нажмите кнопку "ОК".

Чтобы отредактировать подсеть, выберите ее в списке и нажмите кнопку-ссылку "Изменить". Чтобы удалить подсеть из списка защищаемых, нажмите кнопку-ссылку "Удалить".

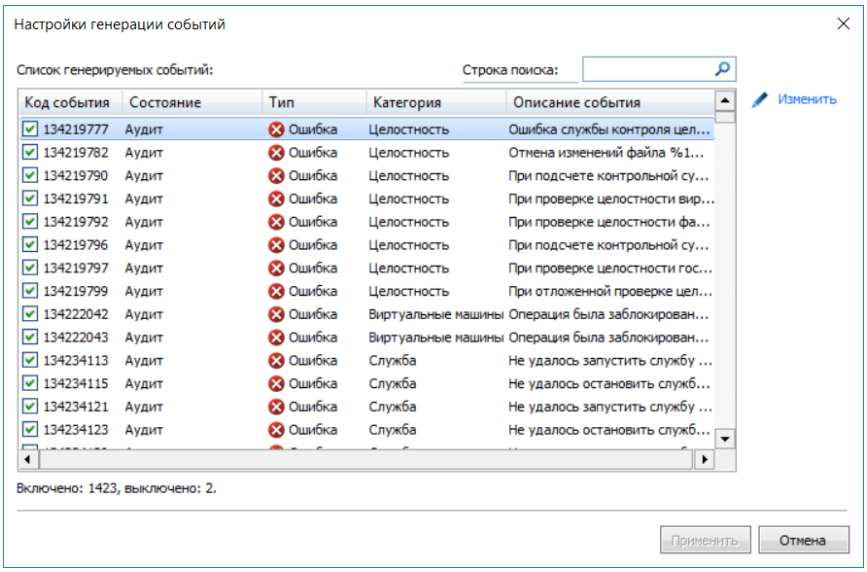
Настройка аудита событий

По умолчанию производится аудит всех событий безопасности vGate. При необходимости можно выбрать события, аудит которых осуществлять не надо.

Для настройки аудита событий:

1. В разделе "Конфигурация" откройте группу параметров "Аудит".
2. В области параметров нажмите кнопку-ссылку "Настройки сбора сообщений".

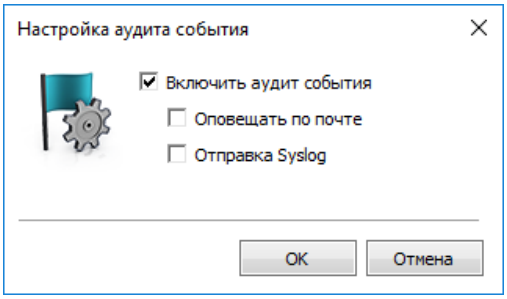
На экране появится следующий диалог.



Чтобы выполнить поиск по всем полям таблицы, используйте поле "Строка поиска".

3. Настройте список регистрируемых событий. Для отмены регистрации какого-либо события удалите отметку слева от кода нужного события. Для включения регистрации какого-либо события установите отметку слева от кода нужного события.
4. Для настройки аудита события выделите его в списке и нажмите кнопку-ссылку "Изменить".

   На экране появится следующий диалог.



5. Укажите параметры аудита событий и нажмите кнопку "ОК".

Параметр	Описание
Включить аудит события	Включение регистрации выбранного события
Оповещать по почте	Включение отправки оповещений по почте о данном событии аудита. О настройке отправки почтовых уведомлений читайте на стр.**72**
Отправка Syslog	Включение отправки выбранного сообщения аудита на сервер Syslog

Настройка отправки уведомлений о событиях по SMTP

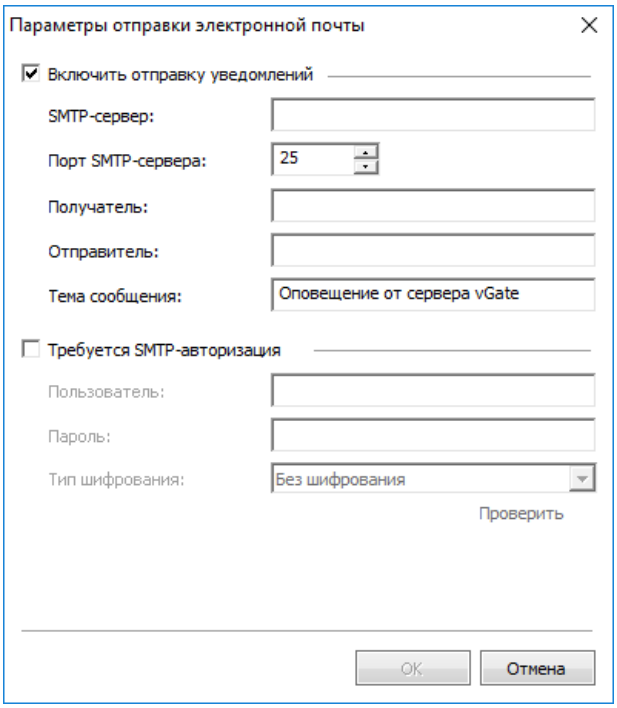
vGate позволяет настроить отправку почтовых уведомлений о событиях аудита по протоколу SMTP.

Для настройки отправки уведомлений:

1. В разделе "Конфигурация" откройте группу параметров "Аудит".

2. В области параметров нажмите кнопку-ссылку "Настройка уведомлений о событиях по протоколу SMTP".

   На экране появится следующий диалог.



3. Для включения отправки уведомлений отметьте поле "Включить отправку уведомлений".
4. Укажите адрес SMTP-сервера и проверьте параметры для отправки уведомлений.

Параметр	Описание
SMTP-сервер	Сетевое имя или IP-адрес SMTP-сервера
Порт SMTP-сервера	Порт SMTP-сервера (по умолчанию 25)
Получатель	Адрес получателя. При указании нескольких получателей в качестве разделителя между адресами используется символ ";"
Отправитель	Адрес отправителя
Тема сообщения	По умолчанию "Оповещение от сервера vGate"

5. Если для доступа на указанный SMTP-сервер требуется авторизация, отметьте поле "Требуется SMTP-авторизация" и укажите аутентификационные данные пользователя.

Параметр	Описание
Пользователь	Имя пользователя
Пароль	Пароль пользователя для доступа к SMTP-серверу
Тип шифрования	Тип шифрования, используемый при авторизации

Для проверки отправки уведомлений нажмите кнопку-ссылку "Проверить".

6. Нажмите кнопку "ОК".

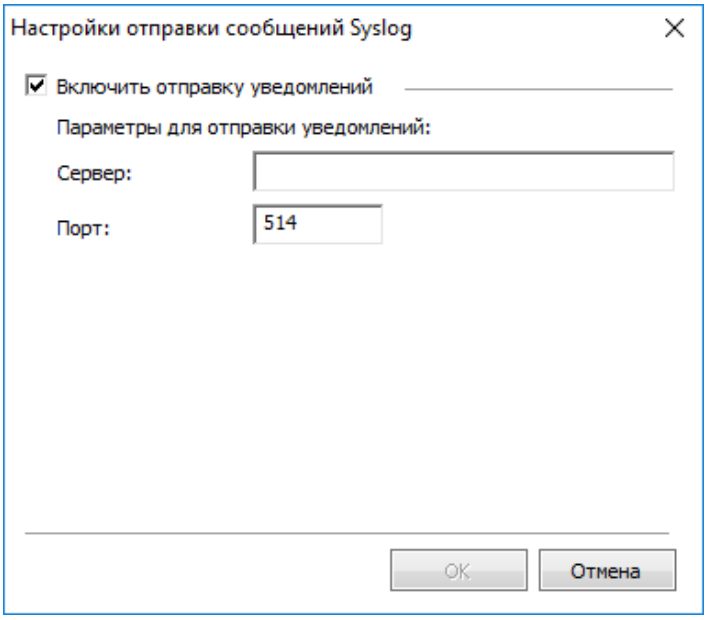
Настройка отправки уведомлений о событиях по протоколу Syslog

vGate поддерживает передачу уведомлений о событиях безопасности из журналов vGate по протоколу Syslog.

Для включения отправки уведомлений:

1. В разделе "Конфигурация" откройте группу параметров "Аудит".
2. В области параметров нажмите кнопку-ссылку "Настройка уведомлений о событиях по протоколу Syslog".

   На экране появится следующий диалог.



3. Для включения отправки уведомлений по протоколу Syslog отметьте поле "Включить отправку уведомлений".
4. Укажите параметры отправки уведомлений и нажмите кнопку "ОК".

Параметр	Описание
Сервер	Имя или IP-адрес сервера Syslog
Порт	Порт сервера Syslog

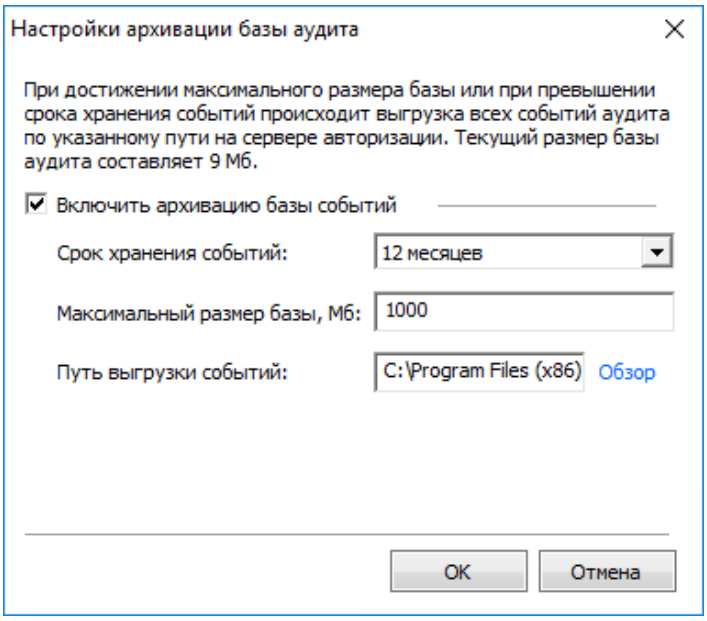
Настройка архивации базы аудита

При достижении максимального размера базы событий аудита или при превышении срока хранения сообщений возможна выгрузка всех событий аудита в выбранный каталог на сервере авторизации.

Для настройки архивации:

1. В разделе "Конфигурация" откройте группу параметров "Аудит".
2. В области параметров нажмите кнопку-ссылку "Настройки архивации базы аудита".

На экране появится следующий диалог.



3. Для включения архивации отметьте поле "Включить архивацию базы событий".
4. Укажите параметры архивации базы событий и нажмите кнопку "ОК".

Параметр	Описание
Срок хранения событий	Срок хранения событий аудита, при превышении которого будет произведена архивация базы событий
Максимальный размер базы, Мб	Размер базы, при превышении которого будет произведена архивация
Путь выгрузки событий	Путь к каталогу для сохранения архива событий аудита

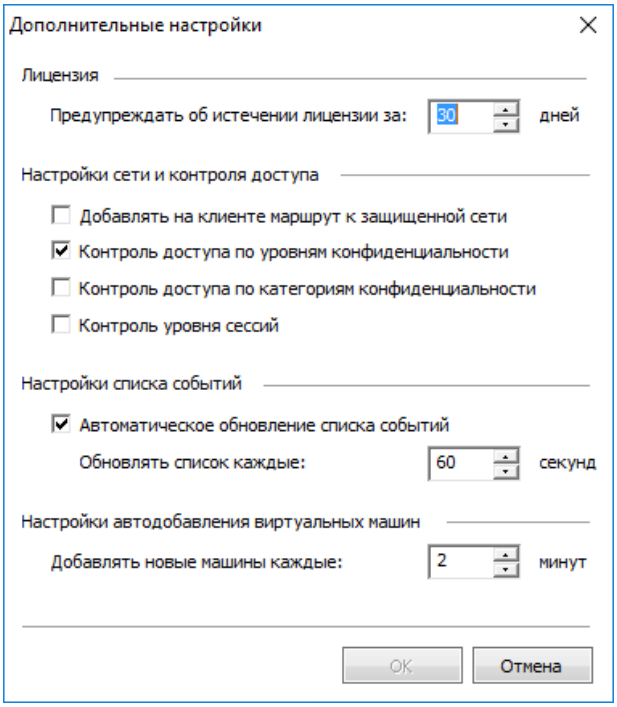
Изменение периода предупреждения об истечении лицензии

По умолчанию предупреждение об истечении срока действия лицензии выдается за тридцать дней до наступления этого события. При необходимости можно изменить это значение.

Для изменения периода предупреждения:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Настройки сети, контроля доступа, лицензирования".

   На экране появится диалог настройки дополнительных параметров.



3. В поле "Предупреждать об истечении лицензии за" укажите, за сколько дней до истечения лицензии необходимо предупреждать об этом событии, и нажмите кнопку "ОК".

Добавление маршрута к защищенной сети

Чтобы АВИ со своих рабочих мест могли получить доступ к элементам управления виртуальной инфраструктурой, размещенным в защищаемом периметре, должны быть определенным образом настроены правила маршрутизации. Один из вариантов настройки маршрутизации подразумевает добавление маршрута к защищенной сети на рабочие места АВИ с сервера авторизации в момент запуска службы аутентификации vGate, после чего маршрут записывается в локальную таблицу маршрутизации ПК.

Подробнее о вариантах настройки маршрутизации см. стр.**11**.

Для добавления маршрута к защищенной сети:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Настройки сети, контроля доступа, лицензирования".

   На экране появится диалог настройки дополнительных параметров.
3. Отметьте поле "Добавлять на клиенте маршрут к защищенной сети" и нажмите кнопку "ОК".

Включение контроля доступа по категориям и уровням конфиденциальности

Категории и уровни конфиденциальности используются для полномочного управления доступом (см. стр.**120**). При необходимости контроль доступа по уровням конфиденциальности можно отключить.

Для включения контроля доступа:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Настройки сети, контроля доступа, лицензирования".

На экране появится диалог настройки дополнительных параметров.

3. Для включения контроля доступа по категориям конфиденциальности отметьте поле "Контроль доступа по категориям конфиденциальности" и нажмите кнопку "ОК".

Примечание. Для отключения контроля доступа по уровням конфиденциальности удалите отметку из поля "Контроль доступа по уровням конфиденциальности" и нажмите кнопку "ОК".

Включение контроля уровня сессий

По умолчанию сессия работы пользователя в защищенной среде получает такой же уровень конфиденциальности, как уровень конфиденциальности, назначенный пользователю. При этом пользователь может выполнять операции с ресурсами такого же или меньшего уровня конфиденциальности. Примеры см. в документе [1]).

При необходимости всем пользователям vGate может быть предоставлена возможность контролировать (выбирать) уровень сессии в агенте аутентификации. 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.

Для включения контроля уровня сессии:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Настройки сети, контроля доступа, лицензирования".

   На экране появится диалог настройки дополнительных параметров.
3. Для включения контроля уровня сессий отметьте поле "Контроль уровня сессий" и нажмите кнопку "ОК".

Примечание. Для отключения контроля уровня сессий повторите действия **1**, **2**, удалите отметку из поля "Контроль уровня сессий" и нажмите кнопку "ОК".

Перечень основных операций с конфиденциальными ресурсами и условия их выполнения при использовании механизма контроля уровня сессий приведены на стр.**166**.

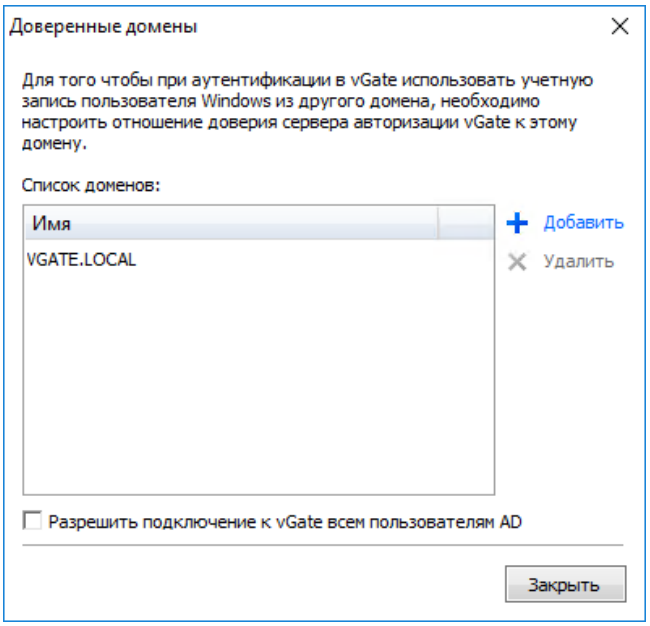
Добавление доверенных доменов

По умолчанию в список пользователей vGate можно добавить учетные записи из домена, в который входит сервер авторизации. Кроме того, можно настроить добавление учетных записей из других доменов этого же леса. Для этого необходимо добавить такие домены в список доверенных в консоли управления.

Для добавления домена:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите ссылку "Доверенные домены".

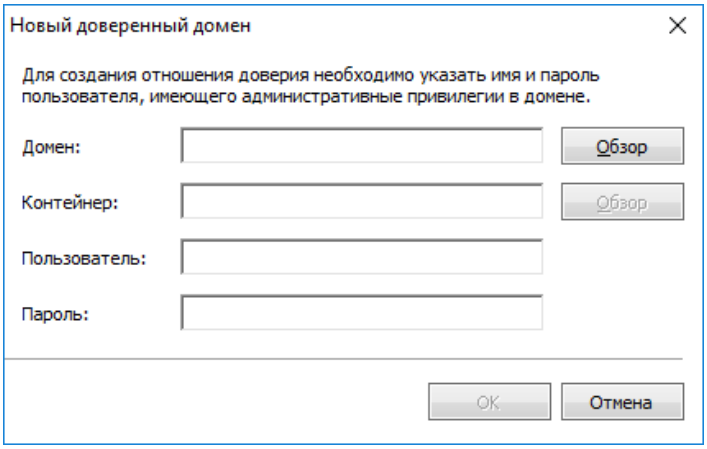
На экране появится диалог для добавления и удаления доверенных доменов.



Примечание. Чтобы разрешить вход в vGate с помощью агента аутентификации пользователям Active Directory, которые не имеют учетных записей в vGate , отметьте параметр "Разрешить подключение к vGate всем пользователям AD".

3. Нажмите кнопку-ссылку "Добавить".

Откроется диалог для ввода параметров нового доверенного домена.



4. Укажите параметры нового доверенного домена и нажмите кнопку "ОК".

Параметр	Описание
Домен	Название домена Active Directory
Контейнер	Название организационного подразделения (OU) в домене Active Directory, предназначенного для хранения служебных учетных записей vGate
Пользователь	Имя пользователя, обладающего административными привилегиями в домене
Пароль	Пароль пользователя, обладающего административными привилегиями в домене

Совет.

- Для выбора домена и контейнера из списка нажмите кнопку "Обзор" рядом с соответствующим полем.
- Чтобы удалить домен из списка доверенных доменов, выберите его в списке и нажмите кнопку-ссылку "Удалить".

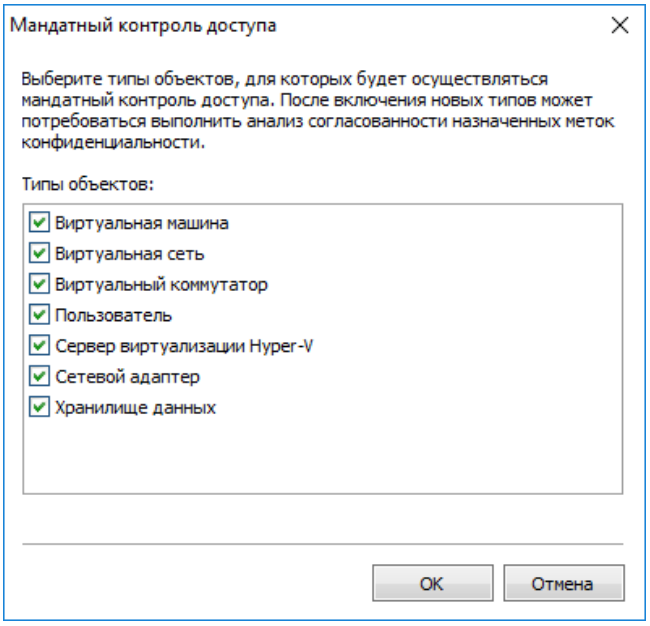
Настройка полномочного управления доступом по типам объектов

vGate предоставляет возможность определить перечень типов объектов, в отношении которых действует механизм полномочного управления доступом. По умолчанию контроль соответствия меток безопасности включен для всех объектов — пользователей, серверов виртуализации Hyper-V, виртуальных машин, виртуальных сетей, распределенных виртуальных коммутаторов, сетевых адаптеров и хранилищ данных. При необходимости можно отключить мандатный контроль доступа для выбранных объектов.

Для настройки полномочного управления доступом:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Настройка мандатного доступа по типам объектов".

   На экране появится диалог выбора типов объектов.



3. Отметьте типы объектов, для которых будет действовать механизм полномочного управления доступом (будет проверяться соответствие меток безопасности), и нажмите кнопку "OK".

Экспорт и импорт конфигурации vGate

Внимание! Выполнение экспорта и импорта конфигурации в консоли управления возможно, только если консоль управления запущена с использованием данных учетной записи главного АИБ.

В консоли управления можно выполнить экспорт и импорт конфигурации vGate 4.4. Конфигурация сохраняется в файле формата XML и может быть использована для восстановления настроек текущего сервера авторизации.

Файл конфигурации содержит информацию о следующих объектах:

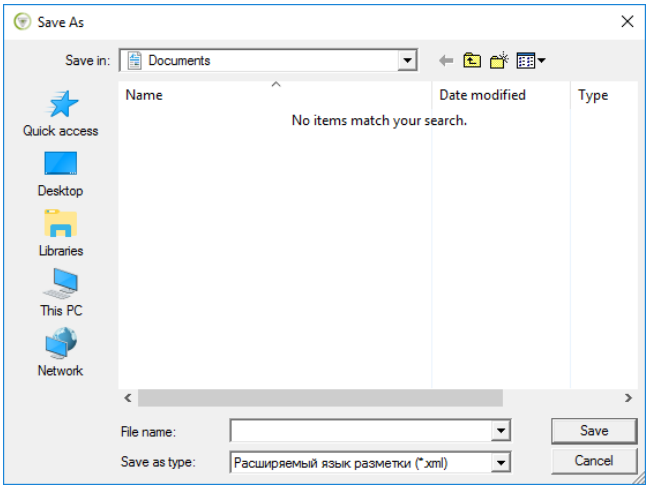
- общая информация о системе (версия vGate, режим работы);
- настроенные наборы политик безопасности;
- настроенные уровни и категории конфиденциальности;
- настроенные правила корреляции для мониторинга;
- созданные группы и объекты, добавленные в них;
- защищаемые серверы и правила разграничения доступа к ним;

- объекты виртуальной инфраструктуры (виртуальные машины, сетевые адаптеры, хранилища данных, виртуальные сети, виртуальные коммутаторы) и назначенные им метки безопасности;
- учетные записи пользователей, их параметры и назначенные метки безопасности;
- общие настройки vGate (матрица допустимых сочетаний уровней и категорий конфиденциальности, настройки сети, контроля доступа, лицензирования и мандатного доступа, защищаемые подсети);
- настройки аудита.

Для экспорта конфигурации:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Экспорт конфигурации".

   На экране появится диалог сохранения файла конфигурации.



3. Выберите путь к папке для сохранения файла конфигурации, задайте имя файла и нажмите кнопку "Сохранить" ("Save").

   Конфигурация vGate будет сохранена в файле формата XML.

Для импорта конфигурации:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Импорт конфигурации".

   На экране появится диалог выбора файла конфигурации.
3. Выберите файл конфигурации vGate и нажмите кнопку "Открыть" ("Open").

   Конфигурация vGate будет обновлена.

Внимание! Импорт конфигурации vGate производится в фоновом режиме. Для корректного обновления настроек необходимо приостановить работу с программой, иначе некоторые изменения могут быть утеряны.

Примечание. Отметьте пункт "Перезаписывать конфликтующую информацию", чтобы заменить всю информацию о существующих объектах информацией об объектах с таким же именем или идентификатором из импортируемого файла конфигурации.

Внимание! Импортируемые настройки не будут восстановлены на серверах, добавленных в список защищаемых объектов в консоли управления vGate, если не отмечен пункт "Перезаписывать конфликтующую информацию".

Внимание! Если отмечен пункт "Перезаписывать конфликтующую информацию", новым учетным записям, не принадлежащим Active Directory, при импорте назначаются свойства "Учетная запись отключена" и "Сменить пароль при следующем входе в систему". Если пункт "Перезаписывать конфликтующую информацию" не отмечен, эти свойства назначаются всем импортируемым учетным записям, не принадлежащим Active Directory.

Синхронизация настроек серверов авторизации

vGate поддерживает одновременную работу нескольких серверов авторизации. Администратор vGate может выполнить синхронизацию настроек серверов авторизации в консоли управления на рабочем месте АИБ.

Функция синхронизации настроек серверов авторизации доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Внимание!
Лицензия vGate Enterprise или Enterprise Plus должна быть зарегистрирована на всех серверах авторизации.

Примечание. Запуск синхронизации из консоли управления на сервере авторизации vGate невозможен.

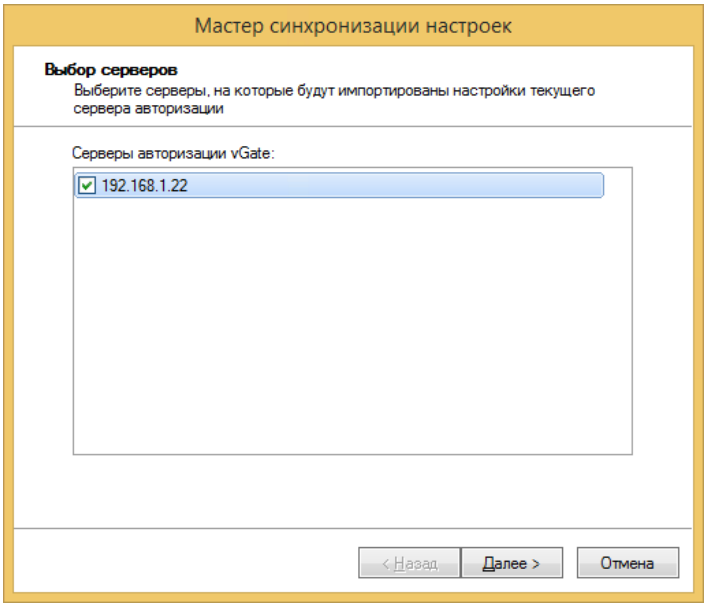
При запуске мастера синхронизации настроек выполняется проверка параметров лицензий на серверах авторизации, к которым подключен агент аутентификации. Для корректной работы мастера необходимо выполнение следующих условий:

- наличие ключа активации vGate Enterprise, Enterprise Plus или демонстрационной версии vGate на всех серверах авторизации;
- суммарное количество физических процессоров (sockets) на серверах виртуализации не превышает значение, заданное в лицензии. Данное условие проверяется только в случае совпадения идентификаторов лицензий на серверах авторизации.

Для синхронизации настроек серверов:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Синхронизация объектов".

   На экране появится окно мастера синхронизации настроек серверов авторизации.

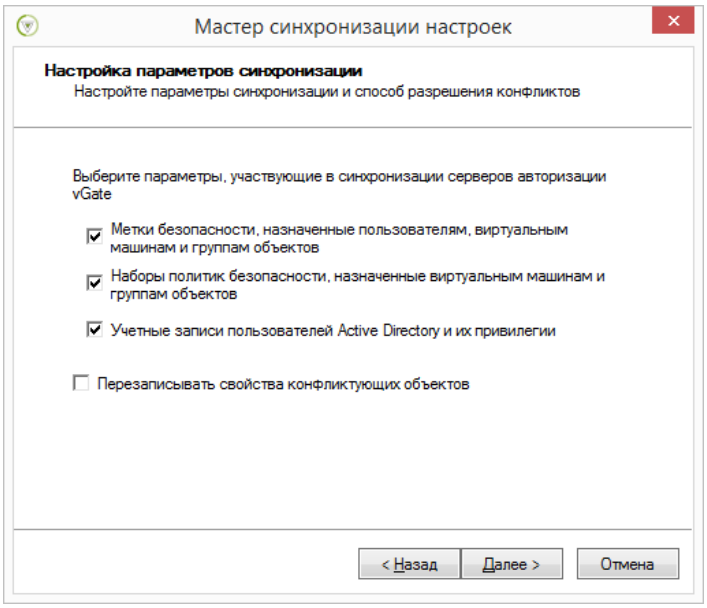


В списке серверов авторизации vGate находятся те серверы, к которым выполнено подключение агента аутентификации.

Внимание! Рекомендуется выполнить подключение к серверам авторизации, на которых будет производиться синхронизация данных, с помощью учетной записи главного АИБ. Иначе возможна потеря данных при переносе учетных записей с правом "Оператор учетных записей". В этом случае все учетные записи Active Directory будут импортированы, но настройки прав доступа для них будут утеряны.

3. Выберите из списка серверы, настройки которых будут синхронизированы с настройками текущего сервера авторизации, и нажмите кнопку "Далее".

   На экране появится диалог настройки параметров синхронизации.



4. Укажите настройки, которые необходимо импортировать на выбранные серверы авторизации, и нажмите "Далее".

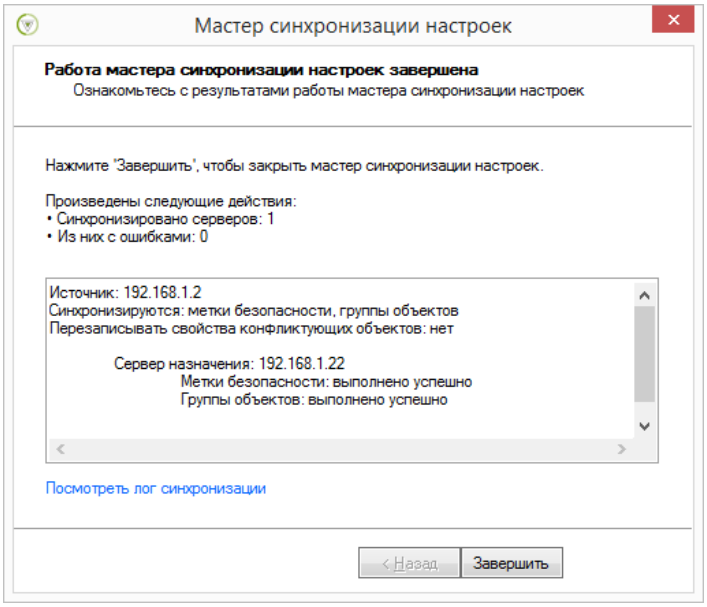
Параметр	Описание
Метки безопасности, назначенные пользователям, виртуальным машинам и группам объектов	Отметьте поле, чтобы синхронизировать: • категории конфиденциальности; • уровни конфиденциальности; • ассоциации категорий конфиденциальности с группами объектов, виртуальными машинами и пользователями Active Directory; • ассоциации уровней конфиденциальности с группами объектов, виртуальными машинами и пользователями Active Directory
Наборы политик безопасности, назначенные виртуальным машинам и группам объектов	Отметьте поле, чтобы синхронизировать наборы политик безопасности и их связи с виртуальными машинами и группами объектов. Следующие политики безопасности всегда синхронизируются выключенными, так как имеют специфичные для каждого сервера авторизации настройки (например, IP-адреса): • "Доверенная загрузка виртуальных машин Hyper-V"; • "Синхронизация времени". После синхронизации нужно произвести настройку данных политик вручную
Учетные записи пользователей Active Directory и их привилегии	Отметьте поле, чтобы синхронизировать учетные записи пользователей Active Directory и их привилегии

Параметр	Описание
Перезаписывать свойства конфликтующих объектов	Отметьте поле, чтобы перезаписывать свойства идентичных объектов при синхронизации. Идентичные объекты — объекты, имеющие одинаковые идентификаторы (для ВМ, пользователей Active Directory и уровней конфиденциальности) или имя (для категорий конфиденциальности и наборов политик безопасности)

Внимание! Если на синхронизируемых серверах авторизации есть идентичные ВМ или пользователи, то при синхронизации необходимо отметить пункт "Перезаписывать свойства конфликтующих объектов", чтобы импортировать все метки безопасности данных объектов.

Внимание! Если синхронизируемые серверы авторизации контролируют разные виртуальные инфраструктуры, то операция миграции виртуальных машин между ними может быть заблокирована vGate, если целевой сервер виртуализации не добавлен в список защищаемых серверов. Для миграции виртуальных машин на сервер, не добавленный в список защищаемых vGate, необходимо временно отключить контроль доступа по уровням и категориям конфиденциальности (см. стр.76). Также необходимо отключить политику "Запрет миграции виртуальных машин Hyper-V", если для ее назначения на ВМ не было веских оснований.

5. Настройки серверов авторизации будут синхронизированы. По окончании процесса синхронизации на экране появится окно с результатами операции.



6. Чтобы просмотреть подробный отчет о процессе синхронизации, нажмите кнопку-ссылку "Посмотреть лог синхронизации".

Управление режимами работы vGate

Помимо штатного режима работы в vGate предусмотрены дополнительные режимы для ослабления контроля за администрированием виртуальной инфраструктуры в служебных целях.

Режим	Описание
Штатный режим	В данном режиме могут использоваться все функциональные возможности vGate по защите виртуальной инфраструктуры. Режим должен быть включен для обеспечения полноценной защиты
Тестовый режим	Данный режим позволяет выполнить ввод в эксплуатацию или настройку конфигурации vGate, не ограничивая работу существующей сетевой инфраструктуры. Обеспечивает доступ к серверам виртуальной инфраструктуры вне зависимости от настроенных в vGate правил разграничения доступа. Режим включен по умолчанию только после первоначальной установки vGate (см. ниже)
Аварийный режим	Режим предназначен для приостановки защиты в случае выхода из строя элементов ИТ-инфраструктуры. Позволяет обойти установленные vGate ограничения доступа к администрированию виртуальной среды на время восстановления работоспособности инфраструктуры (см. стр.**86**). В отличие от штатного и тестового режимов работы, в аварийном режиме не регистрируются события безопасности

Тестовый режим

Внимание! Для полноценной защиты виртуальной инфраструктуры необходимо перевести vGate в штатный режим работы после настройки правил разграничения доступа к защищаемым серверам.

По умолчанию после первоначальной установки и настройки vGate работает в тестовом режиме. Данный режим обеспечивает доступ к серверам виртуальной инфраструктуры с рабочих мест АВИ и АИБ без предварительной настройки правил разграничения доступа и позволяет выполнить ввод в эксплуатацию или настройку конфигурации vGate, не ограничивая работу существующей сетевой инфраструктуры.

Особенности работы vGate в тестовом режиме:

- Для аутентифицированных пользователей vGate разрешены подключения ко всем серверам, размещенным внутри защищаемого периметра сети администрирования, с любого компьютера по всем протоколам и портам.
- Для пользователей, не прошедших процедуру аутентификации в vGate, разрешен доступ ко всем серверам из защищаемого периметра по протоколу ICMP (команда ping).

  Для просмотра перечня ПРД, обеспечивающих работу vGate в тестовом режиме, можно воспользоваться утилитой drvmgr.exe (стр.**163**).
- При наличии ПРД, настроенных в консоли управления vGate, доступ пользователей vGate к защищаемым серверам обеспечивается в соответствии с этими правилами.
- Доступ к выполнению операций с объектами виртуальной инфраструктуры контролируется в соответствии с настроенными метками безопасности (механизм полномочного управления доступом действует как в штатном режиме).
- События установления соединений с серверами из защищаемого периметра регистрируются в журнале событий безопасности vGate.
- Поддерживается доверенная загрузка ВМ (политика "Доверенная загрузка виртуальных машин" действует как в штатном режиме).
- Включается правило фильтрации, разрешающее весь трафик виртуальных машин. Правило имеет минимальный приоритет.

После завершения редактирования списка защищаемых серверов и настройки правил разграничения доступа к защищаемым серверам необходимо перевести vGate в штатный режим работы.

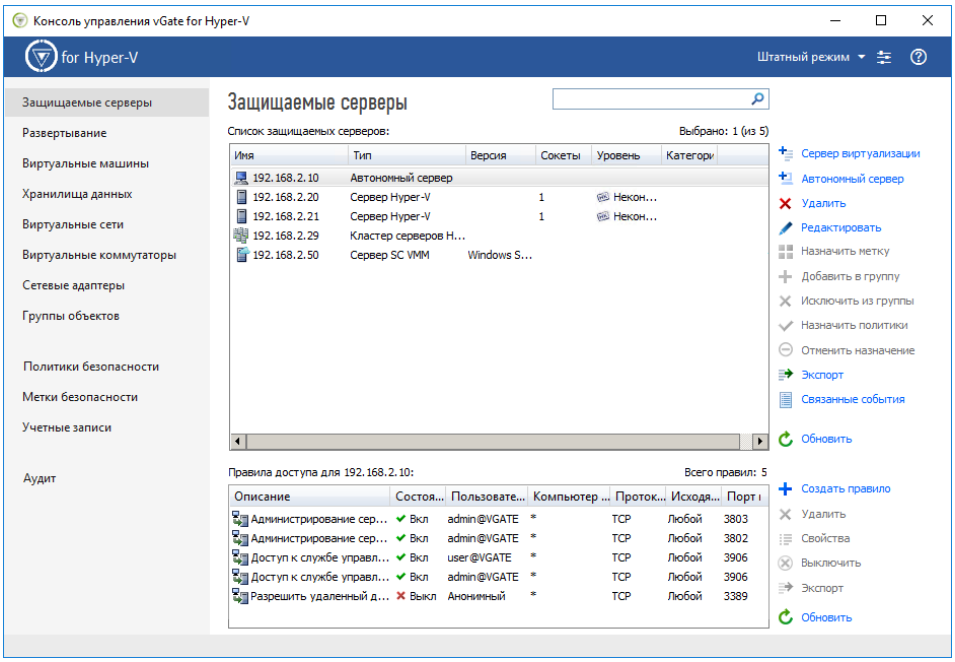
Для переключения vGate в штатный режим:

1. В области главного меню консоли управления нажмите кнопку-ссылку "Тестовый режим" и выберите в раскрывающемся списке вариант "Штатный режим".

   На экране появится предупреждение о переключении vGate в штатный режим.

2. Нажмите кнопку-ссылку "Продолжить" в окне предупреждения.

   Штатный режим работы vGate будет включен. Соответствующее сообщение появится в виде кнопки-ссылки в области главного меню консоли управления.



Контроль доступа пользователей к серверам виртуальной инфраструктуры в штатном режиме будет осуществляться в соответствии с правилами, созданными администратором в консоли управления vGate (подробнее об управлении доступом к защищаемым серверам см. стр.**115**).

При необходимости (например, для смягчения контроля доступа к серверам в защищаемом периметре в случае реорганизации виртуальной инфраструктуры) vGate может быть вновь переведен в тестовый режим работы.

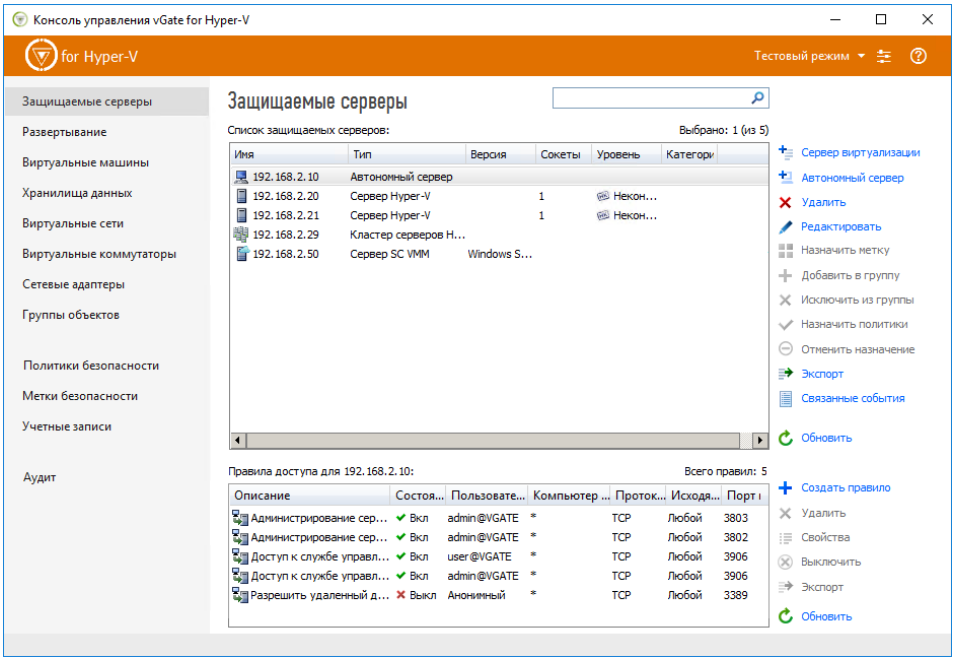
Для переключения vGate в тестовый режим:

1. В области главного меню консоли управления нажмите кнопку-ссылку "Штатный режим" и выберите в раскрывающемся списке вариант "Тестовый режим".

   На экране появится предупреждение о переключении vGate в тестовый режим.

2. Нажмите кнопку-ссылку "Продолжить" в окне предупреждения.

   Тестовый режим будет включен. Область главного меню консоли управления будет окрашена в оранжевый цвет. Ссылка с названием текущего режима работы vGate изменит название на "Тестовый режим".



Аварийный режим

Внимание! Для полноценной защиты виртуальной инфраструктуры необходимо перевести vGate в штатный режим работы после восстановления работоспособности инфраструктуры.

Аварийный режим предназначен для приостановки защиты в случае выхода из строя элементов ИТ-инфраструктуры. Данный режим позволяет администратору обойти ограничения доступа к администрированию виртуальной среды на время восстановления работоспособности инфраструктуры.

В аварийном режиме приостанавливается:

- работа компонентов защиты серверов виртуализации и серверов управления виртуальной инфраструктурой (серверов Hyper-V);
- действие политик безопасности;
- действие правил разграничения доступа к защищаемым серверам;
- проверка меток безопасности.

В аварийном режиме включается правило фильтрации, разрешающее весь трафик виртуальных машин. Правило имеет максимальный приоритет.

Примечание. В аварийном режиме не выполняется аудит событий безопасности для компонентов защиты серверов Hyper-V (подробнее о событиях аудита см. стр.135).

Внимание! После включения аварийного режима доступ к настройкам сервера авторизации возможен только с помощью локальной консоли управления.

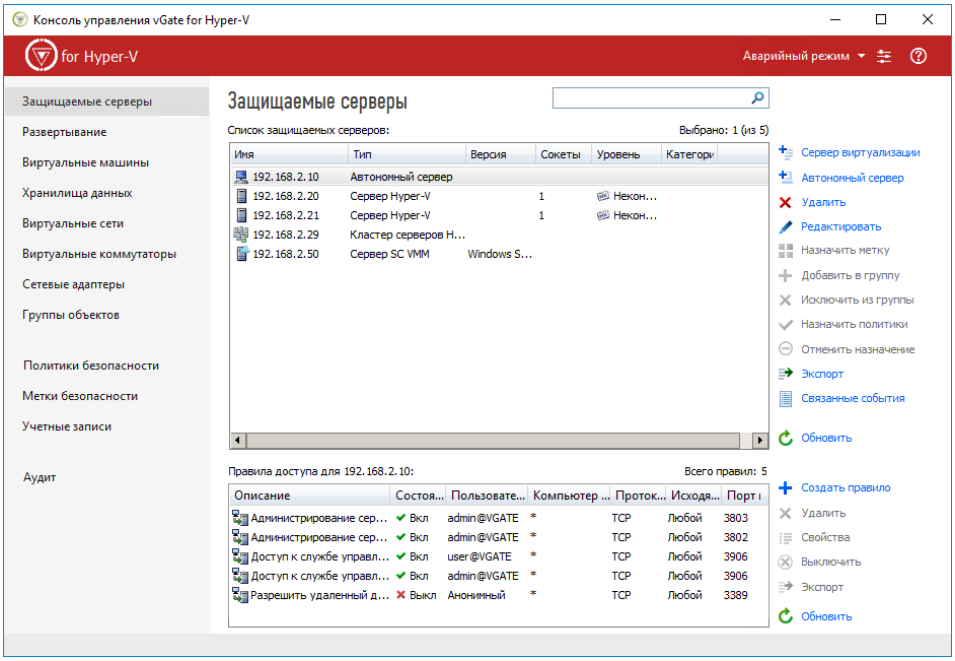
Для переключения vGate в аварийный режим:

1. В области главного меню консоли управления нажмите кнопку-ссылку с названием текущего режима работы (в обычном случае — "Штатный режим") и выберите в раскрывающемся списке вариант "Аварийный режим".

   На экране появится предупреждение о переключении vGate в аварийный режим.

2. Нажмите кнопку-ссылку "Продолжить" в окне предупреждения.

   Аварийный режим будет включен. Область главного меню консоли управления будет окрашена в красный цвет. Ссылка с названием текущего режима работы vGate изменит название на "Аварийный режим".



Внимание! В процессе восстановления работоспособности инфраструктуры могут произойти изменения в конфигурации защищаемых серверов или средств администрирования виртуальной инфраструктуры. Перед переключением vGate в штатный режим необходимо проверить корректность конфигурации vGate в соответствии с планом настройки конфигурации (см. стр.**65**).

Для переключения vGate в штатный режим:

1. В области главного меню консоли управления нажмите кнопку-ссылку "Аварийный режим" и выберите в раскрывающемся списке вариант "Штатный режим".

   На экране появится предупреждение о переключении vGate в штатный режим.

2. Нажмите кнопку-ссылку "Продолжить" в окне предупреждения.

   Штатный режим будет включен. Область главного меню консоли управления будет окрашена в синий цвет. Ссылка с названием текущего режима работы vGate изменит название на "Штатный режим".

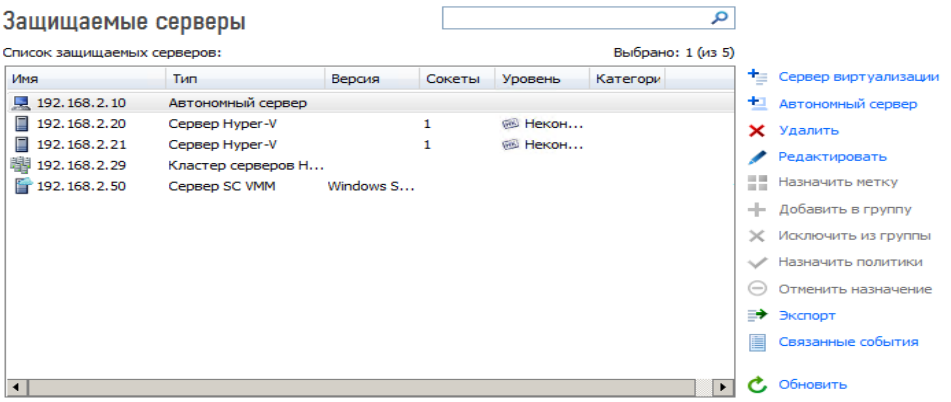
Регистрация защищаемых серверов

Защищаемыми серверами могут быть серверы Hyper-V, серверы SCVMM и другие элементы виртуальной инфраструктуры, имеющие IP-адрес и находящиеся в защищаемом периметре сети администрирования (например, DNS или кластеры серверов Hyper-V).

Для регистрации сервера Hyper-V:

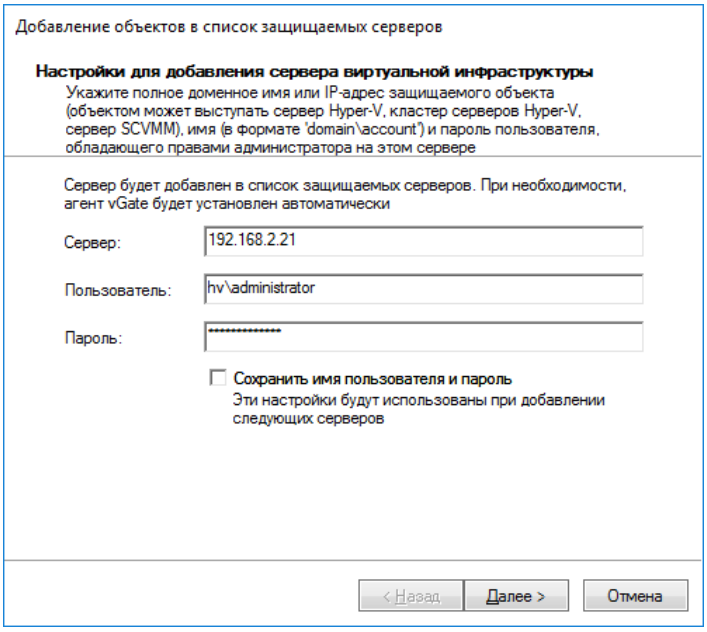
1. В консоли управления выберите функцию "Защищаемые серверы".

В верхней части области параметров появится список защищаемых серверов.



2. Нажмите кнопку-ссылку "Сервер виртуализации".

   На экране появится мастер добавления нового защищаемого сервера.



3. Укажите полное доменное имя или IP-адрес сервера Hyper-V, кластера серверов или сервера SCVMM, а также имя и пароль администратора для данного сервера и нажмите кнопку "Далее".

Совет. Отметьте поле "Сохранить имя пользователя и пароль", чтобы использовать введенные данные в качестве данных общей учетной записи (см. стр.70).

На сервер будет автоматически установлен агент защиты vGate и сервер будет добавлен в список защищаемых объектов. На экране появится сообщение об успешном завершении операции.

Примечание. Агент защиты vGate не устанавливается на кластер серверов Hyper-V.

4. Чтобы завершить работу мастера, нажмите "Завершить".

   Добавленный сервер появится в списке защищаемых серверов. При успешном завершении установки агента защиты в разделе "Развертывание" консоли управления появится номер версии агента и сообщение о его статусе "Запущен".

Для регистрации другого объекта виртуальной инфраструктуры:

1. В консоли управления выберите функцию "Защищаемые серверы".

   В верхней части области параметров появится список защищаемых серверов.

2. Нажмите кнопку-ссылку "Автономный сервер".

   На экране появится диалог для добавления сервера.

3. Укажите сетевое имя или IP-адрес сервера, при необходимости введите комментарий и нажмите кнопку "ОК".

   В списке защищаемых серверов появятся новые записи.

Примечание.
Для редактирования списка защищаемых серверов используйте кнопки-ссылки "Редактировать" и "Удалить".
Кнопка-ссылка "Назначить метку" позволяет назначить метку безопасности для выбранного сервера Hyper-V (см. стр.124).
Кнопка-ссылка "Экспорт" позволяет выгрузить список защищаемых серверов в файл.

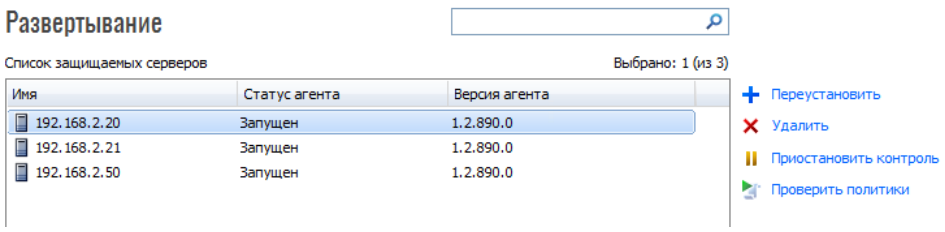
Развертывание компонентов защиты на сервере Hyper-V

Развертывание компонентов защиты на сервере Hyper-V выполняется автоматически при добавлении сервера в список защищаемых серверов (см. стр.87). При необходимости переустановки модуля защиты Hyper-V или временной приостановки контроля за операциями управления виртуальной инфраструктурой воспользуйтесь функцией "Развертывание" в консоли управления.

Для переустановки модуля защиты Hyper-V:

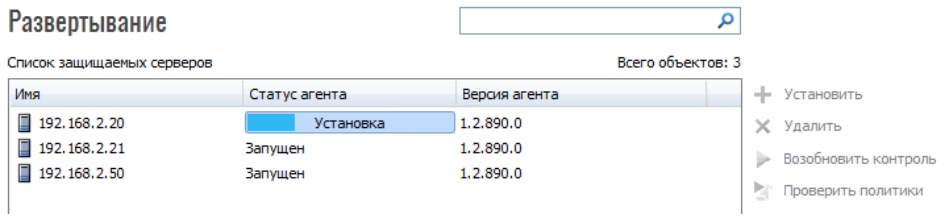
1. В консоли управления выберите функцию "Развертывание".

   В области параметров появится список серверов Hyper-V.



2. Выберите из списка сервер Hyper-V и нажмите кнопку-ссылку "Переустановить".

   На экране появится отображение процесса переустановки.



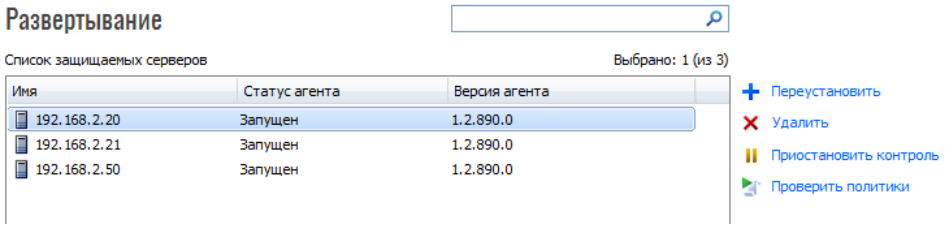
3. При успешном выполнении переустановки модуля защиты Hyper-V параметр "Статус агента" выбранного сервера снова примет значение "Запущен".

Примечание. Кнопка-ссылка "Удалить" используется для запуска процедуры удаления модулей защиты, развернутых на серверах Hyper-V. Их необходимо удалить перед удалением сервера авторизации (см. стр.54).

Для приостановки контроля защиты Hyper-V:

1. В консоли управления выберите функцию "Развертывание".

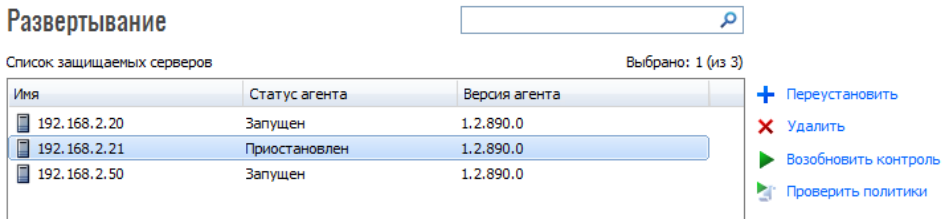
   В области параметров появится список серверов Hyper-V.



2. Выберите из списка сервер Hyper-V и нажмите кнопку-ссылку "Приостановить контроль".

На экране появится окно с предупреждением об отключении контроля. Нажмите кнопку "Да" для подтверждения операции.

Контроль за операциями управления виртуальной инфраструктурой Hyper-V будет приостановлен. Перестанет действовать механизм полномочного управления доступом, и управление доступом к серверам Hyper-V будет осуществляться в соответствии с настроенными правилами разграничения доступа (см. стр.**115**). Параметр "Статус агента" выбранного сервера Hyper-V примет значение "Приостановлен".



Примечание. Для возобновления контроля за операциями управления виртуальной инфраструктурой нажмите кнопку-ссылку "Возобновить контроль". Параметр "Статус агента" выбранного сервера Hyper-V примет значение "Запущен".

Управление учетными записями пользователей

Регистрация пользователей

Изначально управление учетными записями выполняется от имени учетной записи главного АИБ, которая создается при установке сервера авторизации vGate. В дальнейшем возможно предоставление прав на управление списком пользователей учетной записи АИБ.

АИБ может зарегистрировать пользователей двух типов — администратор виртуальной инфраструктуры (АВИ) и администратор информационной безопасности (АИБ) (см. раздел "Функциональные возможности" в документе [1]).

Если управлением vGate занимаются несколько АИБ, то для каждого АИБ следует настроить дополнительные учетные записи.

Внимание! Учетная запись главного АИБ имеет ряд привилегий по сравнению с настроенными в консоли. Только эта учетная запись обладает правами добавлять ПРД для внешнего адаптера основного или резервного сервера авторизации, редактировать учетную запись главного АИБ, а также создавать учетные записи с привилегией "Оператор учетных записей" (см. стр.**92**).

Для аутентификации пользователей (АВИ) в vGate можно использовать существующие доменные учетные записи пользователей Windows. В список пользователей vGate можно добавить учетные записи из домена, в котором находится сервер авторизации, или из доверенного домена (см. стр.**77**). Все доменные пользователи автоматически добавляются в группу "Аутентифицированный", и для

них действуют соответствующие правила доступа к защищаемым серверам (см. стр.**115**).

Для полномочного управления доступом доменные учетные записи необходимо зарегистрировать в vGate с помощью консоли управления.

Внимание!

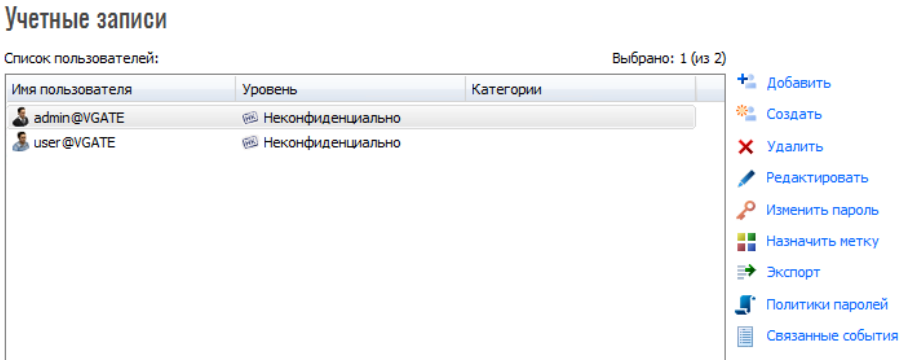
- vGate поддерживает работу только с одним уровнем вложенности групп Active Directory.
- Работа с вложенными группами реализуется только в случае, если контроллер домена Active Directory передает информацию о членстве пользователя во вложенных группах.

Редактирование списка пользователей

Для редактирования списка пользователей:

1. В консоли управления выберите функцию "Учетные записи".

   В области параметров появится список пользователей.



2. Отредактируйте список, используя указанные ниже кнопки.

Кнопка	Описание
Добавить	Добавление учетной записи из Active Directory
Создать	Создание учетной записи пользователя или администратора (см. стр.**92**)
Удалить	Удаление выбранной учетной записи
Редактировать	Изменение свойств выбранной учетной записи, в том числе и отключение учетной записи (см. стр.**94**)
Изменить пароль	Изменение пароля для выбранной учетной записи. Действие недоступно для учетных записей из Active Directory
Назначить метку	Назначение метки конфиденциальности для выбранной учетной записи (см. стр.**124**)
Экспорт	Экспорт выбранных учетных записей в файл
Политики паролей	Изменение уровня сложности паролей (см. стр.**95**). Действие не распространяется на учетные записи из Active Directory
Связанные события	Просмотр событий безопасности, связанных с выбранной учетной записью

Первоначально в списке пользователей могут присутствовать учетные записи компьютеров. Они создаются автоматически при установке агента аутентификации на компьютеры во внешнем периметре сети администрирования, которые не входят в домен сервера авторизации или в доверенные домены. Автоматически учетным записям компьютеров назначается пароль, который хранится в системе в защищенном виде и используется при аутентификации. Такие учетные записи используются для авторизации компьютеров, а также организации доступа служб и сервисов этих компьютеров к защищаемым серверам Hyper-V и другим узлам сети администрирования.

Имена учетных записей компьютеров имеют следующий формат:

<имя компьютера>$@<имя реестра учетных записей>

Например: arm$@VGATE.

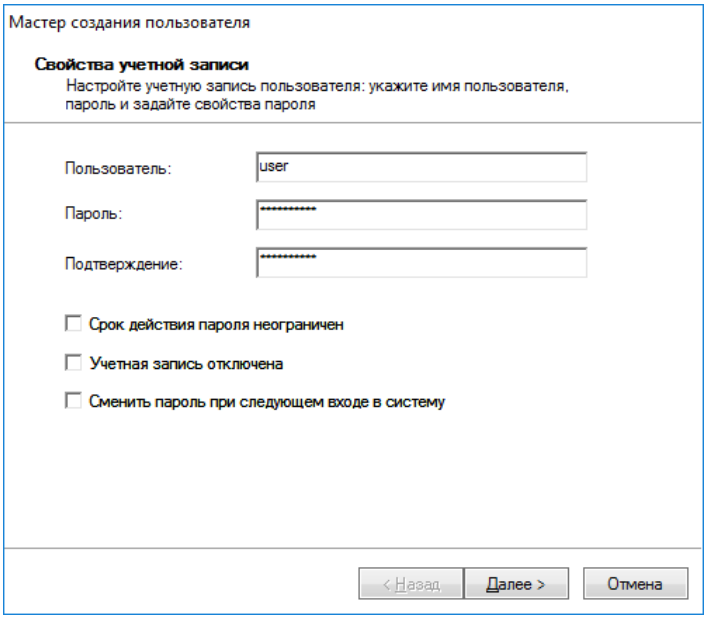
Внимание! Не рекомендуется удалять учетные записи компьютеров, так как для их восстановления потребуется повторная установка агента аутентификации.

Создание учетной записи

Для создания учетной записи:

1. Нажмите кнопку-ссылку "Создать".

   На экране появится окно мастера создания пользователя.

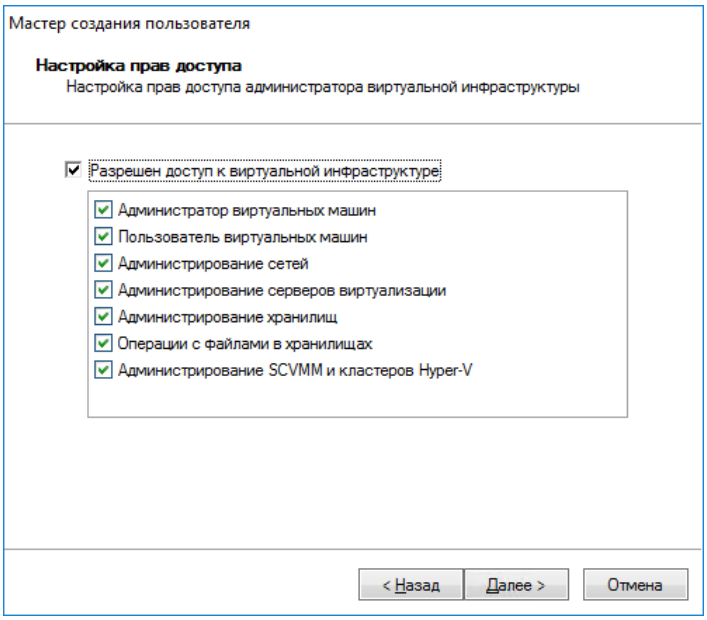


2. Укажите имя пользователя, дважды введите пароль. При необходимости настройте свойства пароля.

Срок действия пароля неограничен
Отметьте это поле для настройки неограниченного срока действия пароля. Если поле не отмечено, то по истечении заданного в политиках срока действия пароля пользователю будет предложено сменить пароль
Учетная запись отключена
Отметьте это поле для временного отключения созданной записи. Если учетная запись отключена, то вход в систему с ее использованием невозможен
Сменить пароль при следующем входе в систему
Если это поле отмечено, при первом входе в систему пользователю будет предложено сменить пароль

Примечание. Настройка свойств пароля недоступна для учетных записей из Active Directory.

3. Нажмите кнопку "Далее". На экране появится окно настройки прав доступа для администратора виртуальной инфраструктуры.

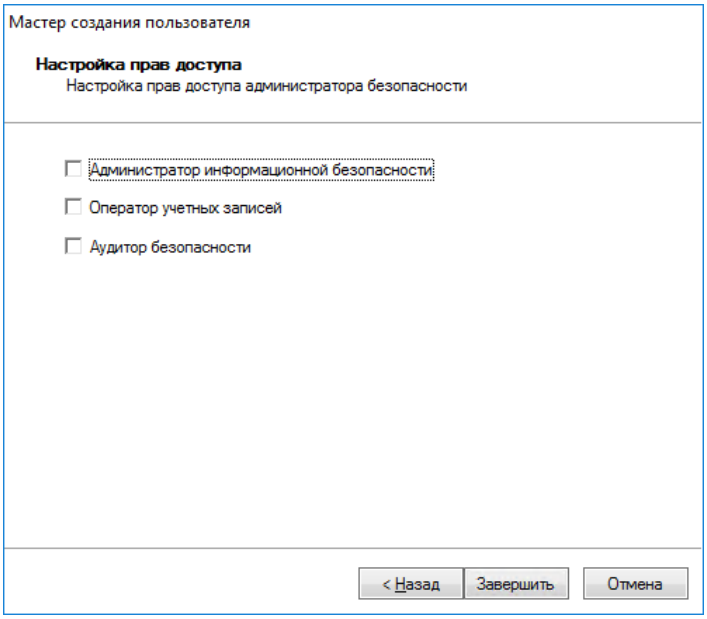


Примечание. Подробнее о привилегиях различных типов пользователей см. стр.161.

4. Для создания учетной записи администратора виртуальной инфраструктуры отметьте пункт "Разрешен доступ к виртуальной инфраструктуре" и выберите в списке действия, которые будут доступны АВИ.

Примечание. Для работы привилегии "Операции с файлами в хранилищах" необходимо, чтобы для данного пользователя было явно настроено соответствующее правило доступа.

5. Нажмите кнопку "Далее". На экране появится окно настройки прав доступа для администратора информационной безопасности.



Администратор информационной безопасности
Отметьте это поле, если создается учетная запись АИБ
Оператор учетных записей
Отметьте это поле для предоставления создаваемой учетной записи прав на управление списком пользователей. При выборе данного параметра пользователю автоматически будут предоставлены права доступа АИБ
Аудитор безопасности
Отметьте это поле, чтобы предоставить пользователю права только на просмотр данных в программе управления vGate, без возможности внесения изменений

6. Чтобы завершить работу мастера, нажмите "Завершить".

   Созданная учетная запись появится в списке.

Отключение учетной записи

Отключение учетной записи запрещает авторизацию данного пользователя.

Однако уже авторизованный пользователь сможет продолжить свою работу и после отключения учетной записи, вплоть до следующей попытки авторизации.

Внимание! Отключение учетной записи главного АИБ, созданной при установке сервера авторизации, невозможно.

Для отключения учетной записи:

1. Выберите учетную запись и нажмите кнопку-ссылку "Редактировать".

   На экране появится диалог для редактирования свойств учетной записи.

2. Отметьте поле "Учетная запись отключена" и нажмите кнопку "ОК".

Примечание. Для включения отключенной учетной записи удалите отметку из поля "Учетная запись отключена" и нажмите кнопку "ОК".

Настройка политик паролей

Политики паролей позволяют обеспечить использование паролей необходимого уровня сложности.

Все пароли, настраиваемые для учетных записей АВИ и АИБ, должны удовлетворять политикам. При смене пароля пользователя как через консоль управления, так и с помощью агента аутентификации проверяется соответствие нового пароля настроенным политикам паролей.

Примечание. Для предотвращения использования легко подбираемых паролей каждый пароль проверяется по словарю часто используемых паролей. Пароль может быть назначен только в случае отсутствия его в словаре. Подробнее о словаре часто используемых паролей см. стр.166.

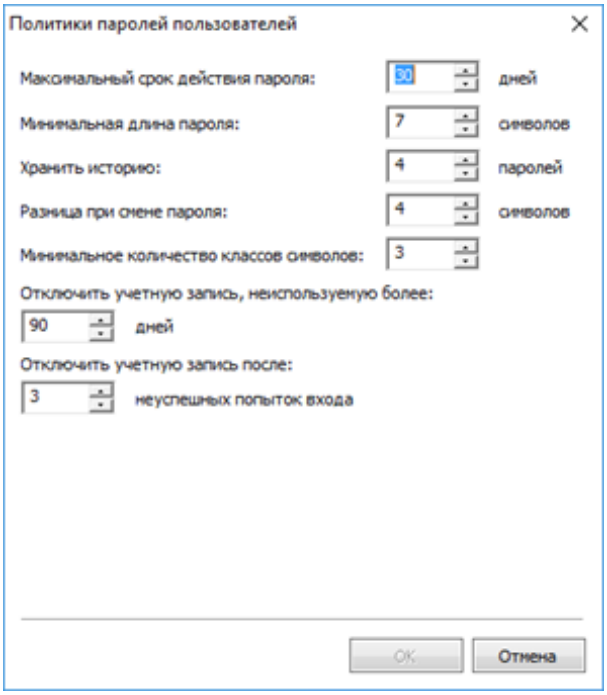
По умолчанию в системе заданы некоторые значения параметров политик паролей (подробнее описано ниже). АИБ может изменить значения этих параметров при необходимости.

Примечание. После изменения политик паролей новые политики начинают действовать на рабочих местах пользователей с небольшой задержкой, поскольку обновление данных на рабочих местах пользователей происходит примерно раз в минуту.

Для настройки парольных политик:

1. В области параметров функции "Учетные записи" нажмите кнопку-ссылку "Политики паролей".

   На экране появится следующий диалог.



2. Измените значения параметров и нажмите кнопку-ссылку "Сохранить".

Максимальный срок действия пароля
Определяет период времени, на протяжении которого действителен текущий пароль пользователя. По истечении заданного периода времени текущий пароль пользователя перестает быть действительным и его требуется изменить. Этот параметр может принимать значение от 1 до 365 дней
Минимальная длина пароля
Определяет минимальное количество символов в пароле. Пользователю нельзя назначить пароль, количество символов в котором меньше значения данного параметра. Этот параметр может принимать значение от 1 до 100
Хранить историю
Определяет число старых паролей каждого пользователя, информация о которых будет храниться системой. При смене пароля пользователя осуществляется сопоставление нового пароля со списком старых паролей этого пользователя. Если новый пароль совпал с одним из старых паролей, то такой пароль запрещается использовать. Этот параметр может принимать значение от 1 до 15
Разница при смене пароля
Определяет количество символов, на которое новый пароль должен отличаться от старого при смене пароля. Этот параметр может принимать значение от 1 до 100
Минимальное количество классов символов
Определяет, сколько именно классов символов (буквы в верхнем и нижнем регистрах, цифры и т. п.) должно присутствовать в пароле. Этот параметр принимает значение от 1 до 4. Значение "1" означает, что пароль может содержать любые символы, например, только буквы в нижнем регистре
Отключить учетную запись, не используемую более
Определяет период времени, через который будут отключены неиспользуемые учетные записи. При необходимости АИБ может включить отключенную учетную запись. Этот параметр может принимать значение от 1 до 1095 дней
Отключить учетную запись после
Определяет количество неуспешных попыток ввода пароля при входе, после которых учетная запись будет отключена. При необходимости АИБ может включить отключенную учетную запись. Этот параметр может принимать значение от 1 до 255

Настройка персонального идентификатора

Для аутентификации пользователя возможно применение персонального идентификатора Рутокен или JaCarta.

Примечание.

- Совместное использование персональных идентификаторов JaCarta и Рутокен не поддерживается.
- Не поддерживается использование JaCarta PKI/ГОСТ.

Для настройки персонального идентификатора:

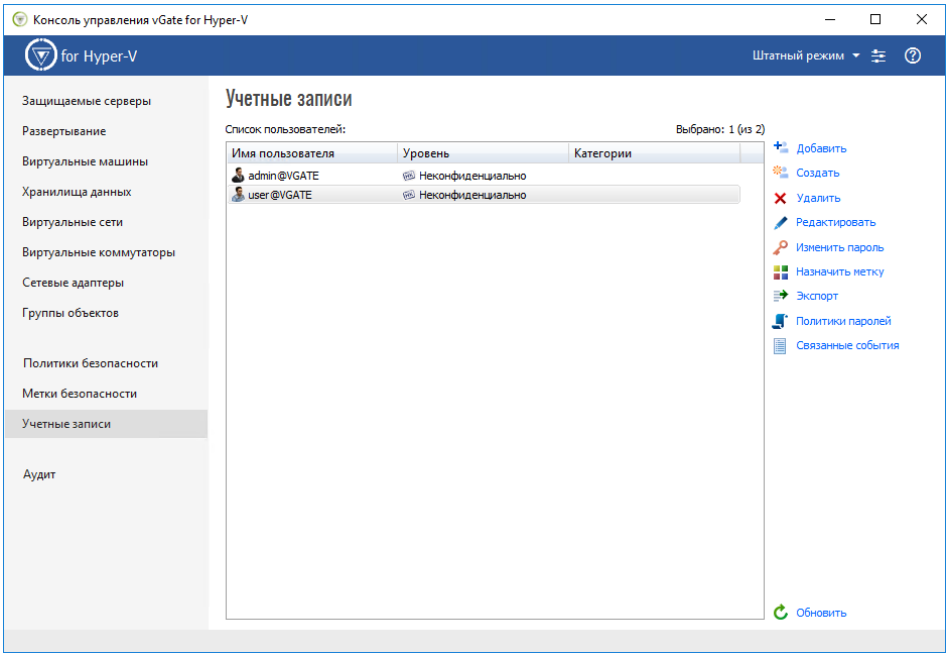
1. Выполните инициализацию персонального идентификатора в Secret Net Studio либо в ПО Рутокен или JaCarta (если Secret Net Studio не используется) согласно документации к этим продуктам.

   Для корректной работы персонального идентификатора Рутокен необходимо установить драйвер устройства Рутокен на компьютер, предназначенный для сервера авторизации vGate, а также на компьютер АВИ/АИБ. Порядок установки ПО vGate и драйверов Рутокен не имеет значения.

   Для корректной работы персонального идентификатора JaCarta необходимо установить драйвер устройства JaCarta (Единый клиент JaCarta) на компьютер, предназначенный для сервера авторизации vGate, а также на компьютер АВИ/АИБ. Порядок установки ПО vGate и драйверов JaCarta не имеет значения. JaCarta Unifield Client (Единый клиент JaCarta) находится на установочном диске vGate в каталоге Redistributables\JaCarta SecurLogon и Единый клиент JaCarta.

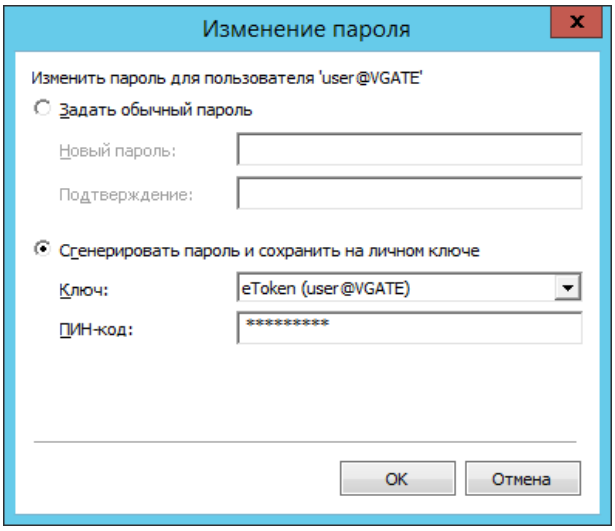
2. Подключите персональный идентификатор к компьютеру, на котором установлена консоль управления vGate.
3. В консоли управления выберите функцию "Учетные записи".

   В области параметров появится список пользователей.



4. Выберите пользователя, которому нужно присвоить персональный идентификатор, и нажмите кнопку-ссылку "Изменить пароль".

   На экране появится следующий диалог.



5. Отметьте пункт "Сгенерировать пароль и сохранить на личном ключе", выберите из списка нужный ключ и задайте PIN-код к нему.
6. Нажмите кнопку "ОК".

   Пароль будет сохранен в персональном идентификаторе.

Использование персонального идентификатора для аутентификации пользователей подробно описано в документе [4].

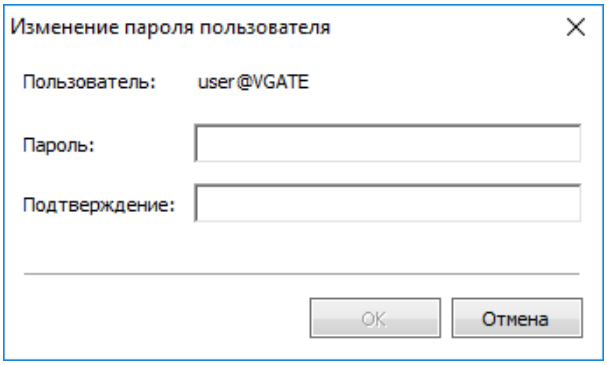
В vGate не поддерживается присвоение персонального идентификатора учетным записям из Active Directory. Если необходимо настроить работу с персональным ключом для таких пользователей, используйте сетевую версию Secret Net. В этом случае персональный идентификатор, присвоенный доменной учетной записи в Secret Net, используется при входе в ОС Windows, а при аутентификации пользователя в vGate будет необходимо выбрать опцию "Использовать текущую сессию Windows".

Смена пароля

Для смены пароля пользователя:

1. Выделите учетную запись и нажмите кнопку-ссылку "Изменить пароль".

   На экране появится следующий диалог.



2. Дважды введите новый пароль и нажмите кнопку "ОК".

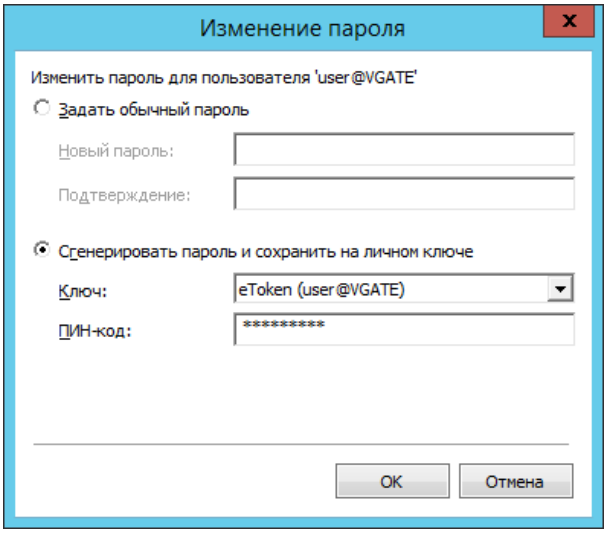
Примечание. Для учетных записей из Active Directory изменение пароля с помощью vGate не поддерживается. Для этого можно использовать средства администрирования Active Directory.

Примечание. Процедура смены пароля пользователем в агенте аутентификации описана в документе [4].

Для генерации пароля персонального идентификатора:

1. Подключите персональный идентификатор к компьютеру, на котором установлена консоль управления vGate.
2. Выделите учетную запись пользователя, которому нужно сменить пароль на персональном идентификаторе, и нажмите кнопку-ссылку "Изменить пароль".

   На экране появится следующий диалог.



3. Отметьте пункт "Сгенерировать пароль и сохранить на личном ключе", в поле "ПИН-код" укажите действующий PIN-код.
4. Нажмите кнопку "ОК".

   Новый пароль будет сгенерирован и сохранен в персональный идентификатор. PIN-код при этом не изменится.

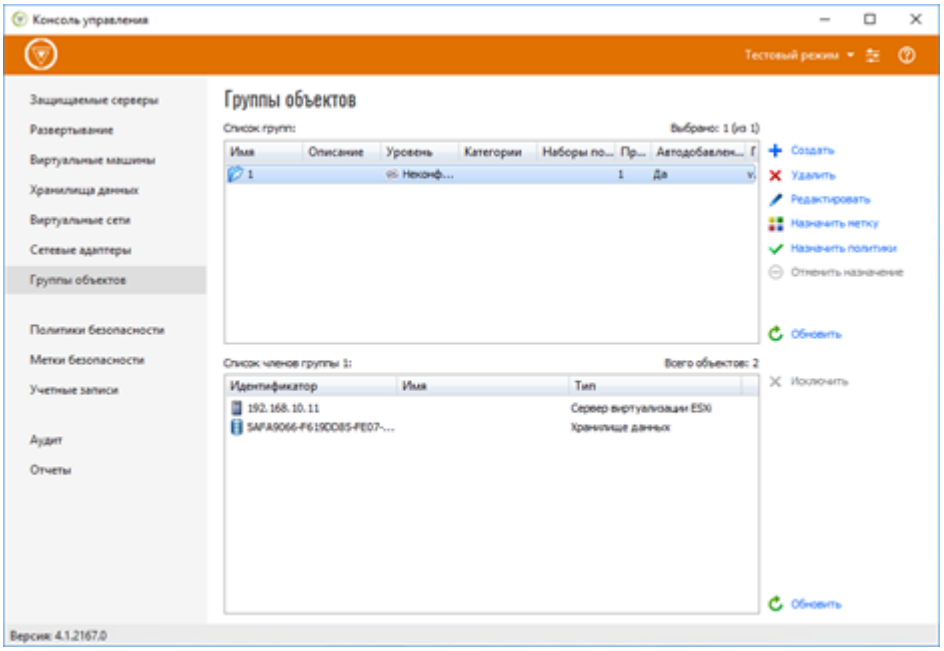
Группировка объектов

В консоли управления vGate 4.4 возможно объединение объектов виртуальной инфраструктуры в группы. Такими объектами могут быть виртуальные машины, серверы Hyper-V, сетевые адаптеры, хранилища данных, виртуальные коммутаторы и виртуальные сети.

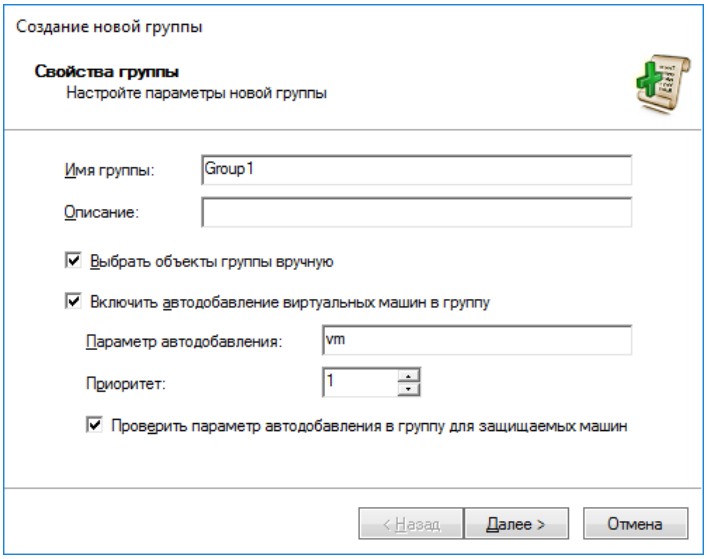
Группам объектов могут быть назначены метки и политики безопасности. Новые настройки будут автоматически применены ко всем объектам, находящимся в группе.

Для создания группы объектов:

1. В консоли управления выберите функцию "Группы объектов".
   В области параметров появится список групп.



2. Чтобы создать группу, нажмите кнопку-ссылку "Создать".
   На экране появится окно мастера создания группы.



3. Настройте параметры новой группы и нажмите кнопку "Далее >".

Параметр	Описание
Имя группы	Имя новой группы
Описание	Описание группы (не является обязательным параметром)
Выбрать объекты группы вручную	Отметьте поле, чтобы на следующем шаге выбрать объекты для добавления в группу
Включить автодобавление виртуальных машин в группу	Отметьте, чтобы настроить автоматическое добавление виртуальных машин в группу по заданному параметру. Задайте параметр автодобавления и приоритет
Параметр автодобавления	Введите текст, по которому будет выполняться поиск в именах виртуальных машин. В результате поиска будут найдены любые имена, в которых присутствует указанный текст. Поиск нечувствителен к регистру символов. Специальные символы, задающие правила поиска, не применяются
Приоритет	Укажите приоритет, согласно которому определяется группа, в которую будет добавлен объект при соответствии его имени нескольким параметрам автодобавления. Группы объектов в инфраструктурах VMware и Hyper-V имеют общую структуру приоритетов. При изменении приоритета одной из групп происходит автоматический пересчет приоритетов остальных групп таким образом, чтобы избежать дублирования приоритетов, а также чтобы между значениями приоритетов не было промежутков
Проверить параметр автодобавления в группу для защищаемых машин	Отметьте поле, чтобы на следующем шаге проверить работу настроенного выше правила автодобавления для существующих виртуальных машин. Выбранные при проверке виртуальные машины будут сразу добавлены в группу. Виртуальные машины, которые не будут выбраны при проверке, в дальнейшем не смогут быть добавлены в группу автоматически

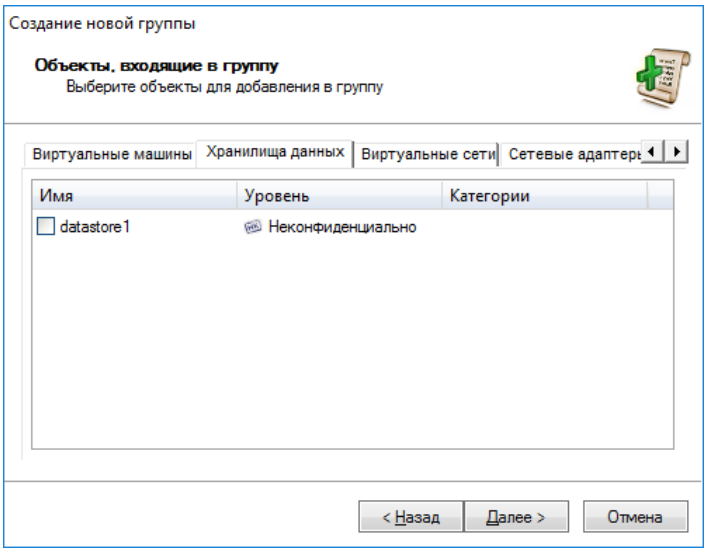
Примечание. По умолчанию автодобавление виртуальных машин в группы объектов выполняется каждые 10 минут. При необходимости настройки автоматического обновления могут быть изменены в консоли управления. Для этого перейдите в раздел "Конфигурация" — "Дополнительные настройки" — "Настройки сети, контроля доступа, лицензирования" и измените значение параметра "Добавлять новые машины каждые".

Добавление (в том числе автоматическое) объекта в группу возможно, только если объект не состоит ни в какой другой группе. При добавлении объекта в новую группу вручную объект исключается из его бывшей группы.

При добавлении объекта в группу с назначенными метками или политиками безопасности происходит применение данных настроек к объекту. Все прошлые метки и политики безопасности для объекта будут отменены.

Автодобавление в группу возможно только для виртуальных машин, с которыми ранее не совершались никакие операции с помощью ПО vGate (добавление в группу, назначение политик или меток безопасности).

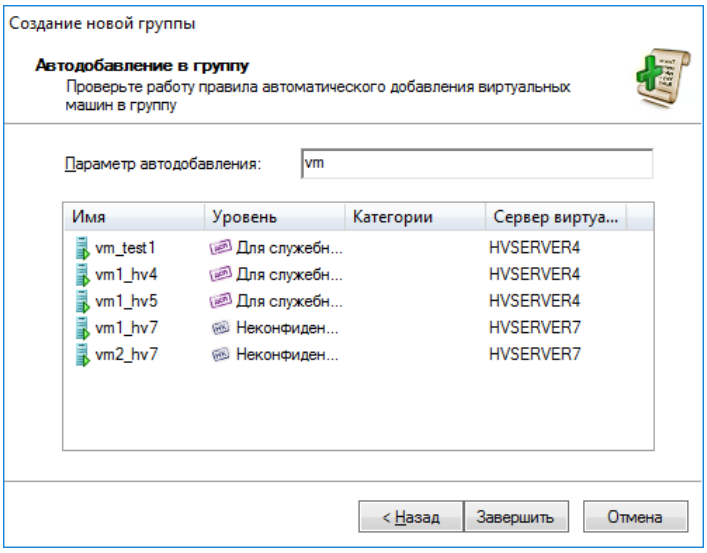
Если был отмечен пункт "Выбрать объекты группы вручную", на экране появится окно выбора объектов.



4. Выберите из списка защищаемые объекты для добавления в группу и нажмите кнопку "Далее >".

Внимание! Добавление объектов в группу может занять длительное время.

Если был отмечен пункт "Проверить параметр автодобавления в группу для защищаемых объектов", на экране появится окно проверки правила автодобавления.



5. Проверьте работу правила автодобавления виртуальных машин по заданному параметру. Нажмите кнопку "Завершить".

   Группа объектов будет создана.

Примечание. Чтобы отключить функцию автодобавления для всех групп, в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate установите значение параметра AddVmToGroupTimeout=0.

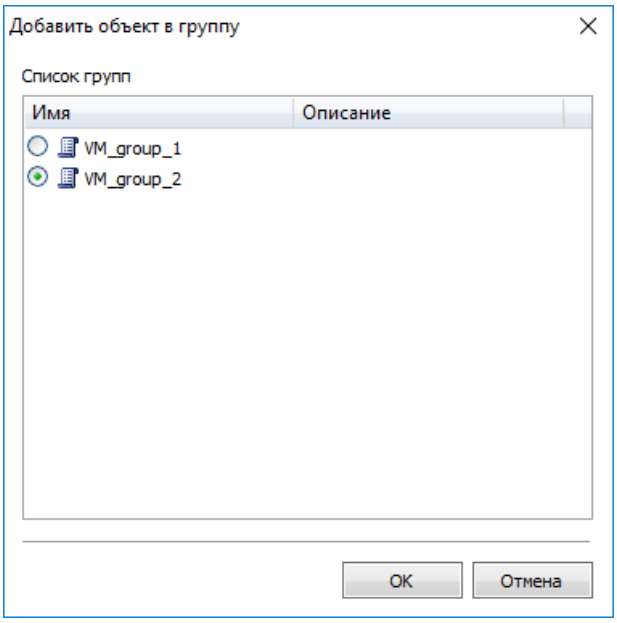
Для добавления объекта в группу:

1. В консоли управления перейдите в раздел "Защищаемые серверы", "Виртуальные машины", "Хранилища данных", "Виртуальные сети" или "Сетевые адаптеры".

   Откроется список объектов.

2. Выделите нужный объект и нажмите кнопку-ссылку "Добавить в группу".

Откроется окно для выбора группы.



3. Отметьте в списке нужную группу и нажмите кнопку "ОК". Объект виртуальной инфраструктуры будет добавлен в группу.

Для исключения объекта из группы:

1. В консоли управления выберите нужный объект.

   В нижней части окна появится список объектов, входящих в состав группы.

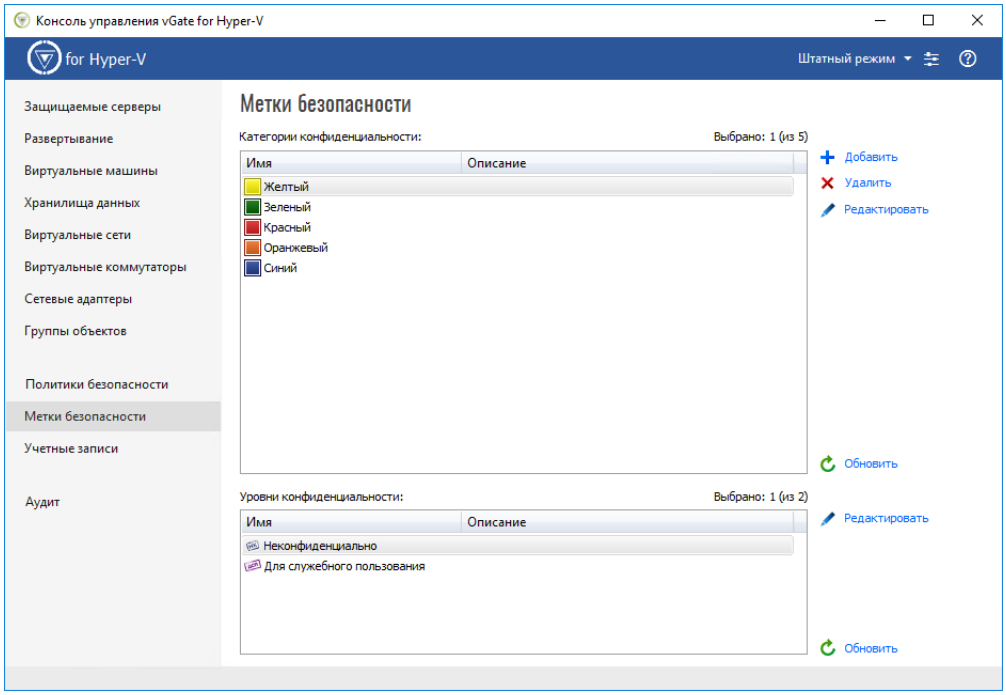
2. Выберите нужный объект и нажмите кнопку-ссылку "Исключить". Объект будет исключен из группы.

Примечание. После исключения объекта из группы все назначенные ему метки и политики безопасности будут удалены. Объекту будет присвоен уровень конфиденциальности "неконфиденциально".

Настройка меток безопасности

Метки безопасности в vGate позволяют настроить механизм полномочного управления доступом пользователей к объектам виртуальной инфраструктуры.

Для просмотра и изменения параметров выберите в консоли управления функцию "Метки безопасности". В области параметров будут отображены значения параметров меток безопасности.



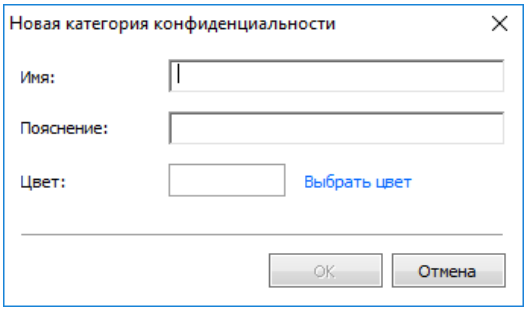
Редактирование списка категорий

По умолчанию в vGate настроен список допустимых категорий конфиденциальности из пяти значений, обозначенных разным цветом. Список допустимых категорий можно адаптировать под свои задачи.

Для добавления категории конфиденциальности:

1. Нажмите кнопку-ссылку "Добавить".

   На экране появится следующий диалог.



   Кнопка-ссылка "Выбрать цвет" открывает палитру для выбора цвета категории.

2. Укажите название категории, выберите цвет и нажмите кнопку "ОК".

   Категория будет добавлена в список категорий конфиденциальности.

Совет. Для редактирования выбранной категории используйте кнопку-ссылку "Редактировать"; для удаления выбранной категории – кнопку-ссылку "Удалить".

Редактирование списка уровней

В группе настроек "Уровни конфиденциальности" отображается перечень допустимых уровней конфиденциальности. Добавить новые значения в список уровней средствами консоли управления нельзя, но можно изменить описание выбранного уровня конфиденциальности с помощью кнопки "Редактировать".

Настройка матрицы допустимых сочетаний уровней и категорий конфиденциальности

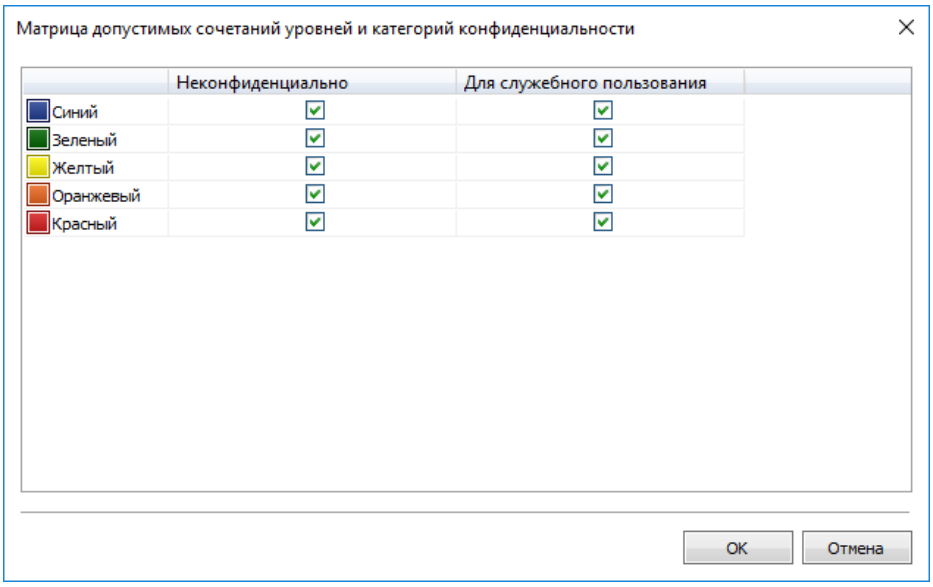
При назначении составных меток (меток, содержащих уровни и категории конфиденциальности одновременно) объектам осуществляется автоматическая проверка возможности задания метки с указанным АИБ сочетанием уровня и категорий конфиденциальности. Для этого используется матрица допустимых сочетаний уровней и категорий конфиденциальности. При попытке назначить метку с недопустимым сочетанием будет выдано предупреждение о невозможности задания такой метки.

По умолчанию в этой матрице разрешены любые сочетания уровней и категорий конфиденциальности.

Для настройки матрицы:

1. Нажмите кнопку в области главного меню консоли управления.
2. Откройте группу параметров "Дополнительные настройки" и нажмите кнопку-ссылку "Допустимые сочетания уровней и категорий".

   На экране появится матрица сочетаний уровней и категорий конфиденциальности.



3. Отметьте нужные сочетания и нажмите кнопку "ОК".

Настройка политик безопасности

Политики безопасности содержат настройки для серверов Hyper-V и ВМ, позволяющие обеспечить определенную степень защиты данных и соответствие требованиям некоторых стандартов безопасности.

Применение политик безопасности и механизма полномочного управления доступом позволяет обеспечить необходимый уровень безопасности.

Шаблоны политик безопасности

Политики безопасности объединены в типовые наборы политик безопасности (шаблоны).

Набор политик	Описание
vGate for Hyper-V	Специально разработанный для vGate набор политик, позволяющий задать более безопасный режим работы серверов Hyper-V и виртуальных машин
PCI DSS	Рекомендуемый набор политик для приведения виртуальной среды в соответствие требованиям PCI DSS. Requirements and Security Assessment Procedures v 3.2
АС 1Г	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду автоматизированных систем класса 1Г в соответствие РД ФСТЭК России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации"
ИСПДн уровни 1 и 2	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных уровней защищенности 1 и 2 в соответствие законодательству в области защиты персональных данных (152-ФЗ, приказ ФСТЭК России № 21)
ИСПДн уровень 3	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных уровня защищенности 3 в соответствие законодательству в области защиты персональных данных (152-ФЗ, приказ ФСТЭК России № 21)
ИСПДн уровень 4	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных уровня защищенности 4 в соответствие законодательству в области защиты персональных данных (152-ФЗ, приказ ФСТЭК России № 21)
ГИС К1 и К2	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду государственных информационных систем классов К1 и К2 в соответствие законодательству в области защиты информации в государственных информационных системах (приказ ФСТЭК России № 17)
ГИС К3 и К4	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду государственных информационных систем классов К3 и К4 в соответствие законодательству в области защиты информации в государственных информационных системах (приказ ФСТЭК России № 17)
СТО БР уровень 2	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем уровня защищенности 2 в соответствие стандарту СТО БР ИББС 2014

Набор политик	Описание
СТО БР уровни 3 и 4	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем уровней защищенности 3 и 4 в соответствие стандарту СТО БР ИББС 2014
ГОСТ Р 56938-2016	Рекомендуемый набор политик для осуществления защиты информации при использовании технологий виртуализации
ГОСТ Р 57580.1-2017 У31	Рекомендуемый набор политик для обеспечения безопасности финансовых (банковских) операций в финансовых организациях. Уровень защиты информации 1
ГОСТ Р 57580.1-2017 У32 и У33	Рекомендуемый набор политик для обеспечения безопасности финансовых (банковских) операций в финансовых организациях. Уровни защиты информации 2 и 3
КИИ К1	Рекомендуемый набор политик для обеспечения безопасности критической информационной инфраструктуры 1 категории значимости
КИИ К2 и К3	Рекомендуемый набор политик для обеспечения безопасности критической информационной инфраструктуры 2 и 3 категорий значимости

Описание политик безопасности

Политики безопасности сервера Hyper-V

Серверам Hyper-V могут назначаться следующие политики безопасности.

Политика	Описание
Запрет удаленного использования PowerShell	Блокирует возможность удаленного использования PowerShell на сервере Hyper-V
Отключение ненужных ролей и компонентов для сервера Hyper-V	Политика позволяет отключить ненужные роли и компоненты для сервера Hyper-V, используя список разрешенных ролей и компонентов. Роли и компоненты, которые нельзя включить: FileAndStorage-Services, Hyper-V, Remote-Desktop-Services, NET-Framework-45-Features, Failover-Clustering, Server-Media-Foundation, Multipath-IO, RSAT, FS-SMB1, User-Interfaces-Infra, PowerShellRoot, WoW64-Support
Отключение функции SMB 1.0/CIFS для сервера Hyper-V	Отключает компонент SMB 1.0/CIFS (Common Internet File System) для сервера Hyper-V под управлением ОС Windows Server 2012 R2
Включение Secure Boot	Включает опцию Secure Boot на виртуальных машинах второго поколения для обеспечения безопасного запуска
Запрет хранения файлов ВМ в корневом каталоге	Проверяет места хранения дисков ВМ и конфигураций ВМ по умолчанию (в настройках сервера), чтобы предотвратить хранение в корневом каталоге (D:/)
Запрет хранения файлов ВМ на системном разделе	Проверяет места хранения дисков и конфигураций ВМ по умолчанию (в настройках сервера), чтобы предотвратить хранение на системном разделе
Отключение RDP Printer Mapping	Отключает RDP Printer Mapping на сервере, чтобы предотвратить возможность атаки через данный механизм
Включение VMQ	Включает VMQ на сетевых адаптерах сервера, подключенных к внешним коммутаторам
Приоритизация сетевого адаптера, используемого для управления ВИ	Перемещает сетевой адаптер, используемый для управления виртуальной инфраструктурой, на первое место в списке приоритета

Политика	Описание
Проверка имени учетной записи администратора	Проверяет, что имя учетной записи локального администратора отвечает заданным требованиям
Проверка имени гостевой учетной записи	Проверяет, что имя гостевой учетной записи отвечает заданным требованиям
Блокирование гостевой учетной записи	Обеспечивает отключение локальной гостевой учетной записи на сервере Hyper-V
Запрет монтирования съемных носителей	Блокирует возможность подключения съемных носителей информации на сервере Hyper-V
Список разрешенных программ	Позволяет создать доверенную программную среду на сервере Hyper-V с помощью списка разрешенных для запуска программ. При включенной опции "Разрешен запуск программ, не входящих в список" осуществляется только регистрация событий запуска программ, не входящих в список разрешенных. Блокировка запуска таких программ не осуществляется
Запрет зеркалирования портов	Запрещает зеркалирование портов для предотвращения дублирования трафика с защищаемых ВМ
Запрет смены MAC-адреса	Запрещает смену MAC-адреса. В некоторых случаях данная политика неприменима. Например, при балансировке нагрузки сети смена MAC-адреса необходима
Использование протокола CHAP для iSCSI	Проверяет использование протокола Mutual CHAP для аутентификации iSCSI-хранилищ, что помогает избежать подмены доверенного хранилища
Разделение сетей управления и сетей виртуальных машин	Проверяет, что не используется одна и та же сеть для управления виртуальной инфраструктурой и для доступа к виртуальным машинам
Отключение IPv6	Отключает протокол IPv6, если он не используется. После применения политики необходим перезапуск сервера
Список зарезервированных диапазонов VLAN	Блокирует добавление VLAN из зарезервированного диапазона
Запрет операций с буфером обмена	Отключает службы "Guest Services" и "Data Exchange", чтобы предотвратить обмен между ВМ и сервером
Синхронизация времени	Включает службу "Time Synchronization" для синхронизации времени между сервером и ВМ
Отключение удаленного управления службами	Отключает удаленный доступ к менеджеру служб на сервере

Политики безопасности ВМ

Виртуальным машинам могут назначаться следующие политики безопасности.

Политика	Описание
Доверенная загрузка виртуальных машин Hyper-V	Контролирует целостность базовой системы ввода-вывода ВМ и конфигурации ВМ. Блокирует запуск ВМ при нарушении целостности
Запрет включения репликации виртуальных машин Hyper-V	Блокирует возможность включения репликации ВМ
Запрет миграции виртуальных машин Hyper-V	Блокирует возможность миграции ВМ

Политика	Описание
Запрет создания и удаления контрольных точек виртуальных машин Hyper-V	Блокирует возможность создания и удаления контрольных точек (checkpoints) ВМ
Запрет экспорта виртуальных машин Hyper-V	Блокирует возможность экспорта ВМ
Затирание остаточных данных на СХД при удалении виртуальной машины Hyper-V	Политика обеспечивает автоматическое затирание файлов жестких дисков при удалении ВМ посредством однократной записи нулевых значений. Данная политика не работает для дисков ВМ, имеющих контрольные точки (checkpoints). Перед удалением ВМ необходимо удалить все ее контрольные точки

Порядок настройки политик безопасности

Назначение политики объекту осуществляется следующим образом:

- на базе шаблона формируется набор политик (см. стр.**109**);
- набор политик назначается объекту (серверу Hyper-V или ВМ) или группе объектов.

Примечание. Проверки, осуществляемые политиками, начинают выполняться автоматически после назначения политик на сервер Hyper-V или виртуальную машину. Также можно запустить проверку изменений политик вручную, нажав кнопку-ссылку "Проверить политики" на странице "Развертывание".

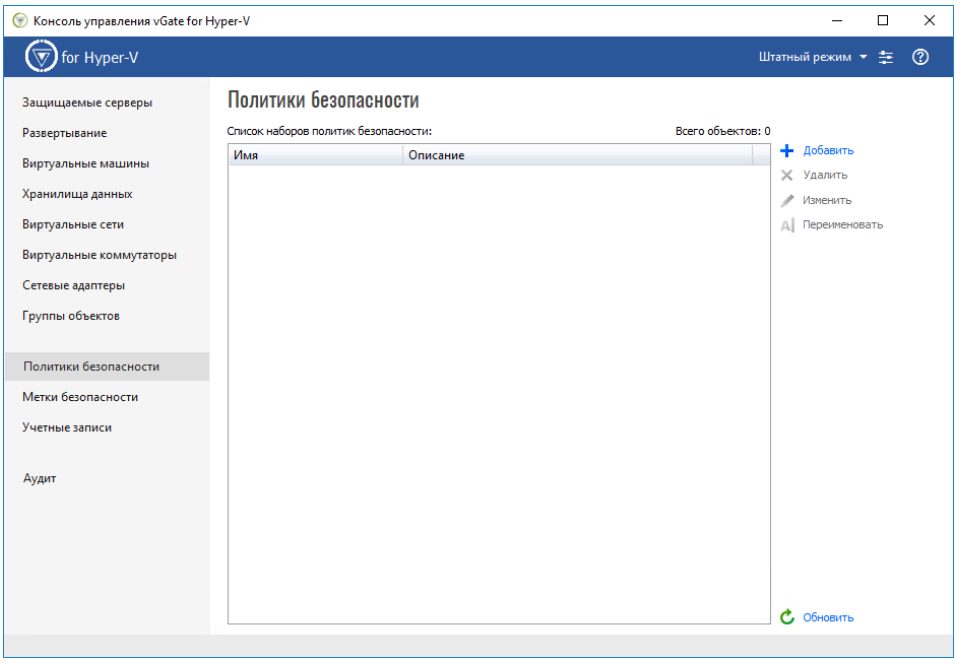
Формирование наборов политик

Для управления политиками:

1. В консоли управления выберите функцию "Политики безопасности".

   В области параметров будет отображен список наборов политик.

   Примечание. При первом обращении к функции "Политики безопасности" список политик будет пустым.



2. Сформируйте список, используя указанные ниже кнопки-ссылки.

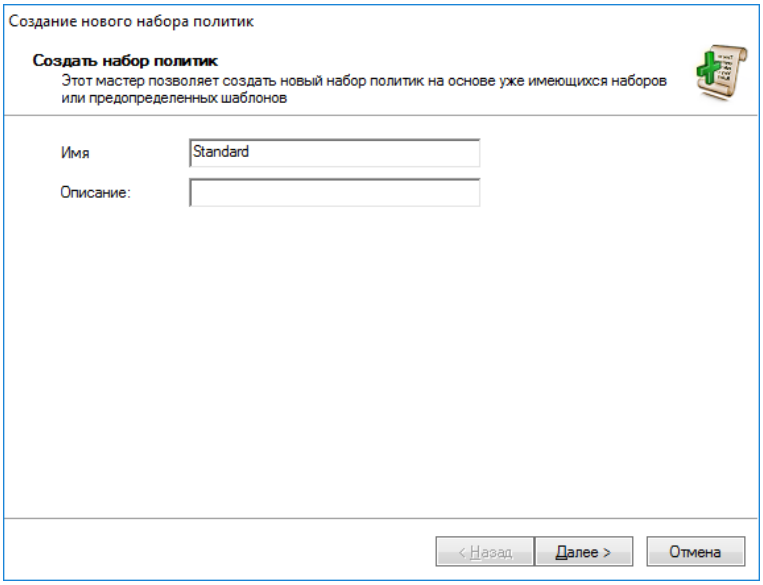
Кнопка	Описание
Добавить	Добавление нового набора политик (см. стр.**110**) или формирование на базе существующего (см. стр.**111**)
Удалить	Удаление выбранного набора политик
Изменить	Изменение настроек выбранного набора политик
Переименовать	Редактирование названия и описания выбранного набора

Добавление нового набора политик

Для добавления набора политик:

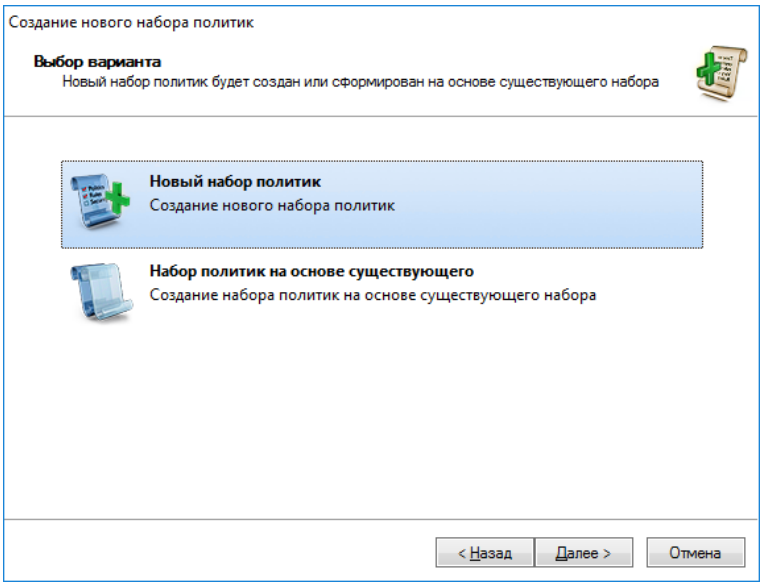
1. Нажмите кнопку-ссылку "Добавить".

   На экране появится следующий диалог.



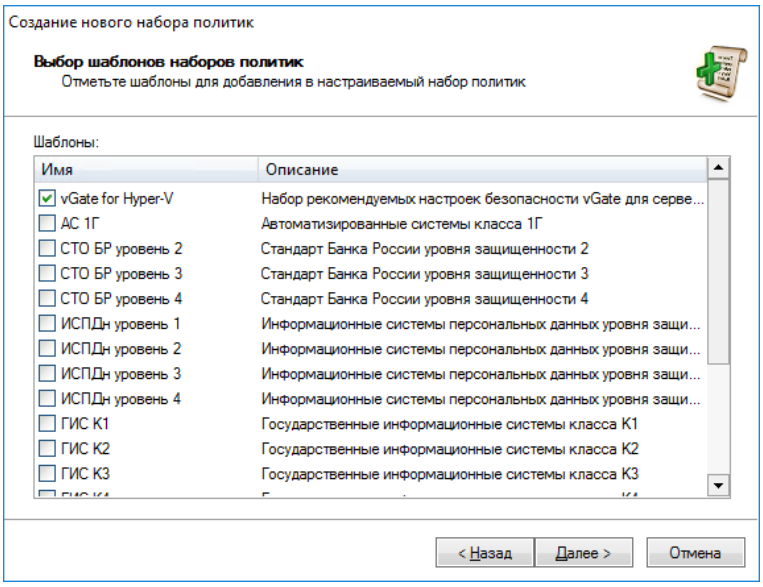
2. Укажите имя набора политик и описание (при необходимости). Нажмите кнопку "Далее".

   При наличии уже настроенных наборов политик на экране появится диалог выбора варианта создания набора.



3. Выберите вариант "Новый набор политик" и нажмите кнопку "Далее".

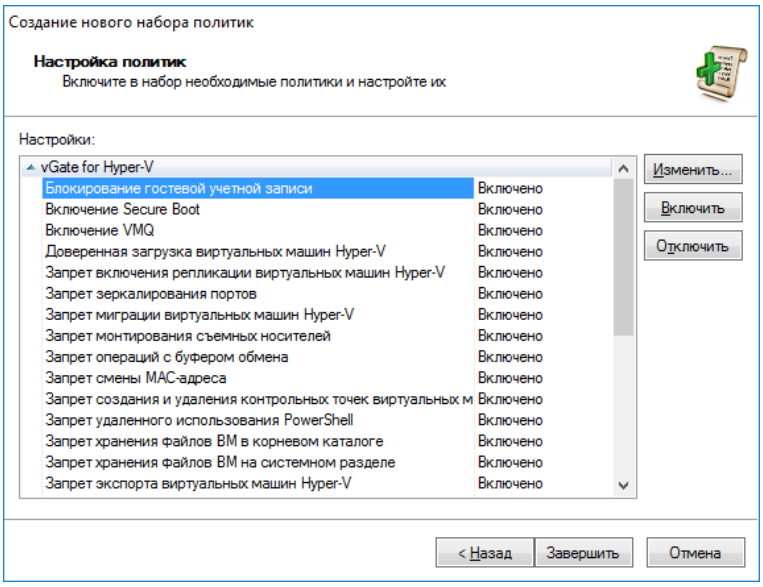
На экране появится диалог выбора шаблонов.



Если отмечено несколько стандартов, то новый (объединенный) набор будет сформирован из политик всех выбранных шаблонов.

4. Отметьте нужные шаблоны и нажмите кнопку "Далее".

   На экране появится диалог настройки политик.



Политики в списке отсортированы по алфавиту.

5. Настройте параметры политик и нажмите кнопку "Завершить".

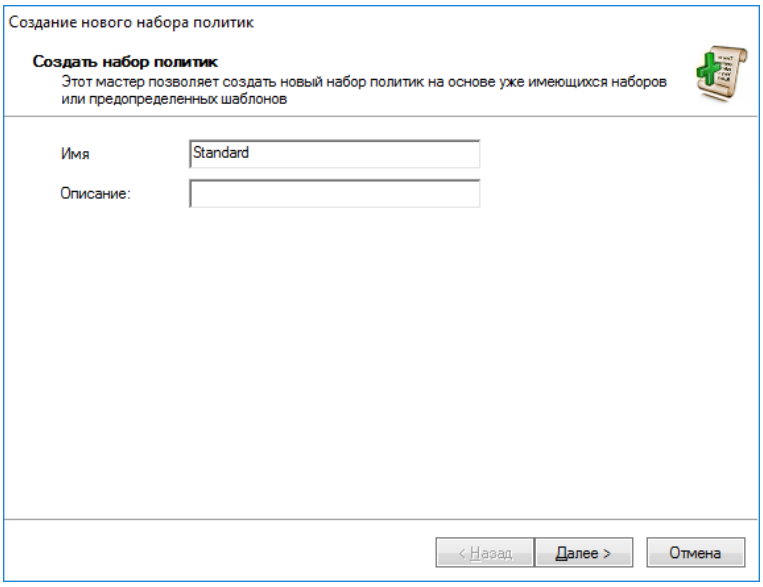
Примечание. Подробнее о настройке политики "Доверенная загрузка виртуальных машин Hyper-V" см. стр.130.

Добавление набора политик на основе существующего

Для добавления набора политик:

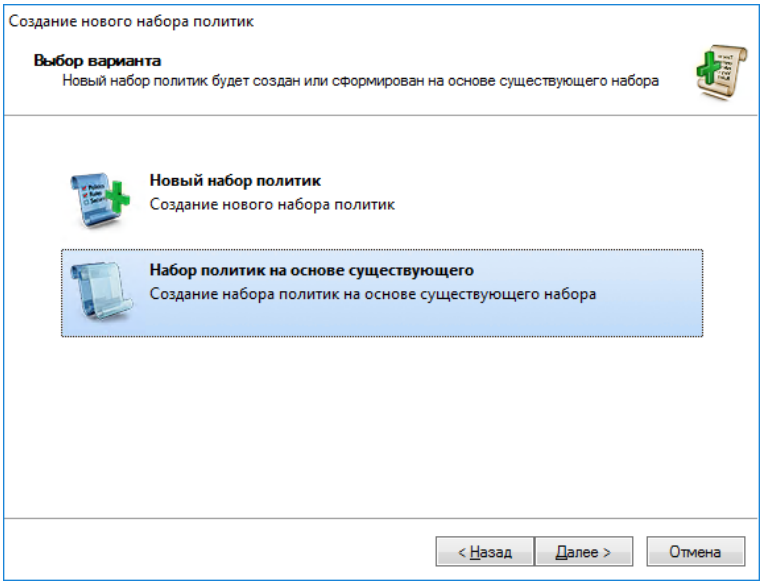
1. Нажмите кнопку-ссылку "Добавить".

   На экране появится следующий диалог.



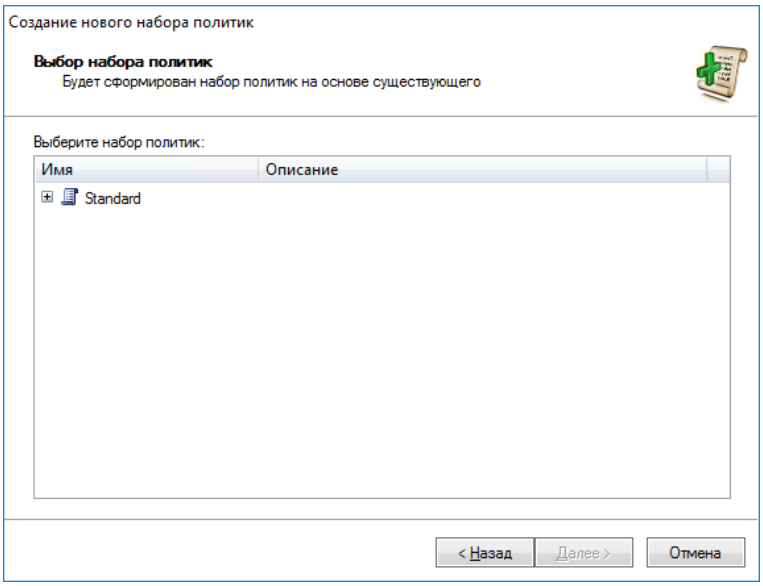
2. Укажите имя набора политик и описание (при необходимости). Нажмите кнопку "Далее".

   На экране появится диалог выбора варианта создания набора политик.



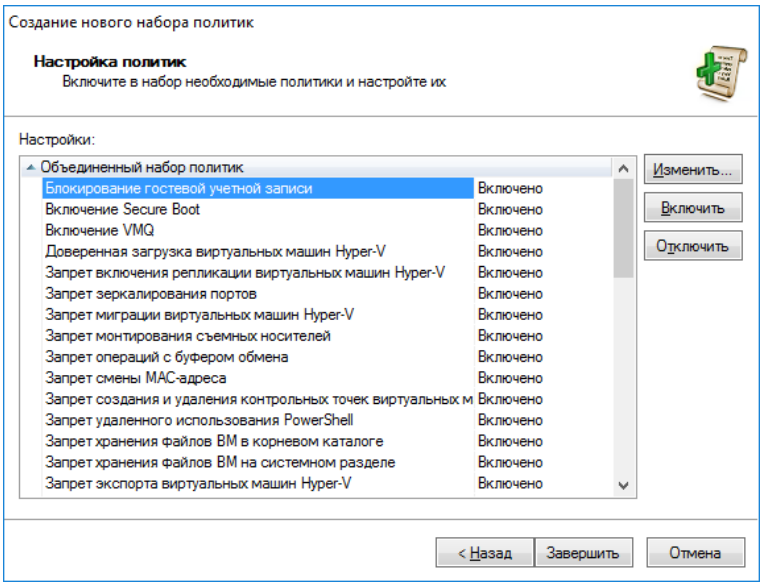
3. Выберите вариант "Набор политик на основе существующего" и нажмите кнопку "Далее".

   На экране появится диалог выбора эталонного набора политик.



4. Выберите эталонный набор политик и нажмите кнопку "Далее".

   На экране появится диалог настройки политик.



   Политики из эталонного набора собраны в начале списка, а все остальные сгруппированы в шаблоне стандарта безопасности "vGate for Hyper-V" в конце списка.

5. Включите в набор необходимые политики, настройте параметры политик и нажмите кнопку "Завершить".

Примечание. Подробнее о настройке политики "Доверенная загрузка виртуальных машин Hyper-V" см. стр.130.

Редактирование набора политик

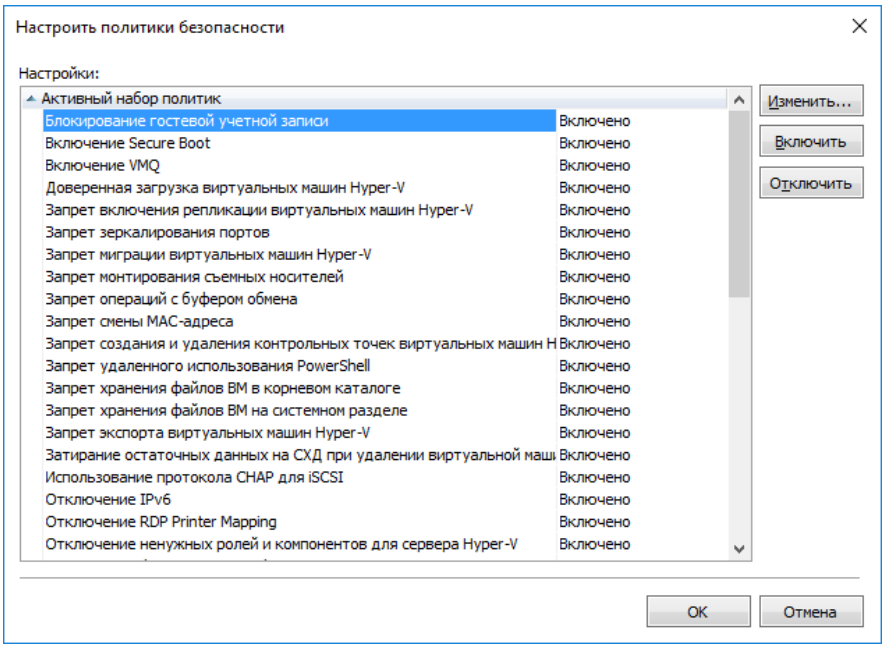
В наборе политик можно включить или отключить выбранную политику или сразу группу политик (выделив активный набор политик), а также изменить параметры политик.

Для большинства политик отключение с помощью консоли управления НЕ позволяет вернуть настройки сервера Hyper-V к первоначальному состоянию (до применения политики).

Для редактирования набора политик:

1. Выберите нужный набор и нажмите кнопку-ссылку "Изменить".

   На экране появится диалог, в котором отображается текущее состояние политик в наборе.



2. Для включения в редактируемый набор нового шаблона выделите название шаблона и нажмите кнопку "Включить".

   Все политики безопасности, входящие в указанный шаблон, получат статус "Включено".

> **Совет.**
> - Для отключения всех политик выбранного шаблона используйте кнопку "Отключить".
> - Чтобы добавить в набор отдельные политики из шаблона, дважды щелкните название шаблона, выделите нужную политику и нажмите "Включить".

3. При необходимости включите, отключите или измените отдельные политики из редактируемого набора, используя соответствующие кнопки.
4. После внесения всех необходимых изменений нажмите кнопку "ОК".

   В списке наборов политик будет обновлена информация о стандарте безопасности, которому соответствует отредактированный набор (о входящем в набор шаблоне).

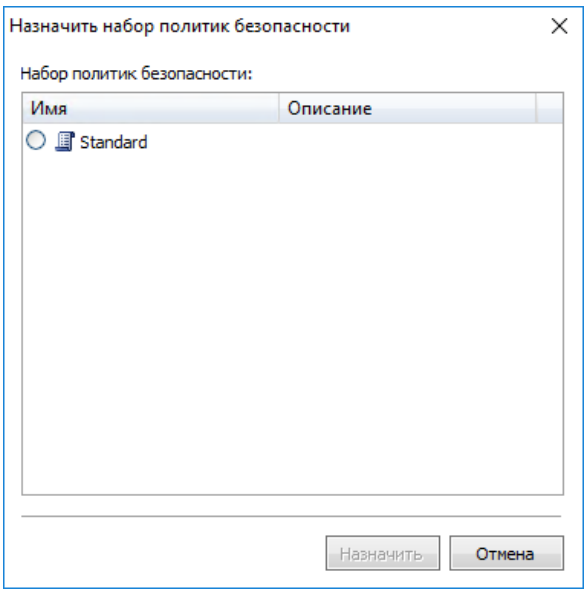
> **Примечание.** Если при редактировании набора были отключены политики, необходимые для защиты по стандарту безопасности "vGate for Hyper-V", в списке наборов политик для данного набора будет указан статус "Нет соответствий стандартам безопасности".

Назначение набора политик объекту или группе

Для назначения набора политик:

1. Выберите защищаемый vGate объект (виртуальную машину, сервер Hyper-V, сетевой адаптер, виртуальный коммутатор) или группу объектов, которым необходимо назначить политики.

   Нажмите кнопку "Назначить политики". На экране появится список настроенных администратором наборов политик.



2. Выберите нужный набор политик и нажмите кнопку "Назначить".

   Название набора политик, назначенного объекту, будет отображено в колонке "Наборы политик безопасности".

Примечание. Для отмены назначения набора политик используется кнопка-ссылка "Отменить назначение".

Управление доступом к защищаемым серверам

До выполнения этой процедуры требуется, чтобы были созданы нужные учетные записи пользователей и компьютеров, чей доступ к защищаемым объектам сети администрирования должен быть регламентирован. Для этого нужно:

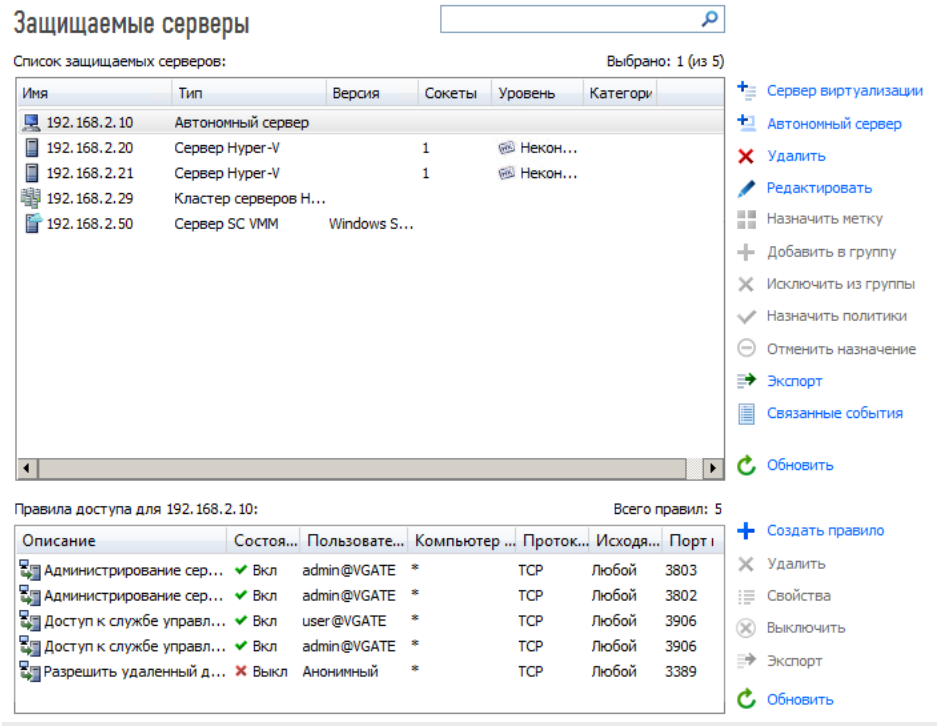
- зарегистрировать пользователей vGate (см. стр.**90**);
- при необходимости установить агенты аутентификации (см. стр.**11**) на компьютеры сервисных служб, которым требуются входящие соединения в защищаемый периметр для организации санкционированного доступа служб и сервисов компьютеров к защищаемым серверам Hyper-V и другим узлам защищаемой сети.

Внимание! После предоставления пользователям доступа к защищаемым серверам необходимо перевести vGate из тестового в штатный режим работы (см. стр.**85**).

Для предоставления доступа:

1. В консоли управления выберите функцию "Защищаемые серверы".

   В области параметров появится список серверов и соответствующий каждому из них список правил доступа.

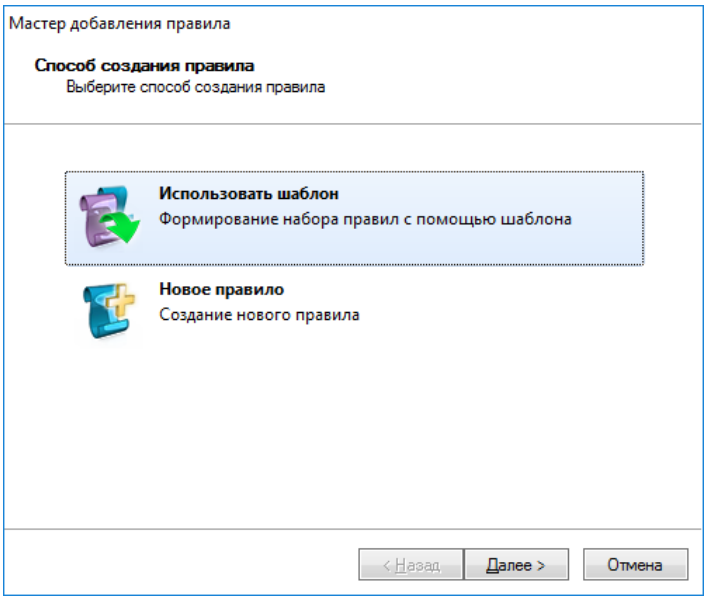


2. Выберите нужный сервер в таблице "Список защищаемых серверов".

   В нижней таблице отобразится список действующих правил.

3. Для создания правила нажмите кнопку-ссылку "Создать правило".

   На экране появится диалог мастера добавления правила.

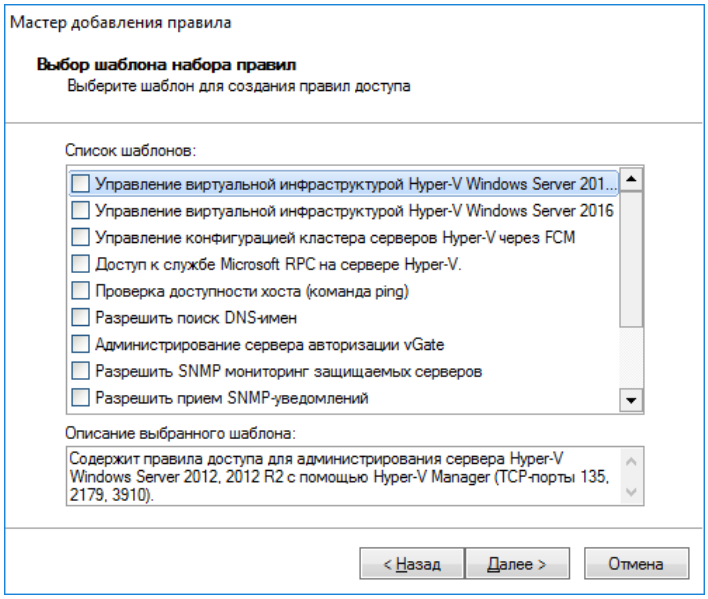


4. Выберите способ создания правила и нажмите "Далее >".

Способ	Описание
Использовать шаблон	Выбор готового набора правил из списка шаблонов, настроенных для разграничения доступа к различным объектам виртуальной инфраструктуры (см. стр.**117**)
Новое правило	Создание и ручная настройка нового правила (см. стр.**119**)

Создание правил на основе шаблона

Если на предыдущем шаге мастера был выбран вариант "Использовать шаблон", на экране появится диалог создания правил по шаблону.

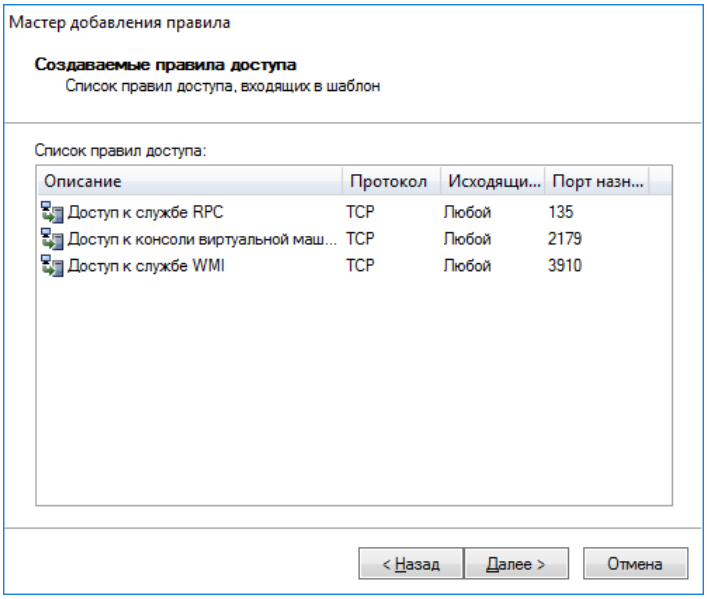


Примечание. Описание правил, входящих в каждый шаблон, приведено в приложении на стр.**164**.

Для создания правил по шаблону:

1. Выберите нужные шаблоны и нажмите кнопку "Далее >".

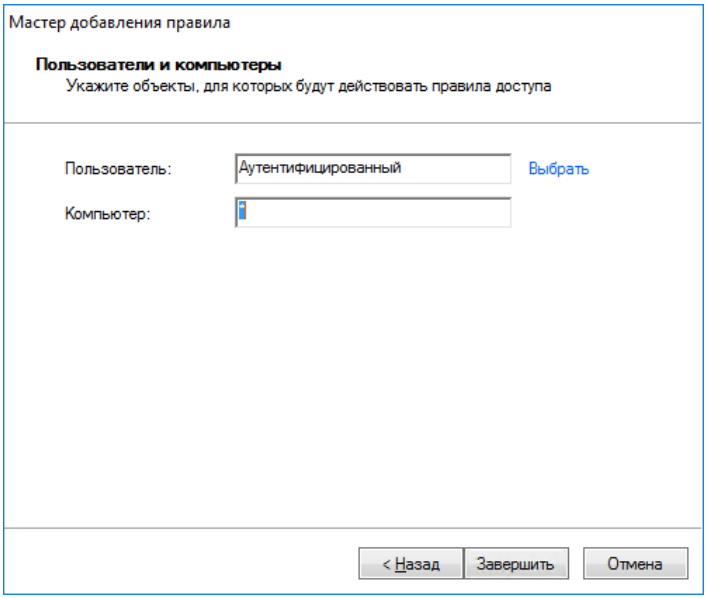
   На экране появится диалог со списком правил, входящих в выбранные шаблоны.



Список содержит правила доступа, определяющие параметры соединения.

2. Нажмите кнопку "Далее >".

   На экране появится следующий диалог.



3. Укажите пользователей и компьютеры, для которых будут действовать правила.

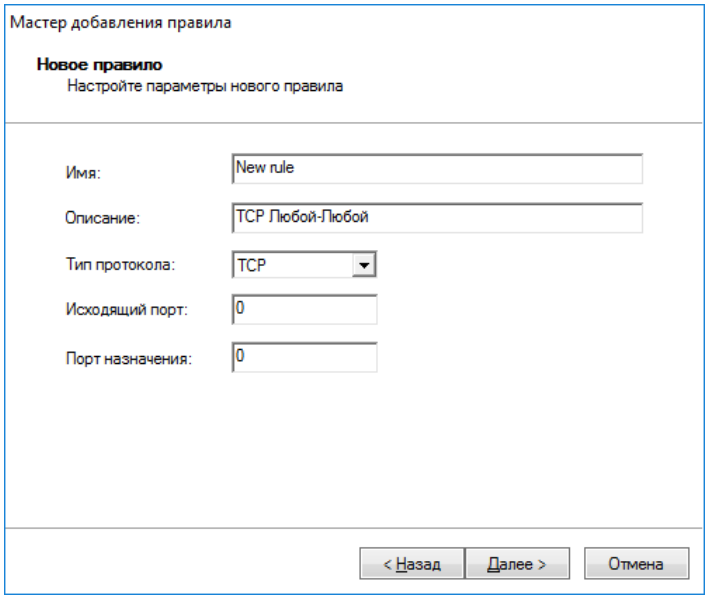
Параметр	Описание
Пользователь	Учетная запись пользователя или компьютера. Для выбора учетной записи нажмите кнопку-ссылку "Выбрать". В появившемся диалоге выберите зарегистрированную учетную запись. Если нужная учетная запись не зарегистрирована в консоли управления, то можно создать новую учетную запись, нажав кнопку "Создать" (см. стр.**92**), или добавить учетную запись из домена Active Directory с помощью кнопки "Добавить". Значение "Аутентифицированный" означает, что правила распространяются на все учетные записи пользователей и компьютеров, зарегистрированные в vGate или входящие в домен, который добавлен в список доверенных доменов на сервере авторизации vGate. Значение "Анонимный" означает, что для доступа по такому правилу аутентификация не требуется (доступно только если маршрутизацию трафика выполняет сервер авторизации). На аутентифицированных пользователей правила для анонимных пользователей не распространяются
Компьютер	Компьютер, с которого данному пользователю разрешен заданный доступ (для учетной записи компьютера не используется). Допустимые значения: NetBIOS-имя, DNS-имя, IP-адрес, символ "*" (звездочка указывает, что правило распространяется на любой компьютер)

4. Нажмите кнопку "Завершить".

   Правила доступа будут добавлены в список.

Создание нового правила

Если на предыдущем шаге мастера был выбран вариант "Новое правило", на экране появится диалог создания нового правила.

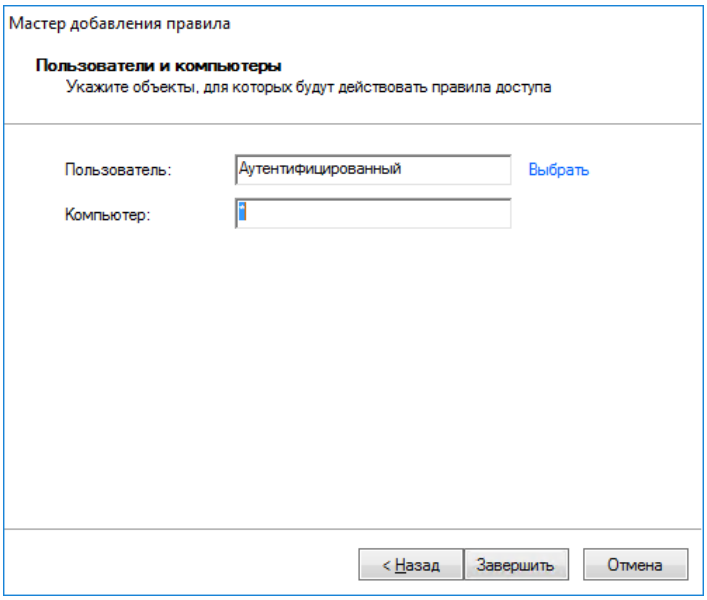


Для создания нового правила:

1. Укажите необходимые значения параметров и нажмите кнопку "Далее >".

Параметр	Описание
Имя	Имя правила
Описание	Описание правила (не является обязательным параметром)
Тип протокола	Тип протокола соединения: TCP, UDP, ICMP или IP level
Исходящий порт	Исходящий порт. Символ "0" (ноль) означает, что правило действует для всех портов
Порт назначения	Порт назначения. Символ "0" (ноль) означает, что правило действует для всех портов

На экране появится следующий диалог.



2. Укажите пользователей и компьютеры, для которых будет действовать правило.

Параметр	Описание
Пользователь	Учетная запись пользователя или компьютера. Для выбора учетной записи нажмите кнопку-ссылку "Выбрать". В появившемся диалоге выберите зарегистрированную учетную запись. Если нужная учетная запись не зарегистрирована в консоли управления, то можно создать новую учетную запись, нажав кнопку "Создать" (см. стр.**92**), или добавить учетную запись из домена Active Directory с помощью кнопки "Добавить". Значение "Аутентифицированный" означает, что правила распространяются на все учетные записи пользователей и компьютеров, зарегистрированные в vGate или входящие в домен, который добавлен в список доверенных доменов на сервере авторизации vGate. Значение "Анонимный" означает, что для доступа по такому правилу аутентификация не требуется (доступно только если маршрутизацию трафика выполняет сервер авторизации). На аутентифицированных пользователей правила для анонимных пользователей не распространяются
Компьютер	Компьютер, с которого данному пользователю разрешен заданный доступ (для учетной записи компьютера не используется). Допустимые значения: NetBIOS-имя, DNS-имя, IP-адрес, символ "*" (звездочка указывает, что правило распространяется на любой компьютер)

Если в сети маршрутизацию трафика выполняет отдельный маршрутизатор, то анонимные правила можно создать с помощью утилиты clacl.exe (см. стр.171).

3. Нажмите кнопку "Завершить".

   Правило доступа будет добавлено в список.

Настройка полномочного управления доступом к конфиденциальным ресурсам

Настройка полномочного управления доступом осуществляется в следующем порядке:

- выбираются и настраиваются допустимые метки безопасности (см. ниже);
- включается управление доступом по выбранному виду меток безопасности (см. стр.**76**);
- назначаются метки безопасности учетным записям пользователей и ресурсам (объектам виртуальной инфраструктуры) или группам объектов (см. стр.**99**).

Примечание. О настройке перечня типов объектов, для которых будет действовать механизм полномочного управления доступом (для которых будет проверяться соответствие меток безопасности), см. стр.79.

Внимание! Будьте внимательны при назначении меток. Если какому-либо пользователю или ресурсу не был назначен уровень конфиденциальности, то объект автоматически получает уровень конфиденциальности "неконфиденциально".

Выбор и настройка допустимых меток безопасности

При настройке функции полномочного управления доступом следует использовать метки одного вида. Подробнее о видах меток см. в разделе "Полномочное управление доступом к конфиденциальным ресурсам" документа [1].

Выбор допустимых меток безопасности определяется в зависимости от состава информации, обрабатываемой в виртуальной инфраструктуре:

- если в виртуальной инфраструктуре обрабатываются сведения, составляющие государственную тайну или относящиеся к персональным данным, следует использовать иерархические метки;
- если в виртуальной инфраструктуре **не** обрабатываются сведения, составляющие государственную тайну или относящиеся к персональным данным, рекомендуется использовать неиерархические метки.

Для более гранулированного разграничения доступа к объектам виртуальной инфраструктуры можно использовать составные метки. Например, составные метки можно использовать для разграничения доступа к персональным данным или сведениям, составляющим государственную тайну, обрабатываемым в разных отделах компании.

Внимание! Поскольку этот способ требует глубокого понимания логики работы функции и учета всех взаимосвязей между объектами виртуальной инфраструктуры, его не следует применять без особой необходимости.

В случае использования неиерархических меток необходимо включить возможность использования категорий конфиденциальности для управления доступом (см. стр. **76**). Кроме того, можно изменить список допустимых категорий конфиденциальности под свои задачи (подробнее о настройке списка категорий см. стр.**104**).

Пример. В качестве категорий можно использовать названия разных отделов компании (например, "Бухгалтерия", "Отдел разработки", "Отдел продаж", "Руководство"). Это позволит ограничить доступ персонала к ресурсам других отделов.

В случае использования составных меток следует настроить матрицу допустимых сочетаний уровней и категорий конфиденциальности (см. стр.**105**).

Общий порядок и правила назначения меток безопасности

Правила и последовательность назначения меток безопасности зависят от вида используемых меток, а также от состояния виртуальной инфраструктуры:

- новая виртуальная инфраструктура: серверы Hyper-V введены в эксплуатацию, подключены физические сетевые адаптеры, настроены хранилища и виртуальные коммутаторы, но виртуальные машины еще не созданы;
- виртуальная инфраструктура используется: на серверах Hyper-V запущены виртуальные машины.

На стр.**126** приведены примеры назначения меток безопасности объектам виртуальной инфраструктуры.

Правила и порядок назначения уровней конфиденциальности

При назначении иерархических меток (уровней конфиденциальности) для объектов виртуальной инфраструктуры следует придерживаться следующей последовательности действий и правил.

1. Задайте уровень конфиденциальности для каждой учетной записи АВИ в соответствии с уровнем допуска пользователя к конфиденциальным ресурсам.
2. Задайте уровень конфиденциальности каждому из защищаемых серверов Hyper-V в соответствии с уровнем конфиденциальности информации, которая будет обрабатываться на нем. Если на сервере Hyper-V планируется обрабатывать информацию разных уровней конфиденциальности, то:
   - отметьте поле "Разрешено исполнять ВМ с меньшим уровнем";
   - установите для сервера Hyper-V уровень конфиденциальности, равный максимальному уровню конфиденциальности обрабатываемой на нем информации.
3. Задайте уровень конфиденциальности каждому физическому сетевому адаптеру сервера Hyper-V. Если через один физический сетевой адаптер будет проходить трафик с виртуальных коммутаторов разных уровней конфиден-

циальности, то отметьте поле "Разрешено подключать коммутаторы с меньшим уровнем".

Примечание. Сценарий работы функции при смешивании трафика с виртуальных коммутаторов разных уровней конфиденциальности на физическом адаптере считается менее безопасным.

4. Если планируется использовать виртуальные сети (VLAN), добавьте их в консоли управления (см. стр. **124**) и назначьте уровень конфиденциальности каждой из них в соответствии с уровнем конфиденциальности передаваемой информации.
5. Задайте уровень конфиденциальности каждому виртуальному коммутатору сервера Hyper-V. Уровень конфиденциальности виртуального коммутатора должен быть:
   - не больше уровня конфиденциальности физического сетевого адаптера, к которому планируется подключать коммутатор (если в настройках уровня конфиденциальности физического адаптера отмечено поле "Разрешено подключать коммутаторы с меньшим уровнем");
   - равен уровню конфиденциальности физического сетевого адаптера, к которому планируется подключать коммутатор (если в настройках уровня конфиденциальности физического адаптера не отмечено поле "Разрешено подключать коммутаторы с меньшим уровнем").

   Если через один виртуальный коммутатор будет проходить трафик от виртуальных машин разных уровней конфиденциальности, то отметьте поле "Разрешено подключение ВМ с меньшим уровнем".
6. Задайте уровень конфиденциальности каждому из хранилищ ВМ в соответствии с уровнем конфиденциальности информации, которая будет в нем храниться. Если в хранилище планируется хранить информацию разных уровней конфиденциальности, то:
   - отметьте поле "Разрешено хранить ВМ с меньшим уровнем";
   - задайте уровень конфиденциальности хранилища, равный максимальному уровню конфиденциальности хранимой в нем информации.

   В случае назначения уровней конфиденциальности для объектов новой виртуальной инфраструктуры процедура окончена. Новые ВМ получат метки конфиденциальности автоматически при их создании. При этом ВМ назначается уровень конфиденциальности хранилища, на котором размещаются файлы ВМ. В случае назначения уровней конфиденциальности для объектов существующей виртуальной инфраструктуры перейдите к шагу **7**.
7. Задайте уровни конфиденциальности для всех существующих ВМ. Уровень конфиденциальности ВМ должен быть:
   - не выше уровня конфиденциальности сервера Hyper-V, на котором она выполняется (если в настройках уровня конфиденциальности сервера отмечено поле "Разрешено исполнять ВМ с меньшим уровнем"), или равен уровню сервера Hyper-V (если поле не отмечено);
   - не выше уровня конфиденциальности хранилища, на котором хранятся файлы ВМ (если в настройках уровня конфиденциальности хранилища отмечено поле "Разрешено хранить ВМ с меньшим уровнем"), или равен уровню конфиденциальности хранилища (если поле не отмечено);
   - не выше уровня конфиденциальности виртуального коммутатора, к которому планируется подключать данную ВМ (если в настройках уровня конфиденциальности коммутатора отмечено поле "Разрешено подключение ВМ с меньшим уровнем"), или равен уровню конфиденциальности виртуального коммутатора (если поле не отмечено).

   Если ВМ планируется перемещать на другой сервер Hyper-V, уровень конфиденциальности ВМ должен быть не выше уровня конфиденциальности этого сервера Hyper-V. Если ВМ имеет подключение к нескольким сетям, отметьте поле "Разрешено подключаться к сетям с меньшим уровнем".

Примечание. При создании новой ВМ с несколькими сетевыми картами проверяется соответствие уровней конфиденциальности ВМ, сетевых карт, VLAN, виртуальных коммутаторов и хранилища. Поэтому при создании ВМ с несколькими сетевыми картами рекомендуется сначала создать ВМ без сетевых карт, а потом создавать сетевые карты с нужными уровнями конфиденциальности.

В процессе дальнейшего функционирования виртуальной инфраструктуры АИБ должен своевременно назначать уровни конфиденциальности новым объектам, вводимым в виртуальную инфраструктуру (серверы Hyper-V, хранилища виртуальных машин, физические сетевые адаптеры, виртуальные сети, виртуальные коммутаторы), а также новым учетным записям пользователей.

Правила назначения категорий конфиденциальности

При назначении неиерархических меток (категорий конфиденциальности) для объектов виртуальной инфраструктуры следует придерживаться следующей последовательности действий и правил.

1. Задайте категории конфиденциальности для каждой учетной записи АВИ в соответствии с допуском пользователя к определенным категориям ресурсов. Каждый пользователь может быть допущен к одной или нескольким категориям ресурсов.
2. Задайте одну или несколько категорий конфиденциальности каждому из защищаемых серверов Hyper-V в соответствии с категорией конфиденциальности информации, которая будет обрабатываться на нем. Если на сервере Hyper-V будет обрабатываться информация разных категорий, то задайте список из этих категорий.
3. Задайте категорию конфиденциальности каждому физическому сетевому адаптеру сервера Hyper-V. При этом список категорий каждого из физических сетевых адаптеров должен иметь хотя бы одну общую категорию со списком категорий сервера Hyper-V.
4. Если планируется использовать виртуальные сети (VLAN), добавьте их в консоль управления и назначьте категории конфиденциальности каждой из них в соответствии с категорией конфиденциальности передаваемой в ней информации.
5. Задайте категорию конфиденциальности каждому виртуальному коммутатору в соответствии с категорией конфиденциальности. При этом список категорий каждого коммутатора должен иметь хотя бы одну общую категорию со списком категорий физического сетевого адаптера.
6. Задайте категории конфиденциальности каждому из хранилищ ВМ, равные категориям конфиденциальности хранящейся на них информации.

   В случае назначения категорий конфиденциальности для объектов новой виртуальной инфраструктуры процедура окончена. Новые ВМ получат метки конфиденциальности автоматически при их создании. При этом ВМ назначается категория из списка категорий хранилища, совпадающая с категорией из списка категорий пользователя, создающего ВМ. Если таковых несколько, то ВМ назначается список категорий. В случае назначения категорий конфиденциальности для объектов существующей виртуальной инфраструктуры перейдите к шагу **7**.
7. Задайте категории конфиденциальности для всех существующих ВМ. Список категорий ВМ должен иметь хотя бы одну общую категорию:
   - со списком категорий сервера Hyper-V, на котором она выполняется;
   - со списком категорий хранилища, на котором хранятся файлы ВМ.

Примечание. При создании новой ВМ с несколькими сетевыми картами проверяется соответствие категорий конфиденциальности ВМ, сетевых карт, VLAN, виртуальных коммутаторов и хранилища. Поэтому рекомендуется сначала создать виртуальные машины без сетевых карт, а потом создавать сетевые карты с нужными категориями конфиденциальности.

В процессе дальнейшего функционирования виртуальной инфраструктуры АИБ должен своевременно назначать категории конфиденциальности новым объектам, вводимым в виртуальную инфраструктуру (серверы Hyper-V, хранилища

виртуальных машин, физические сетевые адаптеры, виртуальные сети, виртуальные коммутаторы), а также новым учетным записям пользователей.

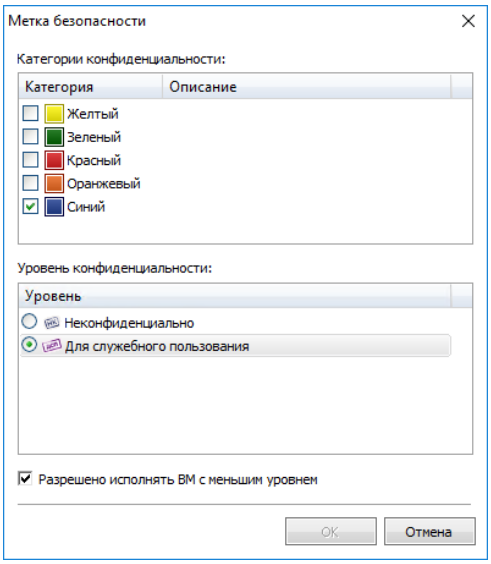
Назначение меток безопасности

Внимание! Перед назначением меток безопасности виртуальным сетям (VLAN) следует добавить их в список виртуальных сетей в консоли управления (см. стр.125).

Для назначения меток безопасности:

1. В консоли управления выберите объект, которому необходимо назначить метку безопасности.
2. Нажмите кнопку-ссылку "Назначить метку".

   На экране появится следующий диалог.



3. Укажите уровень и/или категории конфиденциальности, а также настройте перечисленные ниже дополнительные параметры (при необходимости). Нажмите кнопку "ОК".

Параметр	Описание
Разрешено исполнять ВМ с меньшим уровнем	Дополнительный параметр для серверов Hyper-V
Разрешено хранить ВМ с меньшим уровнем	Дополнительный параметр для хранилищ
Разрешено подключаться к сетям с меньшим уровнем	Дополнительный параметр для ВМ
Разрешено подключение ВМ с меньшим уровнем	Дополнительный параметр для виртуального коммутатора
Разрешено подключать коммутаторы с меньшим уровнем	Дополнительный параметр для физического сетевого адаптера
Разрешен доступ к объектам с меньшим уровнем	Дополнительный параметр для групп объектов

Внимание! Дополнительные параметры учитываются только в случае использования уровней конфиденциальности при настройке полномочного управления доступом.

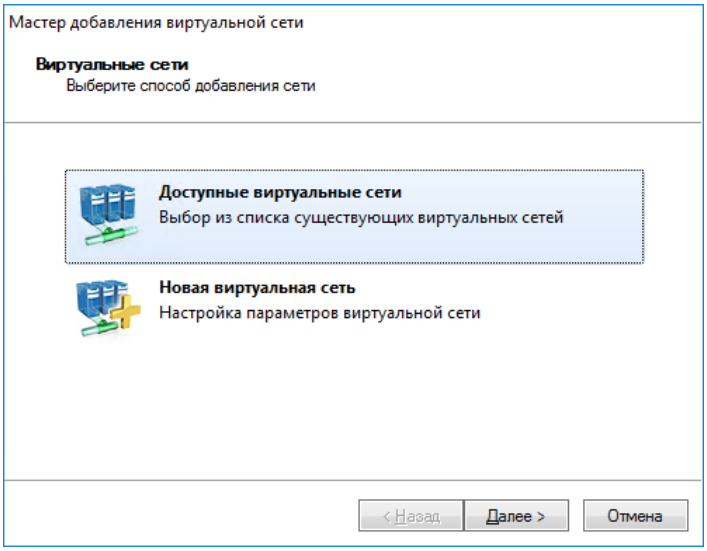
Особенности назначения меток виртуальным сетям

Перед назначением меток безопасности виртуальным сетям (VLAN) следует добавить их в список виртуальных сетей в консоли управления.

Для добавления виртуальной сети:

1. В консоли управления выберите функцию "Виртуальные сети" и нажмите кнопку-ссылку "Добавить".

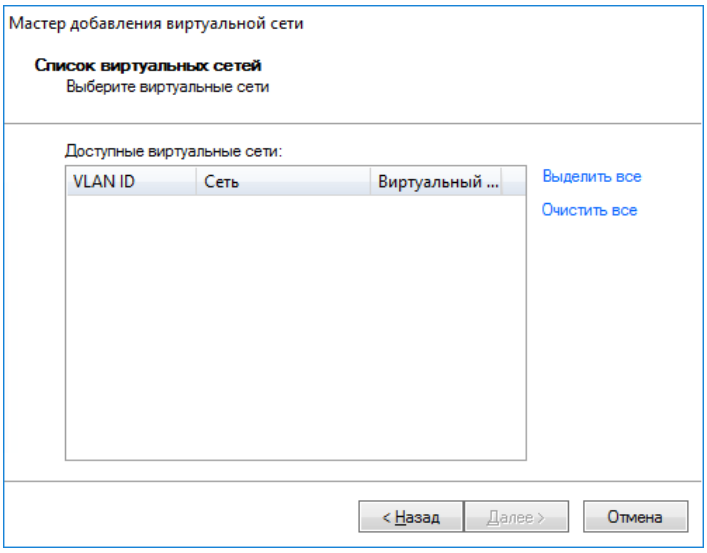
   На экране появится следующий диалог.



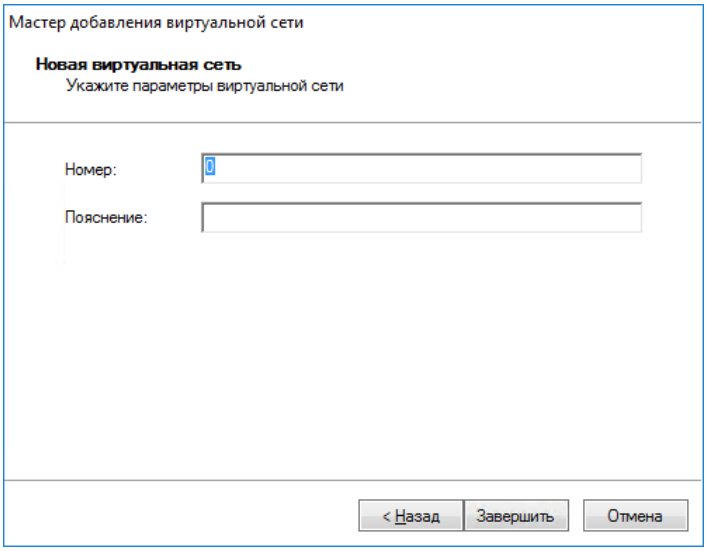
2. Выберите способ добавления виртуальной сети и нажмите "Далее >".

Способ	Описание
Доступные виртуальные сети	Выбор виртуальной сети из списка доступных сетей
Новая виртуальная сеть	Добавление новой виртуальной сети и настройка параметров

Если выбран вариант "Доступные виртуальные сети", на экране появится следующий диалог.



Если же выбран вариант "Новая виртуальная сеть", на экране появится следующий диалог.



3. Выберите виртуальную сеть (при добавлении существующей сети) или введите номер новой сети и пояснение (для добавления новой сети) и нажмите кнопку "Завершить".

   Виртуальная сеть будет добавлена.

Примеры назначения меток безопасности объектам виртуальной инфраструктуры

Пример 1. Использование уровней конфиденциальности

На рисунке приведен пример назначения уровней конфиденциальности объектам виртуальной инфраструктуры.

В примере 1 сервер Hyper-V используется для обработки как неконфиденциальной информации, так и конфиденциальных сведений. Поэтому серверу Hyper-V присвоен уровень конфиденциальности "для служебного пользования" и задан дополнительный параметр "Разрешено исполнять ВМ с меньшим уровнем".

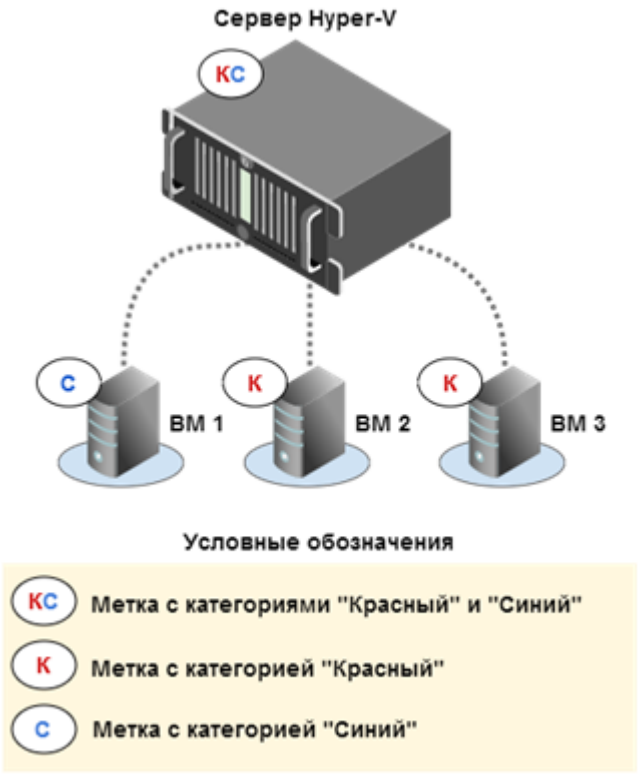
На сервере Hyper-V запущены три виртуальные машины:

- на ВМ 1 и ВМ 2 находится конфиденциальная информация;
- на ВМ 3 находится неконфиденциальная информация.

Виртуальным машинам назначен уровень конфиденциальности в соответствии с уровнем информации, которая на них находится ("для служебного пользования" и "неконфиденциально" соответственно).

Пример 2. Использование категорий конфиденциальности

На рисунке приведен пример назначения категорий конфиденциальности объектам виртуальной инфраструктуры.



В примере 2 сервер Hyper-V используется одновременно для обработки информации категорий "Синий" и "Красный".

На сервере Hyper-V запущены три виртуальные машины:

- на ВМ 1 находится информация категории "Синий";
- на ВМ 2 и ВМ 3 находится информация категории "Красный".

Серверу Hyper-V назначены категории "Синий" и "Красный". Виртуальным машинам назначены категории конфиденциальности в соответствии с категорией информации, которая на них находится ("Синий" и "Красный" соответственно).

Доступ к консоли ВМ

Доступ к консоли виртуальной машины может быть предоставлен или отменен индивидуально для каждого пользователя, зарегистрированного в консоли управления vGate.

Доступ регулируется

- свойством учетной записи "Пользователь виртуальных машин" (см. стр.**90**);
- механизмом полномочного управления доступом.

Свойство "Пользователь виртуальных машин" назначается пользователю по умолчанию и разрешает использование консоли на всех ВМ. Данное право доступа может быть отменено АИБ при создании или редактировании учетной записи пользователя в диалоге изменения свойств учетной записи (стр.**92**).

При попытке пользователя получить доступ к консоли ВМ выполняется проверка соответствия уровня сессии пользователя и уровня конфиденциальности виртуальной машины. Уровень конфиденциальности ВМ должен быть не выше уровня сессии пользователя. В противном случае доступ к консоли ВМ будет запрещен.

Контроль целостности

Объекты и методы контроля

В vGate средства контроля целостности (КЦ) используются для защиты следующих объектов на сервере авторизации, серверах Hyper-V и рабочих местах АВИ и АИБ.

Компонент	Объект контроля	Параметры и методы контроля
Сервер авторизации	Исполняемые модули vGate	Периодически проверяются: • целостность файла-шаблона с контрольными суммами; • целостность полного имени каждого файла, указанного в шаблоне; • целостность содержимого каждого файла, указанного в шаблоне. События нарушения КЦ на сервере авторизации регистрируются в базе данных vGate. Интервал проверки задается в секундах в реестре Windows, ключ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security Code\vGate\InchInterval в случае 64-разрядной версии Windows. По умолчанию интервал равен 600 сек. В случае нарушения КЦ сервера авторизации останавливается служба аутентификации vGate (aupa.exe) и служба проксирования трафика vGate (vcp.exe)
Агент аутентификации	Исполняемые модули vGate	Параметры контроля — как на сервере авторизации. События нарушения КЦ регистрируются в журнале приложений Windows (Application Event Log) на рабочем месте. В случае нарушения КЦ агента аутентификации останавливается служба аутентификации vGate (aupa.exe) на рабочем месте
Сервер Hyper-V	Исполняемые модули vGate	Как на сервере авторизации, за исключением остановки службы аутентификации vGate (aupa.exe) из-за нарушения КЦ. В случае нарушения КЦ компонента защиты Hyper-V останавливается служба vGate Hyper-V Config Server

Компонент	Объект контроля	Параметры и методы контроля
Сервер Hyper-V	Свойства ВМ	Контролируются: • поддерево контрольных точек (checkpoints) ВМ; • параметры конфигурации ВМ. Перечень контролируемых свойств ВМ задается в настройках политики "Доверенная загрузка виртуальных машин Hyper-V" (см. стр.**130**). Контроль целостности производится в момент старта ВМ, а также службой vGate Hyper-V Config Server через заданный интервал времени. Контрольные суммы свойств ВМ хранятся централизованно, в базе данных, для каждой виртуальной машины. Интервал проверки задается на сервере авторизации в реестре Windows, ключ HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate HvPolicyCheckTimeout [DWORD] (в сек.). По умолчанию интервал равен 600 сек.
Сервер SCVMM	Исполняемые модули vGate	Как на сервере авторизации, за исключением остановки службы аутентификации vGate (aupa.exe) из-за нарушения КЦ. В случае нарушения КЦ компонента защиты SCVMM останавливается служба vGate Hyper-V Config Server

Настройка контроля целостности ВМ

Внимание! Не рекомендуется включать на сервере авторизации контроль целостности более чем для 500 виртуальных машин одновременно.

Контроль целостности (КЦ) осуществляется только для тех ВМ, которым назначена политика "Доверенная загрузка виртуальных машин Hyper-V".

Настройка объектов контроля

vGate позволяет выполнить детальную настройку контроля целостности ВМ:

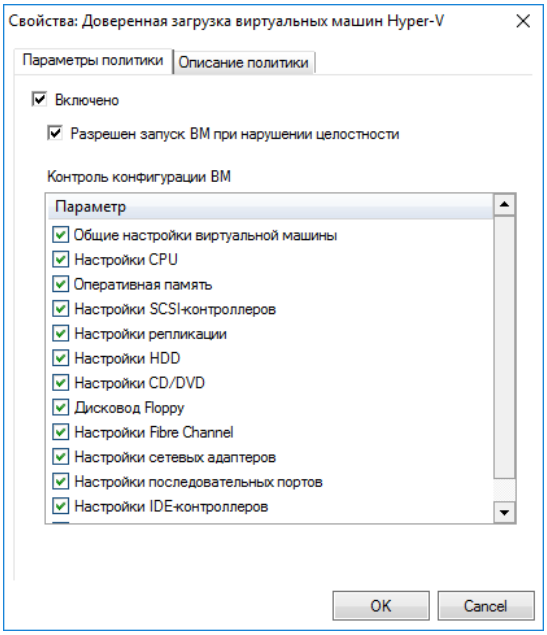
- разрешить или запретить запуск ВМ при нарушении целостности конфигурации;
- включить или отключить контроль поддерева контрольных точек ВМ;
- выбрать параметры конфигурации ВМ, изменение значений которых будет контролироваться политикой "Доверенная загрузка виртуальных машин Hyper-V".

Настройка выполняется в диалоге редактирования параметров политики "Доверенная загрузка виртуальных машин Hyper-V".

Для настройки параметров политики:

1. Выберите политику "Доверенная загрузка виртуальных машин Hyper-V" в списке политик и нажмите кнопку "Изменить".

   На экране появится диалог настройки параметров политики.



2. Отредактируйте параметры политики.

Параметр	Описание
Разрешен запуск ВМ при нарушении целостности	По умолчанию данный пункт отмечен. Удалите отметку, чтобы запретить запуск ВМ при несовпадении контрольных сумм файлов конфигурации ВМ, контролируемых настройками политики
Контроль конфигурации ВМ	Список свойств ВМ, контролируемых политикой. Удалите отметку в нужной строке списка, чтобы отменить контроль за изменением значений соответствующего свойства ВМ

3. После внесения всех изменений нажмите кнопку "ОК".

Внимание! При редактировании параметров политики "Доверенная загрузка виртуальных машин" нужно повторить назначение данной политики виртуальной машине.

Расчет контрольных сумм

Целостность ВМ контролируется компонентами защиты, установленными на сервер Hyper-V (см. стр.**89**).

Для каждой ВМ, на которую назначается политика "Доверенная загрузка виртуальных машин", рассчитывается эталонная контрольная сумма (КС), которая используется для контроля целостности. При миграции ВМ с другого сервера необходимо пересчитать КС, согласовав изменения виртуальной машины в консоли управления (см. стр.**130**), иначе будет зафиксировано нарушение целостности.

Контроль изменений и статус ВМ

На сервере Hyper-V каждые 10 минут (а также при запуске ВМ или при проверке политик вручную) выполняется сравнение эталонной контрольной суммы ВМ с текущей. При несовпадении контрольных сумм ВМ фиксируется нарушение целостности, изменяется статус ВМ (значение в колонке "Контроль целостности") и может быть запрещен запуск данной ВМ.

Внимание! Если политика "Доверенная загрузка виртуальных машин Hyper-V" назначена на кластеризованную ВМ, будет зафиксировано нарушение контроля целостности в следующих случаях:

- если кластеризованная ВМ мигрирует из-за отказа сервера Hyper-V;
- если для кластера серверов Hyper-V настроено правило доступа "Доступ к службе кластера. Порт назначения устанавливается автоматически".

Примечание. Запуск ВМ в случае несовпадения контрольных сумм не будет заблокирован, если в настройках политики "Доверенная загрузка виртуальных машин" отмечен пункт "Разрешен запуск ВМ при нарушении целостности" (данный вариант включен по умолчанию).

Администратор может в зависимости от статуса ВМ принять изменения (согласовать) либо отклонить их (см. стр. **130**). При согласовании изменений эталонная контрольная сумма ВМ заменяется текущей (т. е. контрольная сумма пересчитывается). Кроме того, при согласовании изменений в базе сохраняется текущий конфигурационный файл ВМ. При отклонении изменений текущий конфигурационный файл заменяется эталонным (сохраненным в базе при последнем согласовании).

Внимание! При отклонении изменений конфигурации ВМ будут также затронуты параметры, не контролируемые политикой "Доверенная загрузка виртуальных машин".

В таблице перечислены статусы ВМ, приведено их описание, а также указаны возможные действия администратора с ВМ.

Статус	Описание и доступные операции
Отключен	Контроль целостности для ВМ не настроен
Ошибка подсчета	В процессе подсчета контрольных сумм произошла ошибка. В зависимости от ошибки следует дождаться изменения статуса или выполнить согласование повторно. Если согласование недоступно, кнопка "Согласовать" будет недоступна. Если при выполнении пересчета контрольных сумм происходит ошибка, то ее причины могут быть выявлены при анализе записей в файле HvAdmConsole.exe.log, находящемся на сервере авторизации в каталоге установки продукта
Целостность нарушена	Целостность ВМ нарушена. Подробности о событии можно найти в сообщениях журнала событий (см. стр.**137**). При этом отклонение изменений недоступно, возможно только согласование изменений
В процессе согласования	Запущен процесс согласования изменений и расчет новых эталонных контрольных сумм
Целостность согласована	Согласование изменений выполнено
Изменены свойства ВМ	Свойства ВМ были изменены. Можно выполнить согласование или отклонение изменений

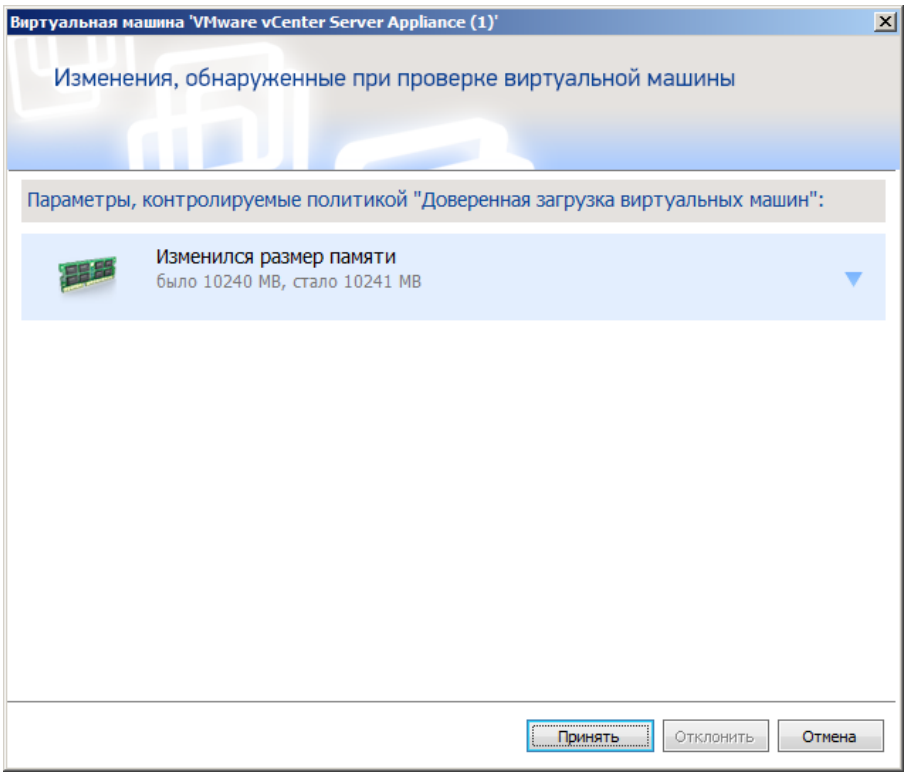
Согласование и отклонение изменений конфигурации ВМ

Внимание! Операции согласования и отклонения изменений рекомендуется выполнять, предварительно выключив виртуальную машину.

Для согласования и отклонения изменений:

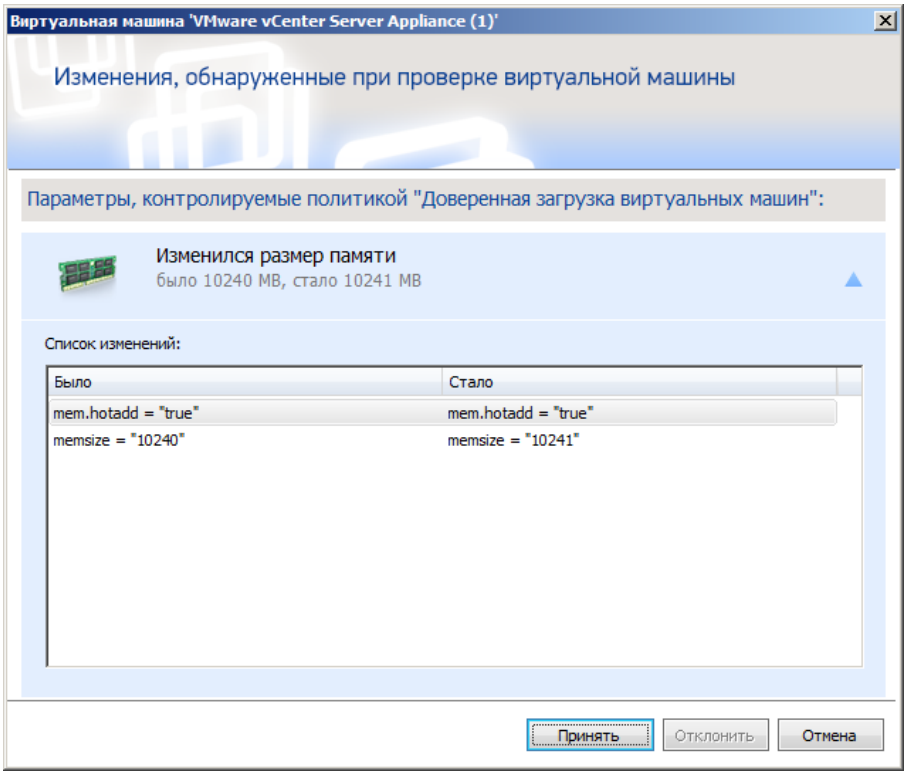
1. В консоли управления выберите функцию "Виртуальные машины".
2. Выберите в списке интересующую вас ВМ.
3. Для согласования изменений нажмите кнопку-ссылку "Согласовать".

На экране появится следующий диалог.



4. Нажмите на заголовок изменения, чтобы просмотреть подробную информацию о нем.

   На экране появится подробный список изменений.



5. Чтобы принять изменения, нажмите кнопку "Принять". Для отклонения изменений нажмите кнопку "Отклонить".

   Кнопка "Принять" может быть неактивна, если на сервере Hyper-V не завершена операция расчета контрольных сумм. Для согласования изменений необходимо дождаться активации кнопки "Принять".

   При отклонении изменений конфигурации ВМ будут также затронуты и не контролируемые политикой "Доверенная загрузка виртуальных машин" параметры.

   Кнопка "Отклонить" может быть неактивна, если статус виртуальной машины "Целостность нарушена".

   Система выполнит пересчет контрольных сумм всех файлов (компонентов) ВМ. После окончания операции на экране появится сообщение об этом.

6. Нажмите кнопку "ОК" в окне сообщения.

   Статус ВМ (значение в столбце "Контроль целостности") изменится.

Глава 6
Аудит событий безопасности

События безопасности регистрируются на всех защищаемых серверах, на которых установлены компоненты защиты vGate, а затем пересылаются на сервер авторизации для централизованного хранения.

На компьютерах внешнего периметра сети администрирования, на которых установлен агент аутентификации, сообщения хранятся локально в журнале приложений Windows (Application Event Log). Для их просмотра (локально или удаленно) необходимо использовать Windows Event Viewer.

Характеристики событий

Табл.1 Описание характеристик событий

Характеристика	Описание
Компоненты	
Служба аутентификации	События аутентификации
Служба контроля доступа к Hyper-V	События, связанные с работой компонента защиты Hyper-V
Служба контроля целостности	События, связанные с работой службы контроля целостности на всех компьютерах
Служба удаленного управления[1]	События, связанные с работой службы удаленного управления
Категории	
Аутентификация	События аутентификации (регистрируются попытки доступа к элементам управления виртуальной инфраструктурой)
Виртуальные машины Hyper-V	События, связанные с контролем доступа к виртуальной инфраструктуре Hyper-V (серверу Hyper-V и виртуальным машинам)
Общее	События, относящиеся к системе в целом. Например, события, связанные с превышением числа лицензий
Политики	События, касающиеся политик безопасности
Развертывание	События, относящиеся к установке модулей защиты сервера Hyper-V
Сегментирование	События, связанные с фильтрацией сетевого трафика
Служба	События, относящиеся к запуску или остановке служб (системных сервисов)
Управление доступом	События, связанные с правилами разграничения доступа
Целостность	События, связанные с нарушением контроля целостности
Типы	
Предупреждение	Предупреждение о неудачном выполнении действий, представляющих угрозу для безопасности системы
Успех	Сообщение об успешном выполнении действий, связанных с безопасностью системы

[1] Служба удаленного управления — специальный сервис, работающий на сервере авторизации и управляющий работой всех подсистем vGate, в том числе и работой серверов виртуализации. Консоль управления и утилита командной строки clacl.exe также работают через эту службу.

Характеристика	Описание
Уведомление	Сообщение об успешном выполнении действий, непосредственно не связанных с безопасностью системы
Ошибка	Сообщение о неудачном выполнении действий, непосредственно не связанных с безопасностью системы
Прочие	
Время	Время возникновения события
Компьютер	Компьютер, на котором зафиксировано событие
Код события	Уникальный числовой код события
Описание	Детальное описание события

Особенности регистрации событий, связанных с контролем целостности

Сервер авторизации
События нарушения КЦ на сервере авторизации регистрируются в базе данных vGate. Интервал проверки задается в реестре Windows, ключ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security Code\vGate InchInterval (в секундах). По умолчанию интервал равен 600 сек.
Рабочее место АВИ
События нарушения КЦ на АРМ АВИ регистрируются в локальном журнале Windows Application Event Log. Интервал проверки задается в реестре Windows, ключ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security Code\vGate InchInterval (в секундах). По умолчанию интервал равен 600 сек.
Рабочее место АИБ
События нарушения КЦ на АРМ АИБ регистрируются в локальном журнале Windows Application Event Log. Интервал проверки задается в реестре Windows, ключ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security Code\vGate InchInterval (в секундах). По умолчанию интервал равен 600 сек.
Сервер Hyper-V
События нарушения КЦ на серверах Hyper-V регистрируются в базе данных vGate. Интервал проверки задается в реестре Windows, ключ HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate InchInterval (в секундах). По умолчанию интервал равен 600 сек.

Примечание. Интервал проверки контроля целостности задается в ключе HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security Code\vGate InchInterval на компьютерах с 64-разрядной версией ОС Windows.

Просмотр журнала событий

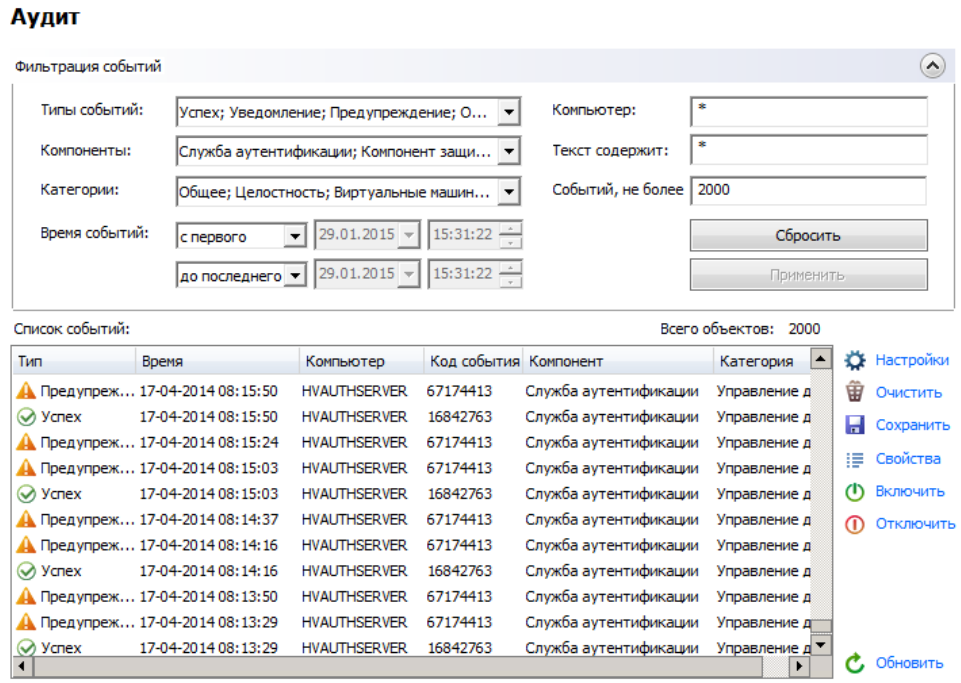
Список записей в журнале событий безопасности обновляется автоматически при выборе функции "Аудит" в консоли управления и через определенный период времени (по умолчанию равен 30 секундам). Отключить автоматическое обновление списка или изменить период между обновлениями можно в разделе "Конфигурация" (см. стр.**141**).

Для просмотра журнала событий безопасности:

1. В окне консоли управления выберите функцию "Аудит".

   В области просмотра параметров появится таблица со списком событий, а над ней — группа параметров для формирования условий отбора записей.

> **Совет.** При первом выборе функции "Аудит" после запуска консоли управления область параметров фильтрации записей скрыта. Чтобы раскрыть данную область, нажмите кнопку справа от заголовка "Фильтрация событий".



2. Укажите условия отбора записей:

   - Каждое регистрируемое событие описывается рядом характеристик (см. стр.**135**). Для выбора параметров отбора записей установите отметки рядом с названиями нужных характеристик в раскрывающихся списках "Типы событий", "Компоненты" и "Категории". При необходимости выберите период времени регистрации событий в полях "Время событий".
   - Для ограничения длины списка событий укажите нужное значение в поле "Событий, не более". По умолчанию в списке отображаются 2000 последних записей.
   - Для возврата к набору параметров фильтрации записей, предлагаемому по умолчанию, нажмите кнопку "Сбросить".

> **Совет.** Для быстрого отбора событий, относящихся к определенному объекту виртуальной инфраструктуры, выберите нужную функцию консоли управления, выберите нужный объект и нажмите кнопку-ссылку "Связанные события" (подробнее см. стр.**138**).

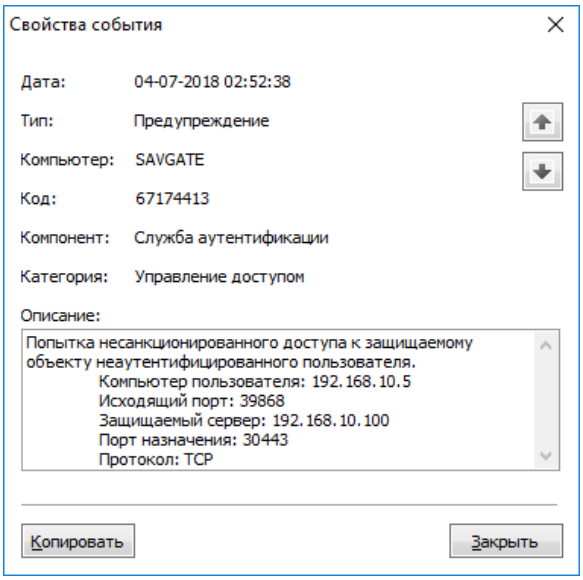
3. Нажмите кнопку "Применить".

   Соответствующий перечень записей появится в таблице "Список событий".

4. Для детального просмотра отдельных записей выделите нужную запись и нажмите кнопку-ссылку "Свойства".

Совет. Для просмотра свойств события можно дважды нажать строку записи.

На экране появится следующий диалог.



Совет.

- Кнопка "Копировать" позволяет скопировать содержимое всех полей события в буфер обмена, откуда его можно обычным образом вставить в любой текстовый редактор.
- Для быстрого перехода между диалогами свойств соседних событий используйте кнопки и .

5. Завершив детальный просмотр событий, нажмите кнопку "Закрыть".

Просмотр связанных событий для выбранного объекта

По умолчанию перечень событий содержит записи, относящиеся ко всем объектам виртуальной инфраструктуры. При необходимости АИБ может получить быстрый доступ к списку событий, связанных с определенным объектом (защищаемый сервер, виртуальная машина, хранилище данных, виртуальная сеть, виртуальный коммутатор, сетевой адаптер, учетная запись пользователя).

Для просмотра связанных событий безопасности:

1. В консоли управления выберите функцию, соответствующую нужному объекту: "Защищаемые серверы", "Виртуальные машины", "Хранилища данных", "Виртуальные сети", "Виртуальные коммутаторы", "Сетевые адаптеры" или "Учетные записи".
2. В области параметров выберите нужный объект и нажмите кнопку-ссылку "Связанные события".

На экране появится таблица со списком событий безопасности, относящихся к выбранному объекту. В группе параметров отбора записей в поле "Текст содержит" будет указано свойство выбранного объекта, на основании которого был выполнен отбор связанных с объектом событий.

Объект	Свойство
Защищаемый сервер	IP-адрес сервера. Например: 192.168.2.2
Виртуальная машина	Идентификатор (UUID) виртуальной машины. Например: fab1ef6c-60eb-4028-8f16-506fe07f400f
Хранилище данных	Идентификатор хранилища данных. Например: 9dc9bed5-d90c-11e2-93e8-806e6f6e6963
Виртуальная сеть	Идентификатор виртуальной сети (VLAN ID). Например: VLAN ID: 1
Виртуальный коммутатор	Идентификатор виртуального коммутатора. Например: 01C450FC-593E-4913-BFA6-3111E98405B6
Сетевой адаптер	MAC-адрес сетевого адаптера. Например: 00:0c:29:cf:c2:39
Учетная запись	Имя учетной записи пользователя. Например: user@VGATE

Совет. Для отмены фильтрации связанных событий и просмотра полного перечня событий безопасности нажмите символ ✕ в поле "Текст содержит", а затем кнопку "Применить".

Сохранение журнала событий

Для сохранения журнала событий безопасности:

1. В окне консоли управления выберите функцию "Аудит".
   В области просмотра параметров появится таблица со списком событий.
2. Нажмите кнопку-ссылку "Сохранить".
   На экране появится диалог выбора пути для сохранения файла.
3. Задайте имя файла и нажмите кнопку "Сохранить" ("Save").
   События будут сохранены в файле формата .txt.

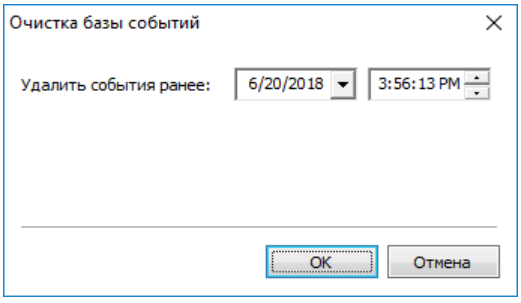
Примечание. Сохранение большого количества событий может занять длительное время.

Очистка журнала событий

Совет. Перед очисткой журнала можно сохранить журнал событий в файл (см. выше).

Для очистки журнала событий безопасности:

1. В окне консоли управления выберите функцию "Аудит".
   В области просмотра параметров появится таблица со списком событий.
2. Нажмите кнопку-ссылку "Очистить".
   На экране появится следующий диалог.



3. Укажите дату и время и нажмите кнопку "ОК".

   Записи о событиях, зафиксированных ранее указанной даты, будут удалены из журнала.

Настройка списка регистрируемых событий

По умолчанию в журнале vGate регистрируются все возможные события информационной безопасности. Если такой детальный мониторинг не требуется, АИБ может отключить те события, регистрация которых не нужна (например, настроить только регистрацию ошибок).

Примечание. События, соответствующие неудачным попыткам аутентификации пользователя Active Directory, не регистрируются в журнале сервера авторизации vGate. Для регистрации таких событий требуется настроить на контроллере домена политику "Аудит событий входа в систему" (Audit account logon events). Просмотр событий осуществляется на контроллере домена в аудите.

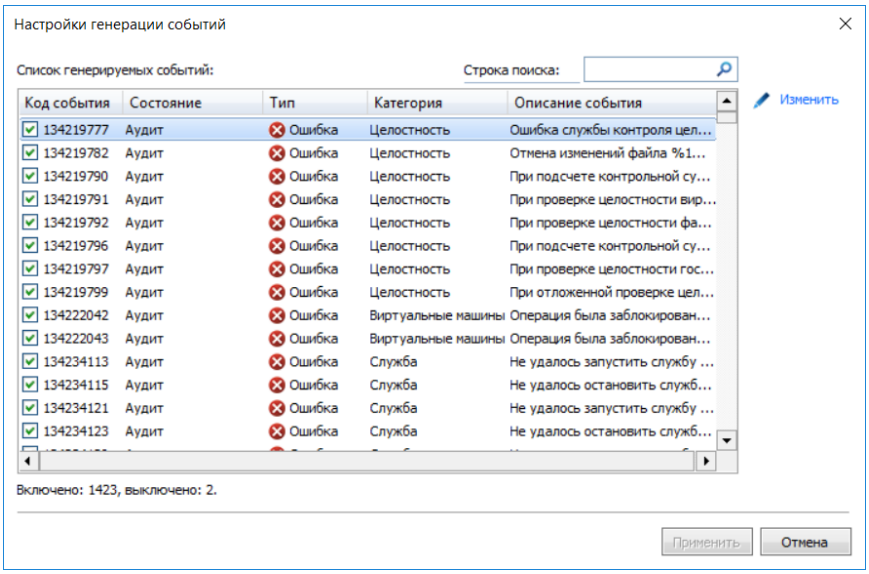
Для настройки параметров регистрации событий безопасности:

1. В окне консоли управления выберите функцию "Аудит".

   В области просмотра параметров появится таблица со списком событий.

2. Нажмите кнопку-ссылку "Настройки".

   На экране появится следующий диалог.



3. Настройте список регистрируемых событий. Для отмены регистрации какого-либо события удалите отметку слева от кода нужного события. Для включения регистрации какого-либо события установите отметку слева от кода нужного события.
4. По завершении настройки списка регистрируемых событий нажмите кнопку "Применить".

Совет. Корректировать список регистрируемых событий можно также из области просмотра параметров функции "Аудит" с помощью кнопок "Включить" и "Отключить".

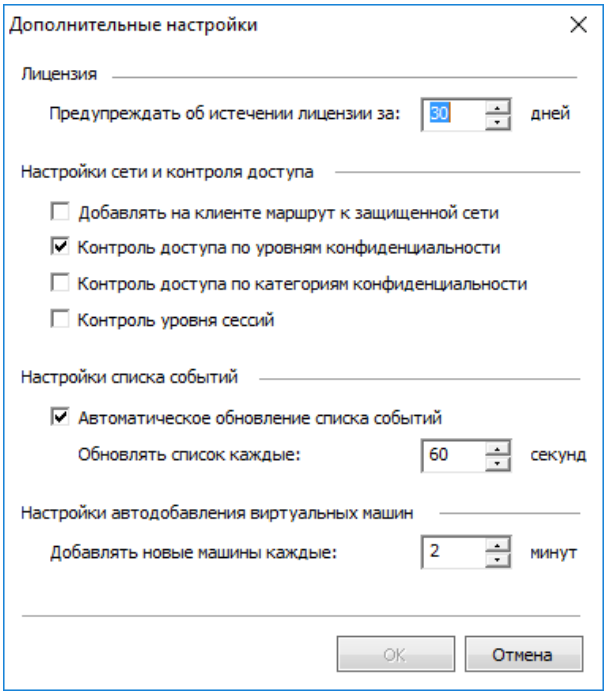
Настройка автоматического обновления списка событий

Список записей в журнале событий безопасности обновляется автоматически при выборе функции "Аудит" в консоли управления и через определенный период времени (по умолчанию равен 30 секундам). При необходимости настройки автоматического обновления могут быть изменены.

Для настройки обновления списка событий:

1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Настройки сети, контроля доступа, лицензирования".

   На экране появится диалог настройки дополнительных параметров.



3. Настройте параметры автоматического обновления списка событий и нажмите кнопку "ОК".

Параметр	Описание
Автоматическое обновление списка событий	Удалите отметку из этого поля, чтобы отключить автоматическое обновление списка событий безопасности. В этом случае обновление списка будет происходить только при выборе функции "Аудит", а также при нажатии кнопки-ссылки "Обновить" или кнопки-ссылки "Связанные события"
Обновлять список каждые ... секунд	Период времени между обновлениями списка событий (в секундах). По умолчанию равен 30 сек.

Интеграция vGate с системами SIEM

vGate может отправлять события безопасности в системы SIEM (Security information and event management). Для отправки сообщений используется протокол Syslog.

Сообщение содержит переменные (код события, категорию, идентификатор приложения, имя сервера и т.д.), но не содержит описание события. Для получения описания события в SIEM необходимо воспользоваться базой управляющей информации (MIB). Файл базы MIB находится на установочном диске vGate. Импорт базы данных осуществляется с помощью SIEM-системы.

Пример:

Ошибка аутентификации одного из сервисов vGate в файле базы MIB будет описана следующим образом:

```
rhuidAuthFailed TRAP-TYPE
ENTERPRISE vgateTraps
VARIABLES
{
vgateMessageSeverity,
vgateMessageCategory,
vgateApplicationID,
vgateHostName,
vgateMessageDatetime,
vgateVar1,
vgateVar2,
vgateVar3
}
DESCRIPTION
"Authentication failed. User: vgateVar1 Address: vgateVar2
Reason: vgateVar3"

--#TYPE "Authentication failed. (67117057)"
--#SEVERITY MINOR
--#CATEGORY "Authentication events"

::= 67117057
```

где

- **vgateMessageSeverity** — код, возможные значения описаны в файле базы MIB;
- **vgateMessageCategory** — категория сообщения, возможные значения описаны в файле базы MIB;
- **vgateApplicationID** — идентификационный номер приложения, возможные значения описаны в файле базы MIB;
- **vgateHostName** — имя сервера, с которого отправлено сообщение;
- **vgateMessageDatetime** — время отправления сообщения;
- **vgateVar1, vgateVar2, vgateVar3** — переменные, значение которых заранее неизвестно. Например, имя пользователя или виртуальной машины.

В систему SIEM будут оправлены код сообщения (67117057) и все переменные из списка "VARIABLES" в исходной последовательности.

Глава 8
Веб-консоль

ПО vGate 4.4 включает в себя веб-консоль для управления и мониторинга событий безопасности.

Чтобы открыть веб-консоль vGate, запустите браузер и введите следующий URL-адрес:

https://<server-IP>

где <server-IP> — IP-адрес сервера авторизации.

Доступ к веб-приложению возможен из сети администрирования с помощью учетной записи АИБ. Поддерживается работа веб-приложения в следующих браузерах:

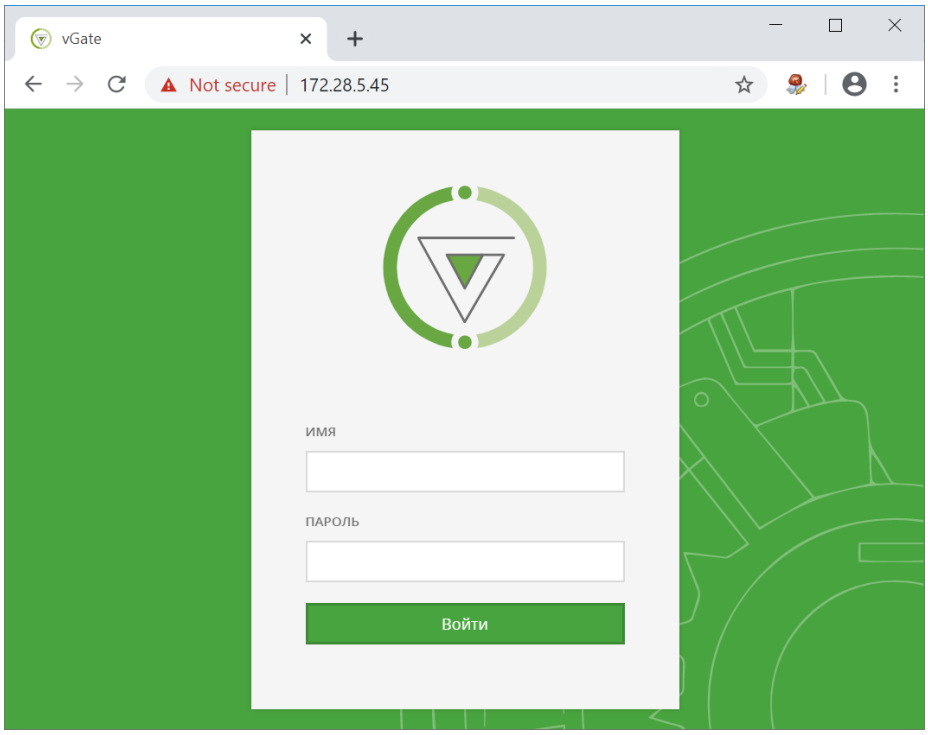
- Chrome версии 83.0.4103.61 (64-bit);
- Firefox версии 76.0.1 (64-bit);
- Opera версии 67.0.3575.79;
- Яндекс.Браузер версии 20.4.3.255 (64-bit).

Внимание! При подключении к серверу мониторинга из внешнего периметра сети администрирования в консоли управления vGate необходимо добавить правило, разрешающее пользователю доступ к серверу авторизации по протоколу TCP и порту 443 (см. стр.115). Чтобы изменить порт, используемый по умолчанию, откройте файл vGate\Web\vgate.webapp.zip\app\config\app.conf и добавьте в него следующую секцию:

```
httpd: {
port: <new port number>
}
```

После этого перезапустите службу веб-консоли vGate (vgate.webapp).

Откроется начальная страница веб-приложения.



Укажите логин и пароль АИБ и нажмите кнопку "Войти". Откроется веб-консоль vGate.

Примечание. Если срок действия пароля истек, откроется окно изменения пароля (см. стр.160).

Главное меню веб-консоли состоит из следующих разделов:

- Сегментирование (только для виртуальных машин VMware);
- Мониторинг (см. стр.**144**);
- Отчеты (только для среды VMware vSphere);
- Журнал событий (см. стр.**154**);
- Учетные записи (см. стр.**154**);
- Соответствие политикам (только для среды VMware vSphere);
- Настройки (см. стр.**156**).

Мониторинг безопасности

Функция мониторинга безопасности доступна только в vGate Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Мониторинг безопасности vGate позволяет осуществлять сбор и анализ данных о событиях на объектах виртуальной инфраструктуры: сервере авторизации vGate, защищаемых серверах, компьютерах сети администрирования, на которых установлен агент аутентификации vGate.

Подключение к серверу мониторинга

Для работы функции мониторинга необходимо выполнить подключение к серверу мониторинга vGate, развернутому в сети (см. стр.**49**). Настройка подключения описана на стр.**159**.

Панель мониторинга

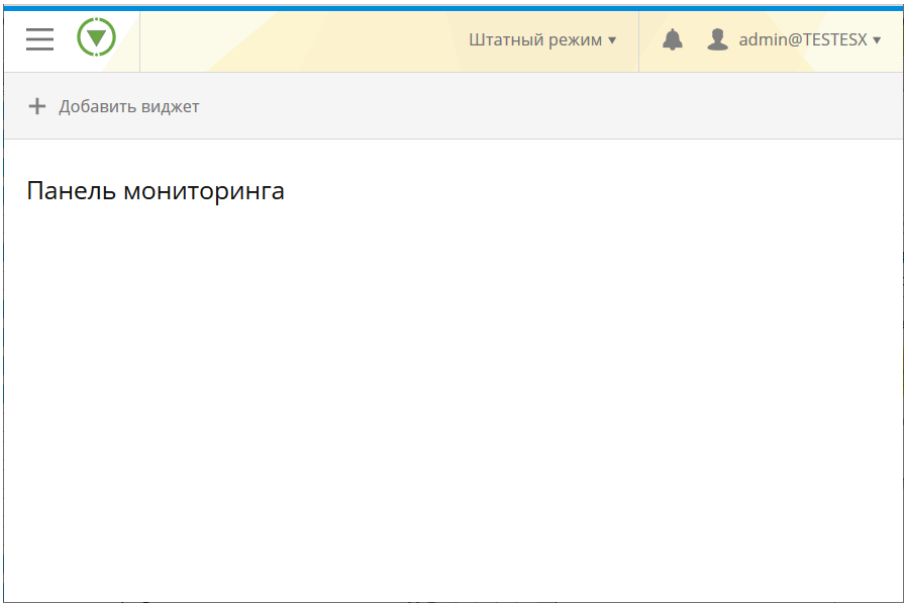
Панель мониторинга представляет собой настраиваемый набор виджетов-диаграмм. Диаграммы в графическом виде отображают данные о событиях и инцидентах, происходящих в виртуальной инфраструктуре.

Примечание. Порядок виджетов может быть изменен с помощью метода "Drag-and-drop" (перемещение с помощью мыши).

Чтобы настроить панель мониторинга:

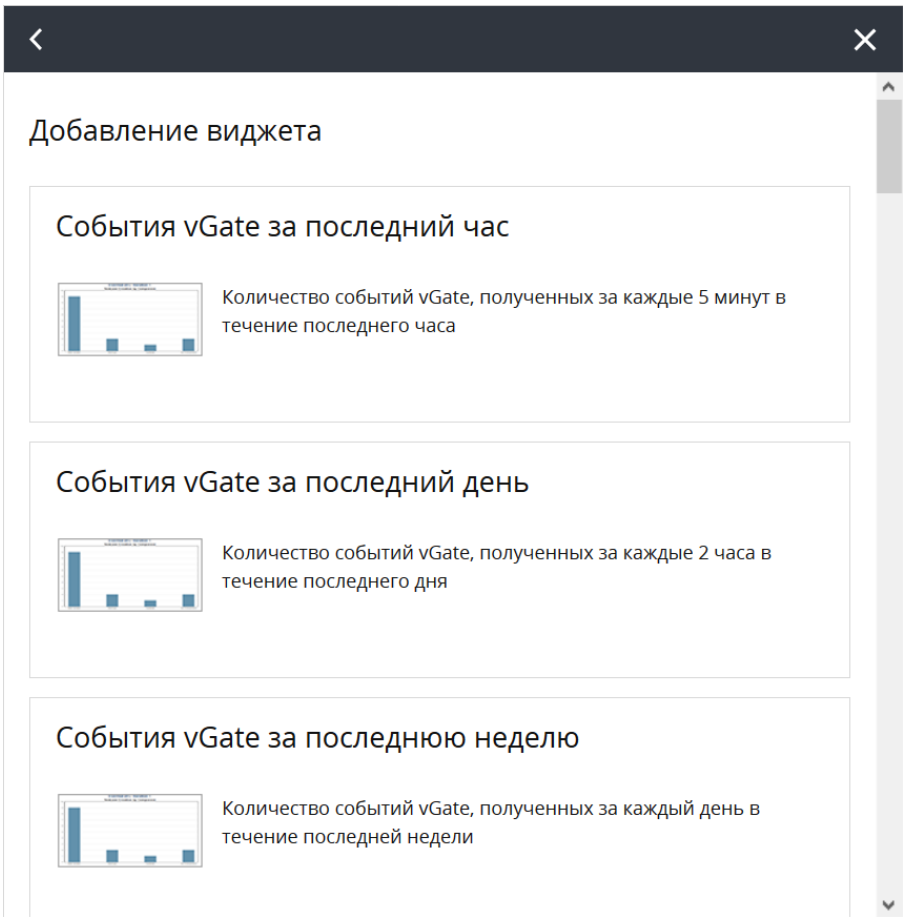
1. В главном меню выберите раздел "Мониторинг", а затем "Панель мониторинга".

   На экране появится окно.



2. Нажмите кнопку "Добавить виджет".

Откроется панель добавления виджетов.

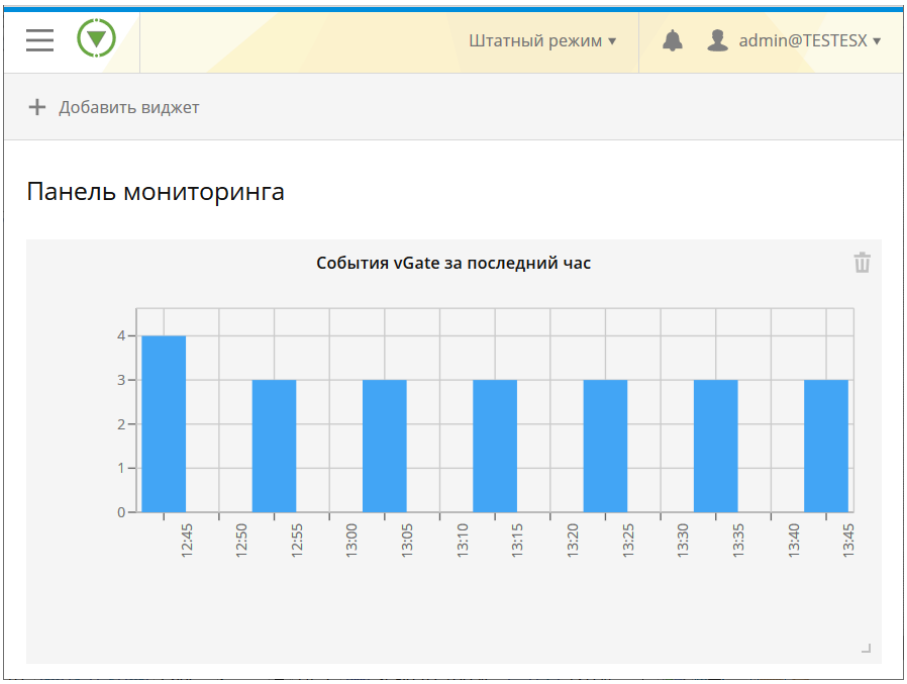


3. Выберите из списка виджет, который необходимо отображать на панели мониторинга.

Виджет	Описание
События vGate за последний час	Количество событий vGate, полученных за каждые 5 минут в течение последнего часа
События vGate за последний день	Количество событий vGate, полученных за каждые 2 часа в течение последнего дня
События vGate за последнюю неделю	Количество событий vGate, полученных за каждый день в течение последней недели
События vGate за все время	Количество событий vGate, полученных за каждый месяц в течение всего времени
События безопасности vGate	Все события vGate, распределенные по типу
Наиболее активные пользователи vGate	Информация о 10 наиболее активных пользователях vGate
Проблемы доступа в vGate	Информация о неудачных попытках аутентификации в vGate. В статистике учитываются 10 IP-адресов, с которых было произведено больше всего неудачных попыток доступа
Проблемы в работе vGate	Информация об ошибках и проблемах, произошедших при работе vGate
Нарушение правил фильтрации сетевых подключений	Информация о попытках несанкционированного доступа с нарушением правил фильтрации сетевых подключений. В статистике учитываются 10 IP-адресов, с которых было произведено больше всего неудачных попыток доступа

Виджет	Описание
Нарушение мандатных правил доступа VMware	Только для среды VMware vSphere
Нарушение мандатных правил доступа Hyper-V	Информация о попытках несанкционированного доступа с нарушением мандатных правил разграничения доступа Hyper-V. В статистике учитываются 10 пользователей, чаще других совершавших неудачные попытки доступа
Инциденты	Количество произошедших инцидентов, распределенных по степени их критичности
Нарушение целостности VMware	Только для среды VMware vSphere
Нарушение целостности Hyper-V	Количество событий, связанных с нарушением целостности файлов виртуальных машин Hyper-V
Действия в обход vGate	Количество операций в виртуальной инфраструктуре, совершенных в обход vGate, распределенных по степени их критичности
Создание виртуальных машин VMware	Только для среды VMware vSphere
Создание виртуальных машин Hyper-V	Информация о событиях создания виртуальных машин Hyper-V. В статистике учитываются 10 хранилищ, на которых было создано больше всего виртуальных машин
Соответствие наборам политик безопасности	Информация о соответствии защищаемых объектов наборам политик безопасности
Миграция виртуальных машин VMware	Только для среды VMware vSphere
Миграция виртуальных машин Hyper-V	Информация о событиях миграции виртуальных машин Hyper-V. В статистике учитываются 10 виртуальных машин, которые мигрировали чаще всего
ESXi-серверы с включенным компонентом фильтрации трафика	Только для среды VMware vSphere
Виртуальные машины, для которых осуществляется контроль трафика	Только для среды VMware vSphere
Активные правила фильтрации	Только для среды VMware vSphere
Статистика срабатывания правил фильтрации	Только для среды VMware vSphere
Соответствие ESXi-серверов стандартам безопасности	Только для среды VMware vSphere
Разрешенный трафик между сегментами	Только для среды VMware vSphere
Заблокированный трафик между сегментами	Только для среды VMware vSphere

Выбранная диаграмма появится на экране.



4. Повторите действия, описанные в пп. 2, 3, чтобы добавить на панель мониторинга все нужные виджеты.

Примечание. Чтобы удалить виджет с панели мониторинга, нажмите значок "Корзина" в правом верхнем углу виджета.

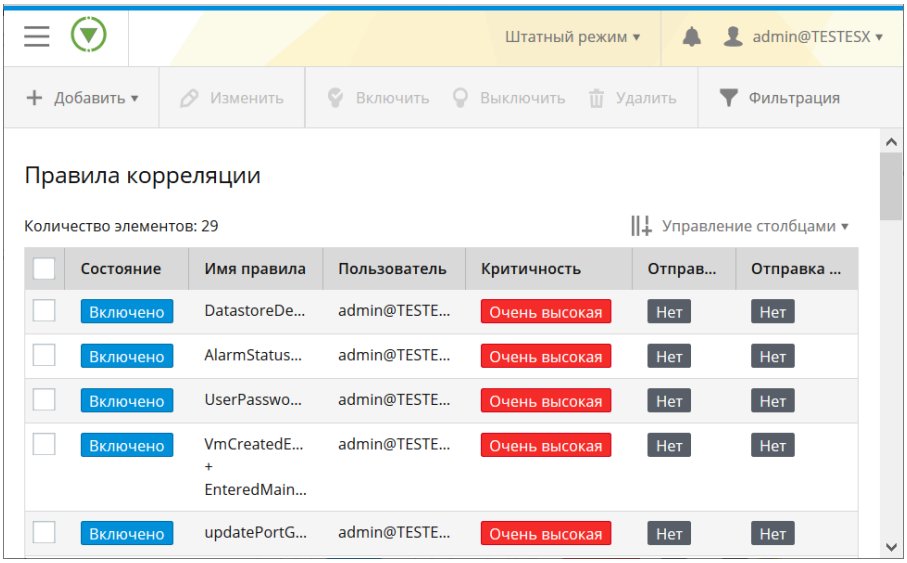
Создание правил корреляции

Правила корреляции позволяют отслеживать конкретные события, происходящие при заданных условиях в виртуальной инфраструктуре. При срабатывании правил создаются инциденты.

Для создания правила:

1. В главном меню выберите раздел "Мониторинг" и перейдите на вкладку "Правила корреляции".

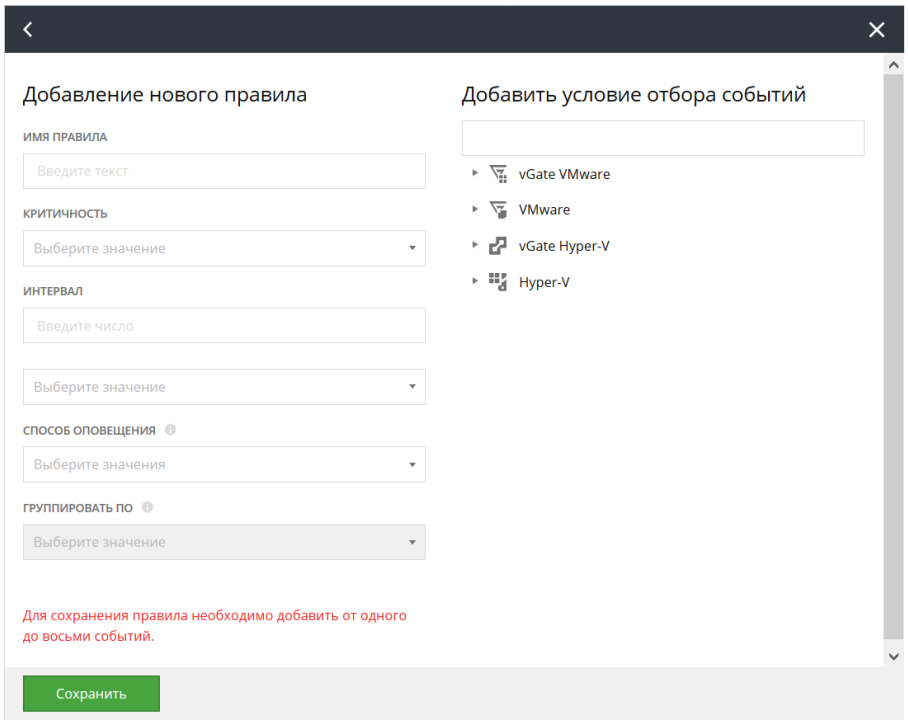
   На экране появится окно.



2. Нажмите кнопку "Добавить", в выпадающем списке выберите нужное действие:
   - Добавить правило (см. стр.**148**);
   - Добавить правило по шаблону (см. стр.**150**);
   - Добавить правило в обход vGate (см. стр.**152**).

Совет.
- Используйте кнопки "Выключить" и "Включить", чтобы управлять работой правила. Чтобы удалить правило, нажмите кнопку "Удалить". Чтобы редактировать параметры правила, нажмите кнопку "Изменить".
- Для использования фильтров нажмите кнопку "Фильтрация", в появившемся окне введите текст для поиска в нужное поле и нажмите кнопку "Применить".
- Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.

Добавление нового правила

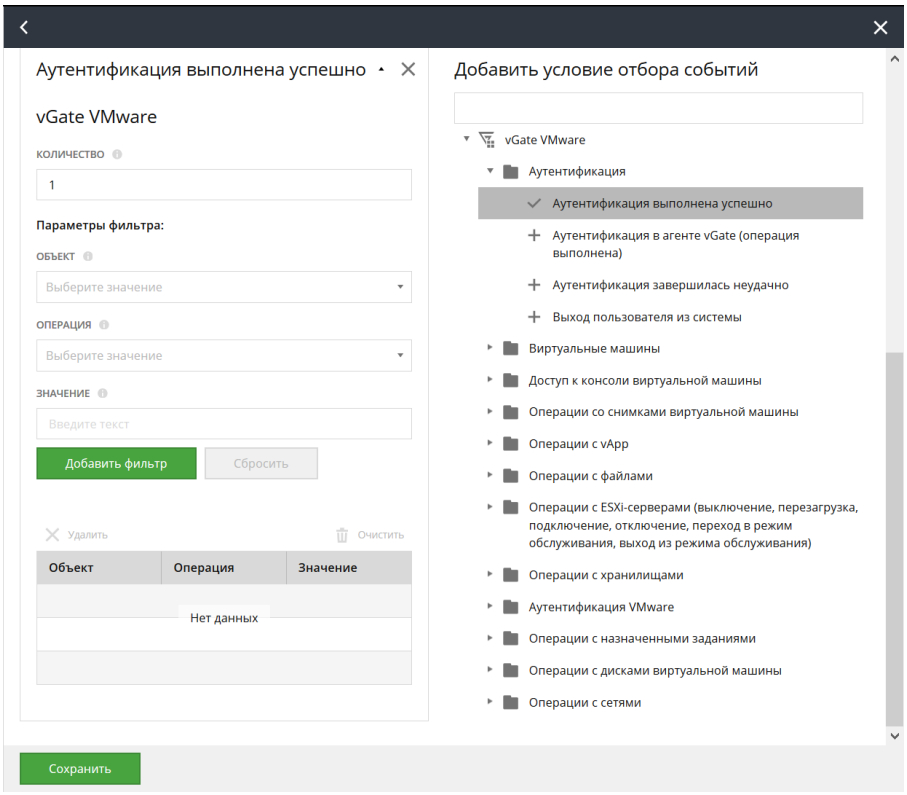


Для добавления правила:

1. Укажите параметры нового правила.

Параметр	Описание
Имя правила	Укажите название правила
Критичность	Укажите критичность правила
Интервал	Укажите интервал проверки событий в секундах, минутах или часах
Способ оповещения	Выберите способ оповещения о срабатывании правила
Группировать по	Выберите параметр, по которому необходимо группировать произошедшие события

2. Добавьте отслеживаемые правилом события. Для этого в правой части экрана выберите из списка событие и нажмите +. Станет доступным окно добавления фильтров.



Примечание. Чтобы удалить условие отбора событий, нажмите ✕.

3. Укажите количество событий, необходимых для срабатывания правила, укажите параметры фильтра и нажмите кнопку "Добавить фильтр".

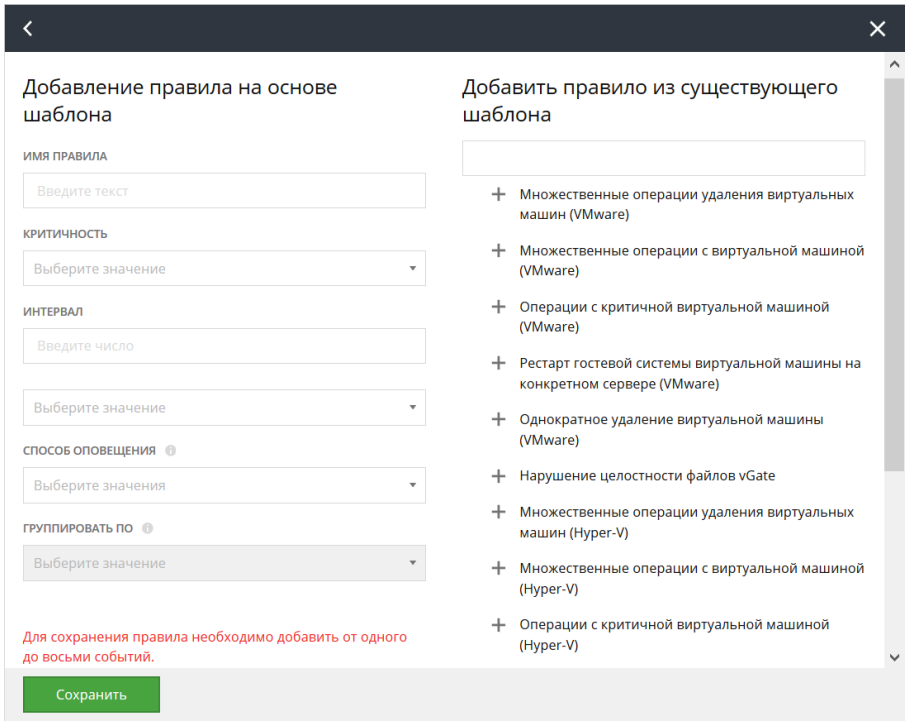
Параметр	Описание
Объект	Выберите один из параметров события
Операция	Выберите из выпадающего списка выражение, подходящее для создания условия: • Содержит; • Равен; • Не равен
Значение	Укажите значение, которое должен принимать выбранный параметр события для срабатывания правила

Совет. Чтобы добавить дополнительные условия отбора событий, повторите действия, описанные в пп. 2–5.

4. Добавленные фильтры появятся в таблице в левой части панели добавления правила. Чтобы удалить фильтр, выделите его и нажмите кнопку "Удалить". Чтобы удалить все фильтры из таблицы, нажмите кнопку "Очистить".

5. В нижней части панели добавления правила нажмите кнопку "Сохранить". Правило будет добавлено в список.

Создание правила по шаблону

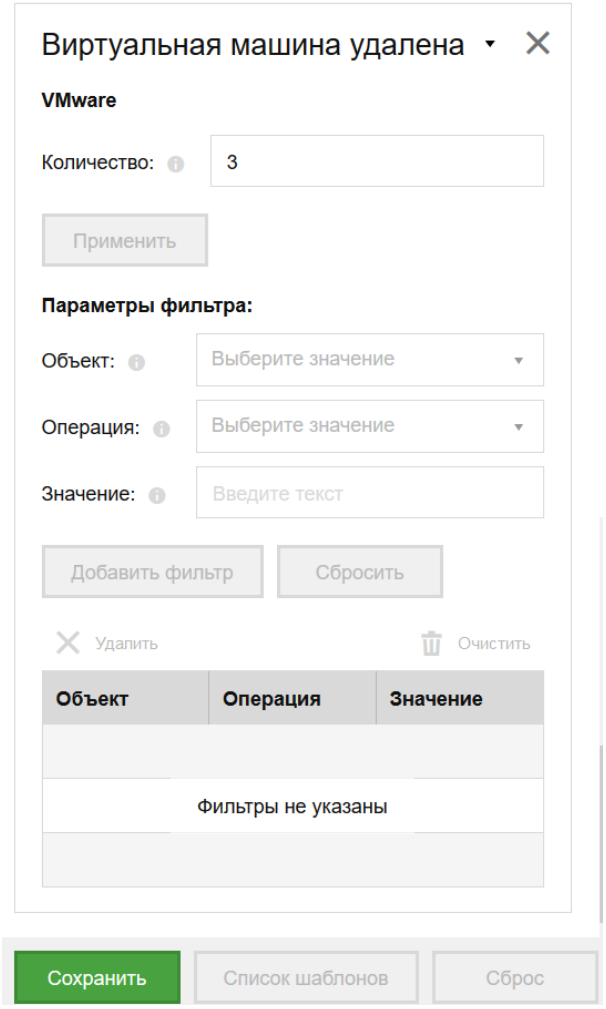


Для добавления правила по шаблону:

1. В правой части панели из списка шаблонов правила выберите шаблон и нажмите +. Параметры правила будут указаны автоматически.

Примечание. Используйте строку поиска для быстрого поиска шаблонов по названию.

В левой части панели добавления правила появится окно добавления фильтров.



Примечание. Чтобы удалить условие отбора событий, нажмите ✕ в правом верхнем углу формы.

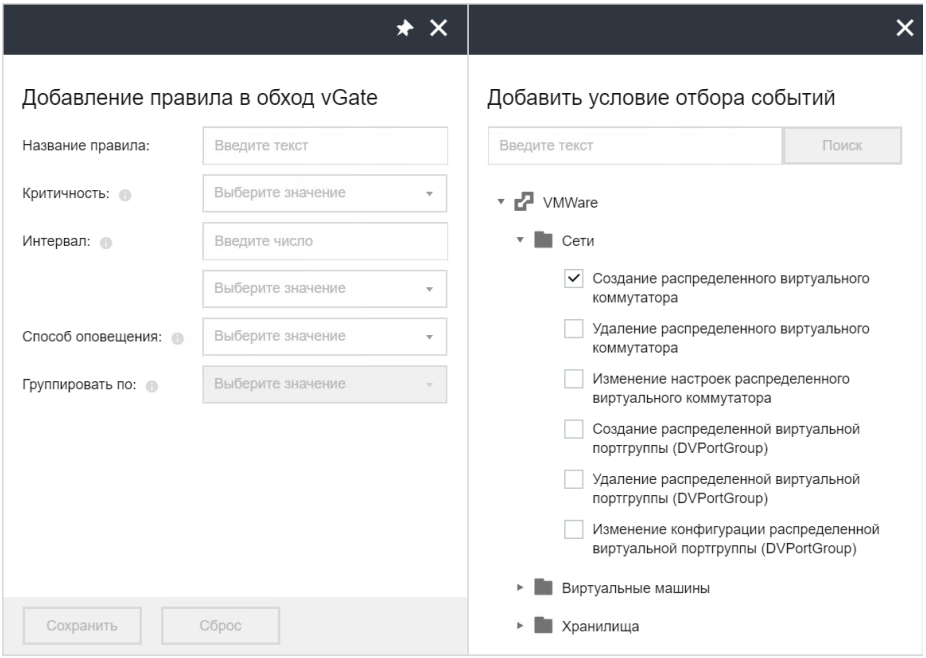
2. Укажите количество событий, необходимых для срабатывания правила, и добавьте фильтры (см. пп. 4, 5 на стр.**148**).

Примечание. Чтобы удалить фильтр или все фильтры, используйте кнопки "Удалить" и "Очистить" над таблицей.

3. В нижней части панели добавления правила нажмите кнопку "Сохранить". Правило будет добавлено в список.

Примечание. При создании правил по шаблону недоступно добавление условий отбора событий. Чтобы добавить дополнительные события для правила, созданного по шаблону, выделите нужное правило в списке правил и нажмите кнопку "Изменить".

Добавление правил, отслеживающих действия в обход vGate



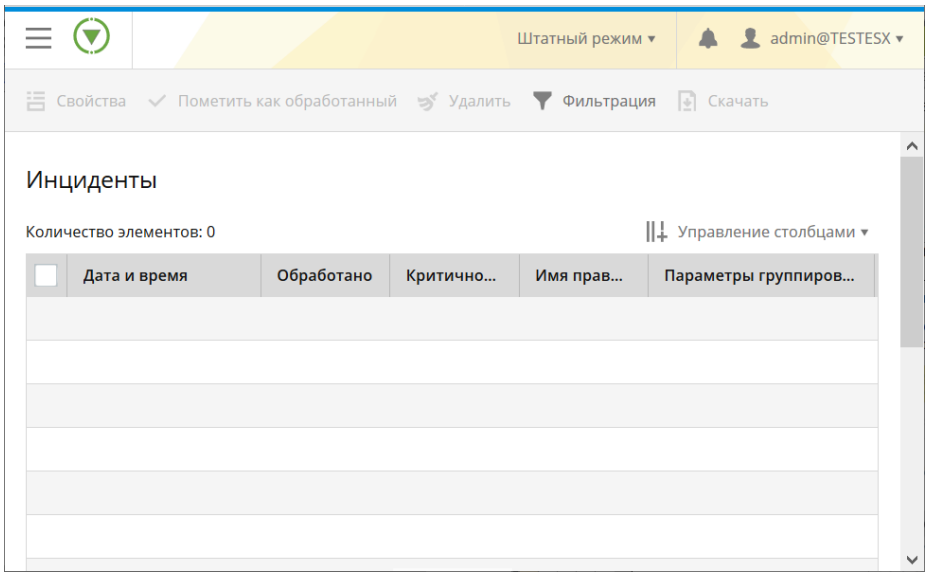
Для добавления правила укажите имя правила, критичность и интервал, а затем выберите из списка типы событий в виртуальной инфраструктуре, которые необходимо отслеживать. Правило сработает, если выбранные события будут зафиксированы на объектах виртуальной инфраструктуры и в vGate не будут получены соответствующие сообщения аудита в течение заданного интервала времени.

Нажмите кнопку "Сохранить", правило будет добавлено в список.

Инциденты

Инциденты — это события, которые создаются при срабатывании правил корреляции.

Для просмотра списка инцидентов в главном меню выберите раздел "Мониторинг", а затем "Инциденты".



Примечание. Информация об инцидентах также отображается в виде диаграмм на панели мониторинга (см. стр.144).

Для просмотра подробной информации о событии выберите его в списке и нажмите кнопку "Свойства".

Чтобы пометить инцидент просмотренным, нажмите кнопку "Пометить как обработанный".

Чтобы удалить выбранный инцидент, нажмите кнопку "Пометить как обработанный", а затем нажмите "Удалить". Для экспорта текстового файла со списком событий нажмите кнопку "Скачать".

Совет.

- Для фильтрации инцидентов нажмите кнопку "Фильтрация", в появившемся окне введите текст для поиска в нужное поле и нажмите кнопку "Применить".
- Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.

Журнал событий

Журнал событий vGate аналогичен журналу в консоли управления vGate (см. стр.**137**). В журнале отображается информация об изменении статусов компонентов защиты vGate. Подробную информацию о заблокированных сетевых пакетах можно просмотреть на серверах Hyper-V с помощью утилиты drvmgr.exe.

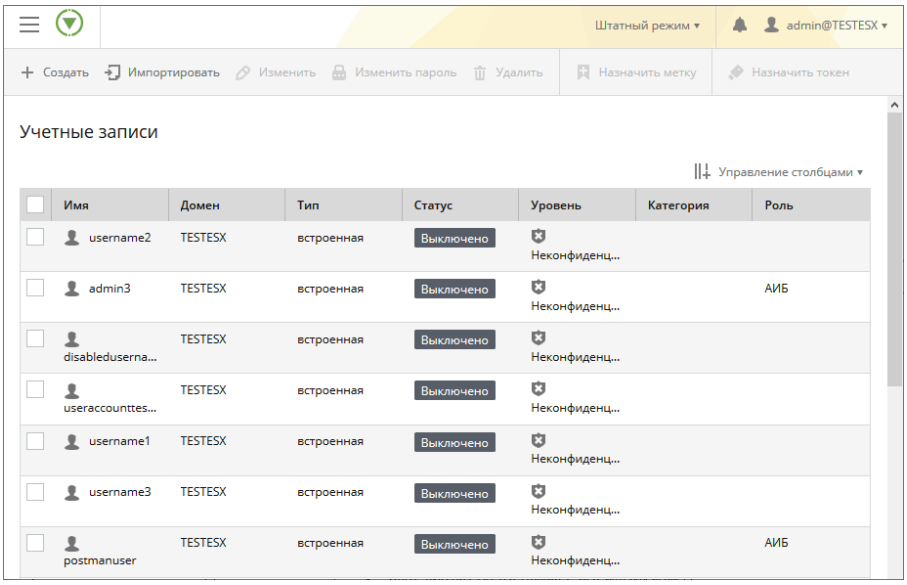
Учетные записи

В веб-консоли доступно управление учетными записями пользователей vGate (подробнее об учетных записях см. стр.**90**).

Для создания учетной записи:

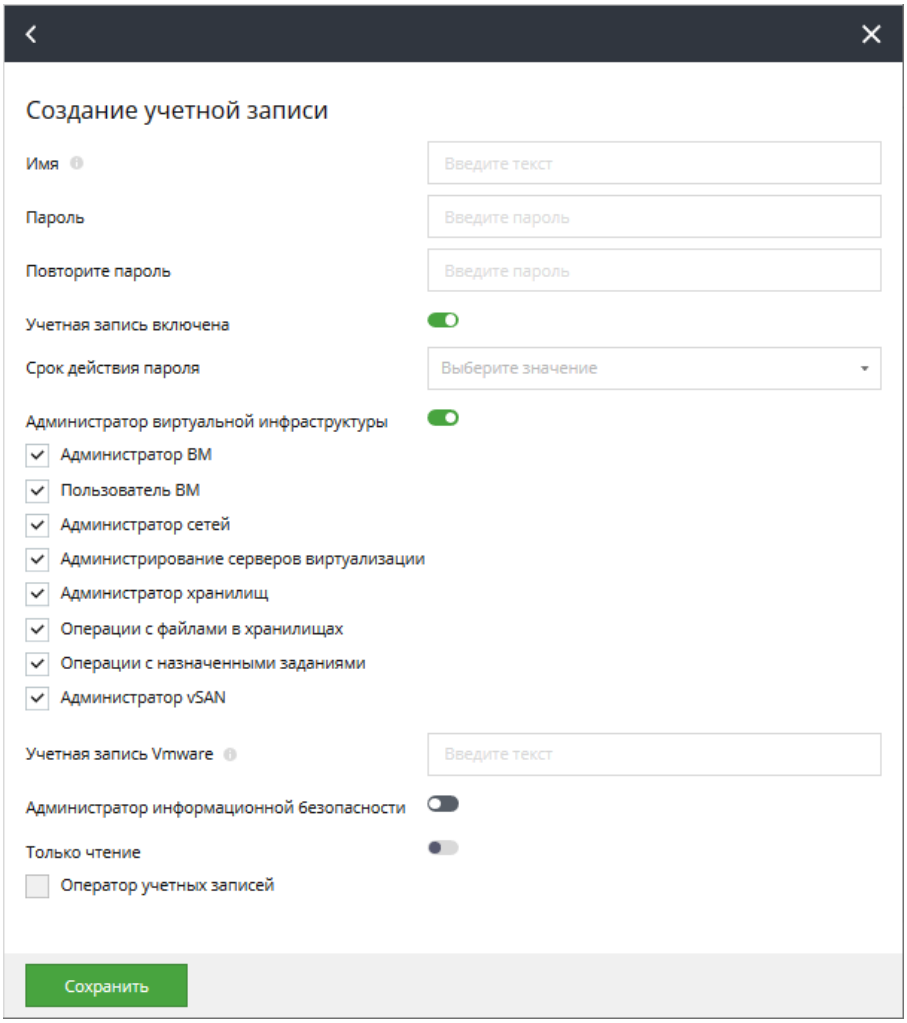
1. В главном меню выберите пункт "Учетные записи".

   На экране появится окно.



2. Нажмите кнопку "Создать".

   В правой части окна откроется панель создания учетной записи пользователя.



3. Укажите имя пользователя, дважды введите пароль. При необходимости настройте свойства пароля.

Параметр	Описание
Учетная запись включена	По умолчанию учетная запись включена. Установите переключатель в положение "Выкл" для временного отключения созданной записи. Если учетная запись отключена, то вход в систему с ее использованием невозможен. Однако уже авторизованный пользователь сможет продолжить свою работу и после отключения учетной записи, вплоть до следующей попытки авторизации
Срок действия пароля	Выберите из списка срок действия пароля
Администратор виртуальной инфраструктуры	Установите переключатель в положение "Вкл" для создания учетной записи администратора виртуальной инфраструктуры и выберите в списке полномочия, которые будут предоставлены АВИ
Учетная запись VMware	Только для среды VMware vSphere
Администратор информационной безопасности	Установите переключатель в положение "Вкл" для создания учетной записи администратора информационной безопасности и выберите в списке полномочия, которые будут предоставлены АИБ
Только чтение	Установите переключатель в положение "Вкл", чтобы разрешить создаваемой учетной записи АИБ доступ к vGate только для чтения

Параметр	Описание
Оператор учетных записей	Отметьте это поле для предоставления создаваемой учетной записи АИБ прав на управление списком пользователей

4. Нажмите кнопку "Сохранить".

   Учетная запись появится в списке.

Примечание.
- Чтобы отредактировать параметры учетной записи, выберите пользователя в списке и нажмите кнопку "Изменить".
- Используйте кнопки "Изменить пароль" и "Удалить", чтобы изменить пароль пользователя или удалить учетную запись. При удалении учетной записи будет предложено удалить правила доступа данного пользователя.

Для импорта учетной записи из Active Directory:

1. В главном меню выберите пункт "Пользователи" и нажмите кнопку "Импортировать". На экране появится панель добавления учетной записи.
2. Выберите в списке учетную запись для добавления из Active Directory и настройте ее параметры для работы в vGate (см. выше).
3. Нажмите кнопку "Сохранить". Учетная запись появится в списке.

Настройки

В веб-консоли возможно редактирование некоторых настроек vGate. В главном меню выберите раздел "Настройки", а затем перейдите на нужную вкладку:

- Общие (см. стр.**157**);
- Сервер виртуализации (см. стр.**158**);
- Защищаемые подсети (см. стр.**158**);
- Доверенные домены (см. стр.**158**);
- Журнал событий (см. стр.**158**);
- Мониторинг (см. стр.**159**);
- Отчеты (только для среды VMware vSphere);
- Уведомления (см. стр.**160**);
- Лицензия (см. стр.**160**);
- Политики паролей (см. стр.**160**);
- Мандатный контроль доступа (см. стр.**160**).

Общие настройки

Для изменения общих настроек:

1. Перейдите на вкладку "Общие" в разделе "Настройки".
2. Укажите значения параметров. Изменения будут сохранены автоматически.

Параметр	Описание
Настройки сессии	
Завершать сеанс через, минут	Время в минутах, по прошествии которого активная сессия пользователя будет завершена
Лицензия	
Предупреждать об истечении лицензии за, дней	Количество дней, за которое будет появляться предупреждение об истечении лицензии (см. стр.**75**)
Настройки сети и контроля доступа	
Добавлять на клиенте маршрут к защищенной сети	Отметьте, чтобы добавить маршрут к защищенной сети (см. стр.**76**)
Контроль доступа по уровням конфиденциальности	Отметьте, чтобы включить контроль доступа по уровням конфиденциальности (см. стр.**76**)
Контроль доступа по категориям конфиденциальности	Отметьте, чтобы включить контроль доступа по категориям конфиденциальности (см. стр.**76**)
Контроль уровня сессий	Отметьте, чтобы включить контроль уровня сессий (см. стр.**77**)
Настройки автодобавления виртуальных машин	
Включить автодобавление виртуальных машин	Установите выключение в положение "Выкл", чтобы отключить автодобавление для всех групп (см. стр.**99**). По умолчанию автодобавление включено
Добавлять новые машины каждые, мин	Укажите интервал. По умолчанию автодобавление виртуальных машин в группы объектов выполняется каждые 10 минут
Доверенные домены	
Разрешить авторизацию пользователей AD, которых нет в vGate	Отметьте, чтобы разрешить вход в vGate пользователям Active Directory, которые не имеют учетных записей в vGate (см. стр.**77**)
Архивация базы аудита	
Включить архивацию базы событий	Отметьте, чтобы включить архивацию базы аудита
Срок хранения событий	Срок хранения событий аудита, при превышении которого будет произведена архивация базы событий
Максимальный размер базы, Мб	Размер базы, при превышении которого будет произведена архивация
Путь выгрузки событий	Путь к каталогу для сохранения архива событий аудита

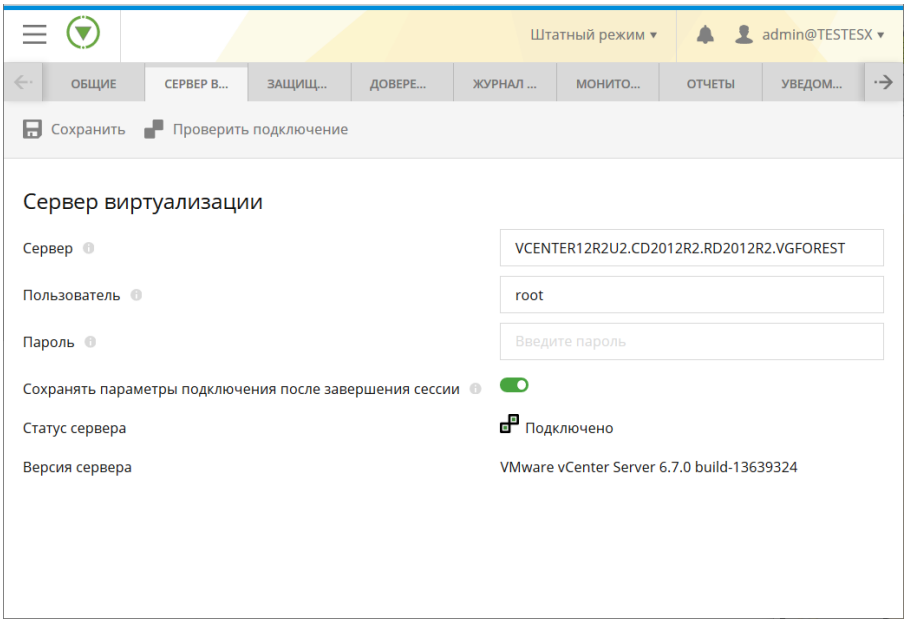
Нажмите кнопку "По умолчанию", чтобы указать значение для параметра, равное 15 минутам.

Сервер виртуализации

Для изменения параметров соединения:

1. В главном меню выберите раздел "Настройки" и перейдите на вкладку "Сервер виртуализации".

   На экране появится окно.



2. Укажите параметры для подключения к серверу виртуализации (подробнее см. стр.**70**) и нажмите кнопку "Сохранить".

   Нажмите кнопку "Проверить подключение", чтобы выполнить проверку введенных учетных данных.

Защищаемые подсети

Если маршрутизацию трафика в сети выполняет сервер авторизации vGate, то в случае появления в конфигурации сети новых подсетей необходимо добавить их в список защищаемых. Добавление подсетей в веб- консоли выполняется аналогично добавлению защищаемых подсетей в консоли управления vGate (см. стр.**71**).

Добавление доверенных доменов

Добавление доверенных доменов в веб-консоли выполняется аналогично добавлению доверенных доменов в консоли управления vGate (см. стр.**77**).

Настройка журнала событий

Для настройки параметров аудита:

1. В главном меню выберите раздел "Настройки" и перейдите на вкладку "Журнал событий".

   На экране появится список событий безопасности vGate.

2. Для управления настройками аудита используйте следующие кнопки.

Кнопка	Описание
В Журнал событий	Переход в раздел "Журнал событий" веб-консоли vGate (см. стр.**154**)
Включить/ Выключить	Включение/Выключение регистрации выбранного события
Включить e-mail/ Отключить e-mail	Включение/Выключение отправки оповещений по почте о данном событии аудита. Настройка отправки почтовых уведомлений выполняется в консоли управления vGate (см. стр.**72**)
Включить Syslog/ Отключить Syslog	Включение/Выключение отправки выбранного сообщения аудита на сервер Syslog. Настройка параметров Syslog выполняется в консоли управления vGate (см. стр.**74**)
Фильтрация	Фильтрация событий аудита. Выполняется аналогично фильтрации в консоли управления vGate (см. стр.**137**)

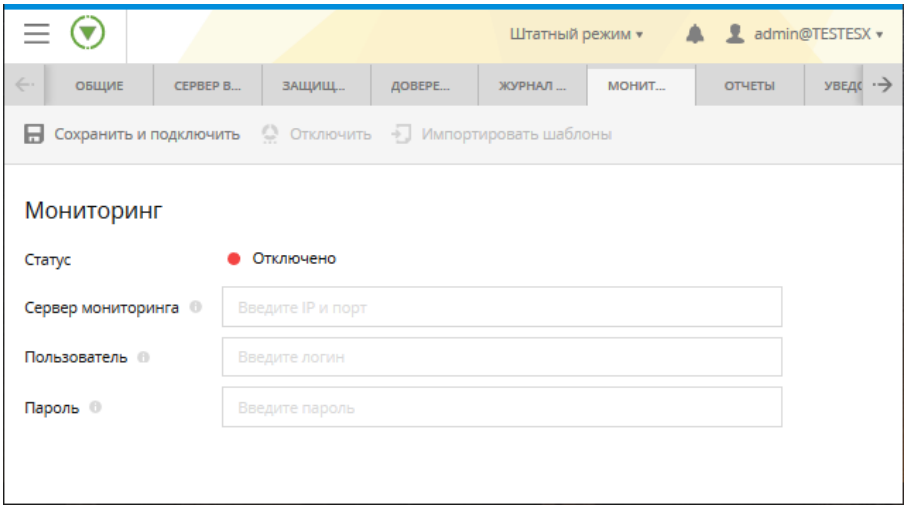
Примечание. Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.

Подключение к серверу мониторинга

Для настройки подключения:

1. В главном меню выберите раздел "Настройки" и перейдите на вкладку "Мониторинг".

   На экране появится окно.



2. Укажите параметры для подключения к серверу мониторинга и нажмите кнопку "Сохранить и подключить".

Параметр	Описание
Сервер мониторинга	Укажите сетевое имя или IP-адрес сервера мониторинга
Пользователь	Имя пользователя RabbitMQ, созданного при установке сервера мониторинга (см. стр.**49**)
Пароль	Пароль пользователя RabbitMQ

Будет выполнено подключение к серверу мониторинга.

- Чтобы отключить функцию мониторинга, нажмите кнопку "Отключить".
- Параметр "Статус" отображает текущее состояние подключения к серверу мониторинга.

vGate 4.4 поддерживает импорт шаблонов правил корреляции. Для этого нажмите кнопку "Импортировать шаблоны" и выберите нужный файл. Новые шаблоны появятся в списке (см. стр.150).

Параметры отправки уведомлений

В веб-консоли vGate можно настроить отправку почтовых уведомлений о событиях аудита по протоколу SMTP или Syslog аналогично настройке в Консоли управления vGate (см. стр.72 и стр.74).

Лицензия

Для загрузки лицензии:

1. В главном меню выберите раздел "Настройки" и перейдите на вкладку "Лицензия".

   На экране появится информация о текущей лицензии vGate.

2. Для загрузки новой лицензии нажмите кнопку "Загрузить лицензию", выберите файл в открывшемся окне и нажмите "Открыть".

Настройка политик паролей

Настройка политик паролей производится аналогично настройке в консоли управления vGate (см. стр.95).

Настройка мандатного контроля доступа

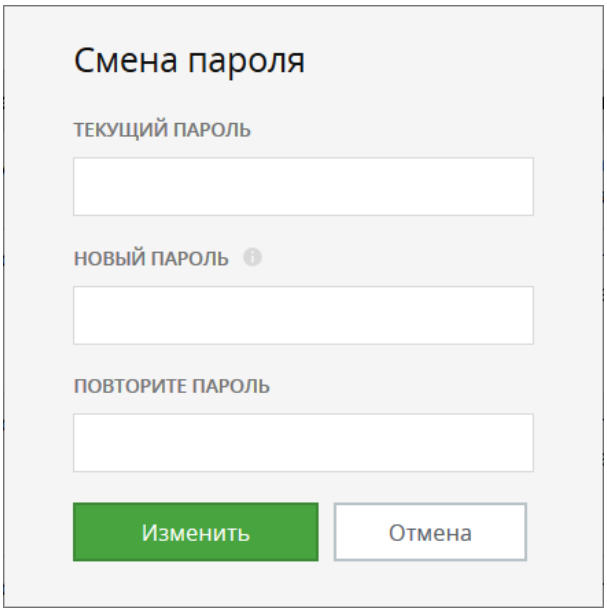
vGate предоставляет возможность определить перечень типов объектов, в отношении которых действует механизм полномочного управления доступом (см. стр.79).

Смена пароля администратора

Для смены пароля администратора:

1. В правом верхнем углу веб-консоли нажмите на имя учетной записи АИБ. В открывшемся меню выберите "Сменить пароль".

   На экране появится следующее окно.



2. Укажите текущий пароль, затем дважды введите новый пароль и нажмите кнопку "Изменить".

Примечание. Длина пароля должна быть не менее 5 символов. Пароль должен содержать от 4 классов символов (буква a-z, A-Z, цифры, специальные символы). Количество новых символов в пароле должно быть не менее 2.

Приложение

Привилегии пользователей

Разным типам пользователей vGate доступны различные операции в виртуальной инфраструктуре.

Роль	Доступные операции
Администрирование виртуальных машин	• Включение, выключение, перезагрузка ВМ. • Приостановка работы ВМ. • Доступ к консоли ВМ. • Изменение конфигурации ВМ. • Миграция ВМ. • Создание ВМ. • Удаление ВМ. • Экспорт ВМ (дополнительно необходимо наличие привилегии "Операции с файлами в хранилищах"). • Импорт ВМ. • Действия со снимками (snapshots) ВМ. • Экспорт снимка ВМ (дополнительно необходимо наличие привилегии "Операции с файлами в хранилищах"). • Настройка репликации ВМ. • Проверка отказа ВМ. • Перемещение хранилища ВМ. • Настройка приоритета узлов ВМ в кластере
Пользователь виртуальных машин	**Виртуальные машины** • Включение ВМ. • Выключение ВМ. • Доступ к консоли ВМ. • Перезапуск ВМ. • Проверка отказа ВМ. • Приостановка ВМ
Администрирование сетей	• Создание виртуального коммутатора. • Удаление виртуального коммутатора. • Создание логической сети. • Удаление логической сети. • Настройка логической сети. • Создание сети ВМ. • Удаление сети ВМ. • Настройка сети ВМ. • Создание пула статических IP-адресов. • Удаление пула статических IP-адресов. • Настройка пула статических IP-адресов. • Изменение настроек виртуальных коммутаторов
Администрирование серверов виртуализации	• Управление режимом обслуживания (Maintenance mode) сервера виртуализации.

Роль	Доступные операции
	• Изменение настроек сервера виртуализации. • Настройка репликации. • Включение сервиса управления виртуальными машинами. • Выключение сервиса управления ВМ. • Добавление узла в кластер. • Исключение узла из кластера. • Включение узла кластера. • Отключение узла кластера
Администрирование хранилищ	• Создание диска ВМ. • Подключение виртуального диска к серверу виртуализации. • Отключение виртуального диска от сервера виртуализации. • Изменение настроек диска ВМ. • Сжатие диска ВМ. • Расширение диска ВМ. • Объединение дисков ВМ. • Добавление кластерных дисков. • Удаление кластерных дисков. • Перемещение кластерных дисков. • Изменение режима обслуживания кластерных дисков. • Изменение настроек кластерных дисков. • Создание библиотеки. • Удаление библиотеки. • Добавление файлов в библиотеку. • Загрузка файлов из библиотеки. • Редактирование настроек библиотек. • Подключение хранилищ. • Отключение хранилищ
Операции с файлами в хранилищах	• Экспорт ВМ (дополнительно необходимо наличие привилегии "Администрирование виртуальных машин"). • Экспорт снимка ВМ (дополнительно необходимо наличие привилегии "Администрирование виртуальных машин")
Администрирование SCVMM и кластеров Hyper-V	• Создание кластера. • Удаление кластера. • Настройка кластера. • Создание объектов кластера. • Удаление объектов кластера. • Исполнение скриптов на серверах виртуализации. • Управление задачами SCVMM

Примечание. Для просмотра свойств кластерных дисков необходимо разрешить доступ к серверам виртуализации Hyper-V по порту 3912.

Защита соединений Hyper-V

Правила фильтрации сетевых соединений сервера Hyper-V можно создать с помощью компонента vGate для защиты соединений — утилиты командной строки drvmgr.exe.

Внимание! Если на сервере Hyper-V включен контроль учетных записей (UAC, User Account Control), то для настройки правил фильтрации соединений утилиту drvmgr.exe следует запускать от имени администратора.

Описание некоторых команд утилиты drvmgr.exe приведено ниже.

> drvmgr
Вызов справки
> drvmgr i 0x031
Просмотр текущих правил фильтрации
>drvmgr A protocol IP_from[:source_port[,mask]] [:destination_port] [Flags]
Добавление правила фильтрации
>drvmgr R protocol IP_from[:source_port[,mask]] [destination_port] [Flags]
Удаление правила фильтрации

Описание аргументов параметров команд утилиты приведено в таблице ниже.

Аргумент	**Описание**
protocol	Тип протокола
IP_from[:source_port [,mask]]	Параметры адресата в формате "IP-адрес: номер порта, маска". Номер порта и маску можно не указывать
[destination_port]	Порт сервера Hyper-V, к которому разрешается доступ. Параметр можно не указывать
[Flags]	Флаг с возможными значениями: • 1 — пакеты пропускаются без ограничений; • 4 — сохранение ПРД в реестре — при добавлении правила или удаление из реестра — при удалении; • 8 — если пакет пропущен с TCP-порта 902, то разрешен обмен файлами в browse datastore
В качестве значений аргументов можно использовать значение "any", соответствующее любому значению	

Примечание. По умолчанию утилита пропускает весь сетевой трафик из защищаемого периметра к серверу Hyper-V. Поэтому перед созданием новых правил фильтрации необходимо очистить таблицу правил.

Чтобы удалить все правила доступа, кроме правил, разрешающих трафик от сервера авторизации, используется команда:

```
>drvmgr cr
```

Для добавления правила, разрешающего доступ к серверу Hyper-V с сервера с IP-адресом 192.168.2.30 по протоколу RDP, формат команды следующий:

```
>drvmgr A TCP 192.168.2.30 3389 4
```

Для удаления вышеуказанного правила следует использовать команду:

```
>drvmgr R TCP 192.168.2.30 3389 4
```

Доступ к файлам виртуальных машин

Для выполнения операции экспорта виртуальных машин необходимо настроить доступ к файлам виртуальных машин в консоли управления vGate.

Для настройки доступа к файлам:

1. В свойствах учетной записи пользователя, от имени которого будут выполняться действия с файлами, отметьте пункты "Операции с файлами в хранилищах" и "Администратор виртуальных машин" (см. стр.**92**).
2. Для нужного сервера Hyper-V создайте правило "Управление виртуальной инфраструктурой Hyper-V", действующее для пользователя, в отношении которого выполнено действие **1**.

Если серверов Hyper-V несколько, то правило нужно создать для каждого из них.

TCP- и UDP-порты, используемые в среде Hyper-V

Список шаблонов правил доступа

Протокол	Исходящий порт	Порт назначения
Управление виртуальной инфраструктурой Hyper-V Windows Server 2019		
TCP	Любой	135
TCP	Любой	2179
TCP	Любой	3910
TCP	Любой	3920
TCP	Любой	5985
Управление виртуальной инфраструктурой Hyper-V Windows Server 2016		
TCP	Любой	135
TCP	Любой	2179
TCP	Любой	3910
TCP	Любой	5985
Управление виртуальной инфраструктурой Hyper-V Windows Server 2012, 2012 R2		
TCP	Любой	135
TCP	Любой	2179
TCP	Любой	3910
Управление конфигурацией кластера серверов Hyper-V через FCM		
TCP	Любой	135
TCP	Любой	445
TCP	Любой	3912
ICMP	Любой	Любой
Доступ к службе Microsoft RPC на сервере Hyper-V		
TCP	Любой	135
Доступ к контроллеру домена в защищаемом периметре		
TCP	Любой	53
TCP	Любой	88
TCP	Любой	135
TCP	Любой	139
TCP	Любой	445
TCP	Любой	464
TCP	Любой	3268
TCP	Любой	3269

Протокол	Исходящий порт	Порт назначения
UDP	Любой	53
UDP	Любой	88
UDP	Любой	135
UDP	Любой	138
UDP	Любой	389
UDP	Любой	445
UDP	Любой	464
Проверка доступности хоста (команда ping)		
ICMP	Любой	Любой
Разрешить поиск DNS-имен		
UDP	Любой	53
Администрирование сервера авторизации vGate		
TCP	Любой	3802
TCP	Любой	3803
TCP	Любой	3906
TCP	Любой	3908
TCP	Любой	443
Разрешить SNMP-мониторинг защищаемых серверов		
UDP	Любой	161
Разрешить прием SNMP-уведомлений		
UDP	Любой	162
Разрешить удаленный доступ к рабочему столу		
TCP	Любой	3389
Разрешить доступ к службе авторизации vGate		
TCP	Любой	3801
UDP	Любой	3801
TCP	Любой	3800
UDP	Любой	3800
TCP	Любой	3902
UDP	Любой	88
UDP	Любой	750
Разрешить общий доступ к файлам и принтерам на сервере Hyper-V		
TCP	Любой	139
TCP	Любой	445
UDP	Любой	137
UDP	Любой	138
Разрешить доступ консоли System Center Virtual Machine Manager (SCVMM) к серверу SCVMM		
TCP	Любой	8100

Контроль целостности. Список проверяемых модулей vGate

Список проверяемых модулей указан в конфигурационном файле esign.json, который находится в каталоге установки vGate.

Словарь часто используемых паролей

Словарь часто используемых паролей содержит список WellKnown паролей. При создании учетной записи пользователя или при смене пароля осуществляется проверка отсутствия нового пароля в словаре.

Словарь часто используемых паролей хранится в текстовом файле pwdict.txt в каталоге: \<каталог установки vGate>\Kerberos\ на сервере авторизации.

При необходимости список паролей в словаре можно отредактировать.

Для редактирования словаря:

1. Откройте файл pwdict.txt любым текстовым редактором (например, можно использовать "Блокнот").
2. Отредактируйте список паролей. При добавлении нового пароля в список каждый пароль следует вводить с новой строки.
3. Сохраните файл под тем же названием. Если в словарь были добавлены пароли в русскоязычной раскладке, сохраните файл в кодировке UTF-8.
4. Перезапустите сервис "vGate Kerberos KDC Service".

Примечание. При использовании механизма резервирования сервера авторизации словарь часто используемых паролей автоматически на резервный сервер не дублируется. Файл со словарем следует скопировать вручную заранее.

Перечень основных операций с конфиденциальными ресурсами и условия их выполнения

При предоставлении доступа АВИ к объектам виртуальной инфраструктуры для выполнения основных операций осуществляется проверка соблюдения определенных условий. Как правило, возможность выполнения операций регламентируется полномочным управлением доступом на основе меток безопасности, назначенных учетным записям пользователей и объектам виртуальной инфраструктуры (подробнее см. в разделе "Полномочное управление доступом к конфиденциальным ресурсам" документа [1]).

Некоторые операции управляются политиками безопасности (подробнее см. в разделе "Политики безопасности" документа [1]) или особыми привилегиями пользователей. К ряду операций с объектами виртуальной инфраструктуры условия не предъявляются, т. е. они доступны для выполнения всегда.

Ниже приведены операции, выполнение которых регламентируется полномочным управлением доступом, а также приведены условия их выполнения при использовании механизма контроля уровня сессий (см. стр.**77**). Если какое-либо из условий не соблюдено, то операция не выполняется.

Внимание! Если возможность контроля уровня сессий отключена, то для выполнения перечисленных ниже операций с защищаемыми объектами уровень сессии пользователя должен быть больше или равен уровню конфиденциальности объекта.

Условия выполнения операций	
Уровень конфиденциальности	**Категории конфиденциальности**
Start Virtual Machine (Запуск ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** Если отмечено поле "Разрешено исполнять ВМ с меньшим уровнем", то уровень конфиденциальности сервера Hyper-V должен быть не меньше уровня конфиденциальности ВМ. Иначе уровень конфиденциальности сервера Hyper-V должен быть равен уровню конфиденциальности ВМ	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Список категорий сервера Hyper-V должен включать хотя бы одну из категорий ВМ
TurnOff/Reset Virtual Machine (Выключение/перезапуск ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ
Pause/Save/Resume Virtual Machine (Приостановка ВМ в памяти/приостановка ВМ и сохранение на диск/возобновление ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ
Операции с контрольными точками (checkpoints)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** Для операции экспорта контрольных точек уровень сессии пользователя должен быть равен уровню конфиденциальности целевого хранилища. **3.** На ВМ не должна быть назначена политика "Запрет создания и удаления снимков виртуальных машин Hyper-V"	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Для операции экспорта контрольных точек список категорий пользователя должен включать хотя бы одну из категорий целевого хранилища. **3.** На ВМ не должна быть назначена политика "Запрет создания и удаления снимков виртуальных машин Hyper-V"
New Virtual Machine (Создание ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V. **2.** Уровень сессии пользователя должен быть равен уровню конфиденциальности хранилища. ВМ автоматически назначается уровень конфиденциальности хранилища	**1.** Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V. **2.** Список категорий пользователя должен включать хотя бы одну из категорий хранилища. ВМ автоматически назначается категория хранилища. Если таковых несколько, то ВМ назначается список категорий
Delete Virtual Machine (Удаление ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ

Условия выполнения операций	
Уровень конфиденциальности	**Категории конфиденциальности**
Import Virtual Machine (Импорт ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V. **2.** Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **3.** Уровень сессии пользователя должен быть равен уровню конфиденциальности хранилища. При отсутствии на ВМ меток безопасности ей автоматически назначается уровень конфиденциальности хранилища	**1.** Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V. **2.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **3.** Список категорий пользователя должен включать хотя бы одну из категорий хранилища. При отсутствии на ВМ меток безопасности ей автоматически назначается категория хранилища. Если таковых несколько, то ВМ назначается список категорий
Export Virtual Machine (Экспорт ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** Уровень сессии пользователя должен быть равен уровню конфиденциальности целевого хранилища. **3.** На ВМ не должна быть назначена политика "Запрет экспорта виртуальных машин Hyper-V". **4.** Пользователь должен обладать привилегией "Операции с файлами в хранилищах"	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Список категорий пользователя должен включать хотя бы одну из категорий целевого хранилища. **3.** На ВМ не должна быть назначена политика "Запрет экспорта виртуальных машин Hyper-V". **4.** Пользователь должен обладать привилегией "Операции с файлами в хранилищах"
Enable Replication (Включение репликации ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** Уровень конфиденциальности сервера Hyper-V, на который реплицируется ВМ, должен быть равен уровню конфиденциальности ВМ (если отмечено поле "Разрешено исполнять ВМ с меньшим уровнем", то равен или выше уровня конфиденциальности ВМ). **3.** На ВМ не должна быть назначена политика "Запрет включения репликации виртуальных машин Hyper-V"	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Список категорий сервера Hyper-V, на который реплицируется ВМ, должен включать хотя бы одну из категорий ВМ. **3.** На ВМ не должна быть назначена политика "Запрет включения репликации виртуальных машин Hyper-V"
Start/Pause/Resume/Cancel/Remove Replication (Запуск, приостановка, возобновление, отмена, удаление репликации ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ

Условия выполнения операций	
Уровень конфиденциальности	**Категории конфиденциальности**
Move Virtual Machine (Миграция ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** В случае миграции на другой сервер Hyper-V уровень конфиденциальности сервера Hyper-V, на который мигрирует ВМ, должен быть равен уровню конфиденциальности ВМ (если отмечено поле "Разрешено исполнять ВМ с меньшим уровнем", то равен или выше уровня конфиденциальности ВМ). **3.** Уровень конфиденциальности хранилища, на которое мигрирует ВМ (или файлы ВМ), должен быть равен уровню конфиденциальности ВМ (если отмечено поле "Разрешено хранить ВМ с меньшим уровнем", то равен или выше уровня конфиденциальности ВМ). **4.** На ВМ не должна быть назначена политика "Запрет миграции виртуальных машин Hyper-V"	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** В случае миграции на другой сервер Hyper-V список категорий сервера Hyper-V, на который мигрирует ВМ, должен включать хотя бы одну из категорий ВМ. **3.** Список категорий хранилища, на которое мигрирует ВМ (или файлы ВМ), должен включать хотя бы одну из категорий ВМ. **4.** На ВМ не должна быть назначена политика "Запрет миграции виртуальных машин Hyper-V"
Add/Set VMHardDiskDrive (Добавление/настройка диска ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности хранилища. **2.** Уровень конфиденциальности хранилища должен быть равен уровню конфиденциальности ВМ (если отмечено поле "Разрешено хранить ВМ с меньшим уровнем", то равен или выше уровня конфиденциальности ВМ)	**1.** Список категорий пользователя должен включать хотя бы одну из категорий хранилища. **2.** Список категорий хранилища должен включать хотя бы одну из категорий ВМ
Remove VMHardDiskDrive (Удаление диска ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ
Операции с жесткими дисками (VHD) (Create/Convert/Compact/Expand/Get/Test/Merge/Set VHD)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности хранилища	Список категорий пользователя должен включать хотя бы одну из категорий хранилища
Mount VHD/Dismount VHD (Подключение жесткого диска к серверу, отключение жесткого диска от сервера Hyper-V)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V. **2.** Уровень сессии пользователя должен быть равен уровню конфиденциальности хранилища	**1.** Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V. **2.** Список категорий пользователя должен включать хотя бы одну из категорий хранилища
Изменение параметров сервера Hyper-V	
Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V	Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V

Условия выполнения операций	
Уровень конфиденциальности	**Категории конфиденциальности**
Start/Stop Service (Старт/остановка службы VMMS)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V	Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V
Create Virtual Switch (Создание виртуального коммутатора)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V	Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V
Modify Virtual Switch (Изменение виртуального коммутатора)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности сервера Hyper-V. **2.** Уровень сессии пользователя должен быть равен уровню конфиденциальности физического сетевого адаптера. **3.** Уровень конфиденциальности физического сетевого адаптера должен быть равен уровню конфиденциальности виртуального коммутатора (если отмечено поле "Разрешено подключать коммутаторы с меньшим уровнем", то равен или выше уровня конфиденциальности коммутатора). Новому коммутатору автоматически назначается уровень конфиденциальности физического сетевого адаптера	**1.** Список категорий пользователя должен включать хотя бы одну из категорий сервера Hyper-V. **2.** Список категорий пользователя должен включать хотя бы одну из категорий физического сетевого адаптера. **3.** Список категорий физического сетевого адаптера должен включать хотя бы одну из категорий виртуального коммутатора. Новому коммутатору автоматически назначается уровень конфиденциальности физического сетевого адаптера
Remove Virtual Switch/Virtual Switch Settings (Удаление виртуального коммутатора, изменение настроек коммутатора)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности виртуального коммутатора	Список категорий пользователя должен включать хотя бы одну из категорий виртуального коммутатора

Connect VM to Switch (Connect-VMNetworkAdapter) (Присоединение ВМ к коммутатору, изменение настроек коммутатора)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** Уровень конфиденциальности виртуального коммутатора должен быть равен уровню конфиденциальности ВМ (если отмечено поле "Разрешено подключение ВМ с меньшим уровнем", то равен или выше уровня конфиденциальности ВМ). **3.** Уровень конфиденциальности ВМ должен быть равен уровню конфиденциальности виртуальной сети (если отмечено поле "Разрешено подключаться к сетям с меньшим уровнем", то равен или выше уровня конфиденциальности виртуальной сети). **4.** Уровень конфиденциальности виртуального коммутатора должен быть равен уровню конфиденциальности виртуальной сети	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Список категорий виртуального коммутатора должен включать хотя бы одну из категорий ВМ. **3.** Список категорий виртуальной сети должен включать хотя бы одну из категорий ВМ. **4.** Список категорий виртуального коммутатора должен включать хотя бы одну из категорий виртуальной сети
Remove VM from Switch (Отключение ВМ от коммутатора)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ

Утилита clacl.exe

В состав vGate входит утилита clacl.exe, которая позволяет выполнить его настройку. Большая часть команд утилиты дублирует возможности консоли управления.

Утилита доступна из командной строки на сервере авторизации. В случае если рабочее место АИБ располагается на отдельном компьютере, необходимо скопировать утилиту на этот компьютер с сервера авторизации. Для вызова подробной информации об утилите откройте редактор командной строки и введите следующую команду:

```
clacl.exe –H
```

Создание правил разграничения доступа

Утилита clacl.exe может быть использована для настройки правил разграничения доступа к защищаемым серверам.

Для создания правила:

- Откройте редактор командной строки и выполните следующую команду:

  clacl.exe rules add -q **<имя>** -e **<описание>** -n **<сервер>** -m **<компьютер>** -u **<пользователь>** -p **<номер протокола>** -t **<порт>** -o **<порт>** -k **<администратор>** -s **<пароль>**

  где

  - -q **<имя>** — имя правила;
  - -e **<описание>** — описание правила;
  - -n **<сервер>** — полное доменное имя или IP-адрес сервера, для которого будет действовать правило;
  - -m **<компьютер>** — компьютер, с которого разрешен доступ пользователю;

- -u **<пользователь>** — учетная запись пользователя или компьютера (символ "*" означает, что правило действует для всех аутентифицированных пользователей, "#" — для анонимных пользователей);
- -p **<номер протокола>** — номер, обозначающий тип протокола соединения (см. подробное описание параметра с помощью команды **clacl.exe rules add –H**);
- -t **<порт>** — исходящий порт (символ "0" означает, что правило действует для всех портов;
- -o **<порт>** — порт назначения (символ "0" означает, что правило действует для всех портов;
- **<администратор>** — имя АИБ;
- **<пароль>** — пароль АИБ.

Примечание. Подробное описание параметров, которые необходимо указать при создании нового правила, приведено на стр.**119**.

Пример:

```
clacl rules add -q "For RPC" -e "For RPC" -n 192.168.2.20 -m
* -u * -p 6 -t 0 -o 135 -k admin -s pAssword
```

Данная команда добавляет правило доступа к TCP-порту 135 сервера Hyper-V для всех аутентифицированных пользователей.

Для вызова подробной информации о параметрах команды добавления нового правила введите в командной строке следующую команду:

```
clacl.exe rules add –H
```

Утилита db-util.exe

В состав vGate входит утилита db-util.exe для управления базой данных конфигурации и настройками резервирования сервера авторизации.

Утилита располагается в каталоге, в который был установлен компонент "Сервер авторизации".

Для вызова подробной информации об утилите откройте редактор командной строки и введите следующую команду:

```
db-util.exe –h
```

Проверка подключения к серверу PostgreSQL

Используя утилиту db-util.exe, можно выполнить проверку учетных данных, с помощью которых происходит подключение к серверу PostgreSQL.

- Откройте редактор командной строки и выполните следующую команду:

  db-util.exe --test-connect **<сервер>** -D **<база данных>**-U **<пользователь** -P **<пароль>**

  где:

  - **<сервер>** — имя или IP-адрес сервера, на котором располагается база данных;
  - **<база данных>** — имя базы данных;
  - **<пользователь>** — имя пользователя для доступа к базе данных;
  - **<пароль>** — пароль пользователя для доступа к базе данных.

  На экране появится сообщение о результатах тестового подключения к базе данных.

Перемещение удаленных событий аудита

При очистке журнала событий в консоли управления vGate события аудита помечаются удаленными, но физически не удаляются из базы данных. С помощью утилиты db-util.exe можно выгрузить удаленные сообщения аудита в выбранный каталог, тем самым удалив их из базы.

Для перемещения удаленных событий из базы:

- Откройте редактор командной строки и выполните следующую команду:

  db-util.exe --hard-compact **<путь>**

  или

  db-util.exe --soft-compact **<путь>**

  где:

  - команда hard-compact — выполняет сжатие базы данных. Может нарушить работу резервирования, если оно включено;
  - команда soft-compact — выполняет сжатие базы данных. Не очищает память на диске после удаления записей из базы данных. Данная команда не влияет на резервирование данных;
  - **<путь>** — путь к созданной папке для хранения удаленных событий.

  В указанной папке будет создан архив в формате gzip с названием

  vgate-audit-[DATETIME].gz, где DATETIME — дата и время выполнения команды.

Примечание. Если команда db-util.exe --hard-compact была выполнена при наличии установленного резервного сервера, то для восстановления репликации выполните команду db-util.exe –recreate-replica на резервном сервере авторизации.

Для загрузки удаленных событий обратно в базу:

- Откройте редактор командной строки и выполните следующую команду:

  db-util.exe --load **<путь>**

Настройка резервирования

С помощью утилиты db-util можно удалить настройки репликации данных между основным и резервным серверами авторизации vGate.

Для удаления настроек резервирования:

- Откройте редактор командной строки на основном сервере авторизации и выполните следующую команду:

  db-util.exe --delete-cluster

Для восстановления репликации:

- Откройте редактор командной строки на резервном сервере авторизации и выполните следующую команду:

  db-util.exe --recreate-replica **<IP>**: **<порт>**

  где:

  - **<IP>** — IP-адрес основного сервера авторизации;
  - **<порт>** — порт PostgreSQL основного сервера авторизации, по умолчанию 5432.

Для просмотра отставания резервного сервера авторизации от основного:

- Откройте редактор командной строки на резервном сервере авторизации и выполните следующую команду:

  db-util.exe --replication-delay

  В результате выполнения команды на экране появится информация об отставании резервного сервера от основного в байтах WAL-логов PostgreSQL либо - 1, если произошла ошибка (резервирование не включено, WAL переполнен, нет связи между основным и резервным серверами авторизации).

Изменение роли сервера авторизации

С помощью утилиты db-util.exe можно изменить роли серверов авторизации — назначить основной сервер авторизации резервным, а резервный сервер — основным (например, при сбое основного сервера).

Для изменения ролей серверов:

- Откройте редактор командной строки на основном сервере авторизации и выполните следующую команду:

  db-util.exe --switch-roles-fm --log **<путь>**

  где **<путь>** — путь к лог-файлу операции смены ролей.

  Примечание. Параметр --log **<путь>** не является обязательным. По умолчанию лог-файл операции будет сохранен в каталоге установки продукта в папке vGate\Logs.

Передача управления резервному серверу авторизации

В случае выхода из строя основного сервера авторизации можно временно назначить резервный сервер основным.

Внимание! Не рекомендуется применять команду передачи управления резервному серверу авторизации при включенном автоматическом переключении.

Для передачи управления резервному серверу:

- Откройте редактор командной строки на резервном сервере авторизации и выполните следующую команду:

  db-util.exe --failover --log **<путь>**

  Примечание. Параметр --log **<путь>** не является обязательным. По умолчанию лог-файл операции будет сохранен в каталоге установки продукта в папке vGate\Logs.

Утилита cfgTransfer.exe

В состав vGate входит утилита CfgTransfer.exe, предназначенная для экспорта конфигурации vGate версии 4.0 и выше.

Утилита располагается на установочном диске vGate в каталоге \vGate.

Для вызова подробной информации об утилите откройте редактор командной строки и введите следующую команду:

```
cfgtransfer.exe -h
```

Предполагается использование утилиты CfgTransfer.exe при установленном на компьютере сервере авторизации vGate.

Если ПО vGate было удалено до начала экспорта конфигурации, необходимо в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate установить следующие значения:

- HaronIntIface (строка) — IP-адрес сервера авторизации vGate в сети администрирования инфраструктуры;
- BdPort (строка) — порт базы данных. Указывается в случае, если был использован порт, отличный от порта по умолчанию (5432);
- RhuidPort (DWORD) — любое значение;
- NetworkMode (строка) — режим работы vGate ("router" — если vGate установлен для работы без отдельного маршрутизатора, "simple" — если в сети есть отдельный маршрутизатор);
- AddVmToGroupDefaultTimeout (DWORD) — тайм- аут операции автодобавления виртуальных машин в группы.

Для экспорта конфигурации:

Откройте редактор командной строки и выполните следующую команду:

```
cfgtransfer.exe -t <тип операции> -f <путь к файлу>
```

где

-t **<тип операции>** — тип операции (export/import);

-f **<путь к файлу>** — полный путь к файлу в формате XML, в который будет записана конфигурация vGate.

Команда может содержать ключ pg_only (-o). В этом случае экспорт данных будет произведен только из базы данных, без попыток опроса защищаемых серверов.

При экспорте конфигурации vGate версии 4.0 необходимо, чтобы команда содержала следующие ключи:

- pg_user (-d) — имя пользователя PostgreSQL;
- pg_pwd (-p) — пароль пользователя PostgreSQL.

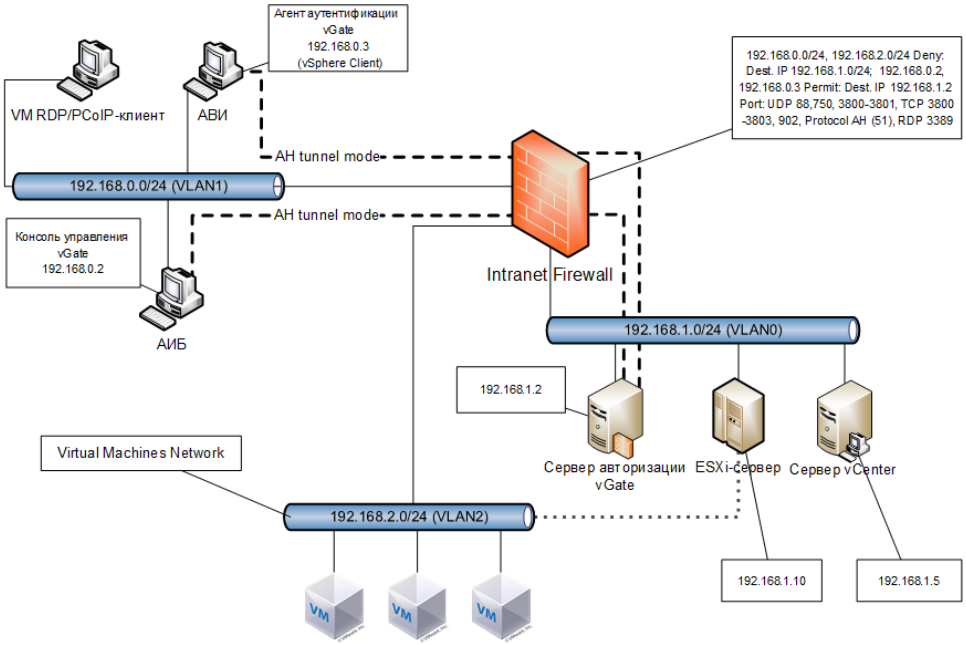
Настройки маршрутизатора

Если маршрутизацию трафика между сетью защищаемых серверов и внешним периметром сети администрирования выполняет отдельный маршрутизатор, в его настройках необходимо создать правила, разрешающие соединения между сервером авторизации vGate и рабочими местами АИБ и АВИ по следующим портам:

- порт TCP 3801;
- порт UDP 3801;
- порт TCP 3800;
- порт UDP 3800;
- порт TCP 3802;
- порт TCP 3803;
- порт TCP 3808 (при резервировании сервера авторизации vGate);
- порт TCP 3911;
- порт TCP 3912;
- порт UDP 88;
- порт UDP 750;
- порт TCP 3389 (при подключении к серверу авторизации vGate по RDP);
- протокол AH (№ 51).

Схема сети

Схема размещения элементов виртуальной инфраструктуры и компонентов ПО vGate, установленных с использованием стороннего маршрутизатора.



Где:

- 192.168.0.0/24 — сеть администрирования инфраструктуры;
- 192.168.1.0/24, 192168.2.0/24 — защищаемые сети.

При установке ПО vGate с использованием маршрутизатора (Intranet Firewall), расположенного внутри сети, необходимо создать правила доступа из сети администрирования инфраструктуры в защищаемую сеть, при этом трафик между этим сетями должен быть запрещен. Доступ в защищаемую сеть могут иметь учетные записи компьютеров АИБ и АВИ, для них должны быть открыты порты на сервере авторизации vGate, перечисленные выше.

Пример настройки маршрутизатора Cisco PIX

Для создания правил, разрешающих соединения между сервером авторизации vGate и рабочими местами АИБ и АВИ, выполните в командной строке маршрутизатора следующие команды:

```
access-list 102 permit tcp 192.168.1.0 255.255.255.0 host
192.168.2.10 range 3800 3801 3802 3803
access-list 102 permit udp 192.168.1.0 255.255.255.0 host
192.168.2.10 range 3800 3801
access-list 102 permit ah 192.168.1.0 255.255.255.0 host
192.168.2.10
access-list 103 permit ah host 192.168.2.10 192.168.1.0
255.255.255.0
access-group 102 in interface outside
access-group 103 in interface inside
```

где:

- 192.168.1.0/24 — сеть администрирования, в которой размещены рабочие места АИБ и АВИ;
- 192.168.2.0/24 — сеть защищаемых серверов виртуальной инфраструктуры;
- 192.168.2.10 — IP-адрес сетевого адаптера сервера авторизации vGate в защищенной сети.

Совместная работа vGate и Secret Net Studio

Поддерживается совместная работа ПО vGate и Secret Net Studio 8.5.

Порядок установки (удаления) компонентов vGate и Secret Net Studio при совместном использовании не имеет значения.

Внимание! Не поддерживается установка сервера авторизации vGate и сервера безопасности Secret Net Studio на один компьютер.

Внимание! Если на сервере авторизации vGate установлено ПО Secret Net Studio с включенным механизмом затирания данных, не рекомендуется использовать утилиту db-util.

Если в Secret Net Studio используется механизм замкнутой программной среды (ЗПС) в жестком режиме, то при установке компонентов vGate нужно либо отключить механизм ЗПС, либо вывести его из жесткого режима.

Также можно выполнить установку vGate с помощью учетной записи, на которую механизм ЗПС не действует.

После установки vGate необходимо настроить механизм ЗПС так, чтобы он не блокировал запуск модулей и загрузку библиотек, необходимых для работы vGate. Методика настройки механизма ЗПС приведена в документации к ПО Secret Net Studio (см. "Руководство администратора. Настройка и эксплуатация").

Если в Secret Net Studio включен и настроен на vGate механизм контроля целостности или механизм ЗПС, то при переустановке vGate необходимо пересчитать эталонные значения контролируемых параметров в заданиях Secret Net Studio.

Совместная работа vGate и Антивируса Касперского

Настройка Kaspersky Endpoint Security 11

Для доступа к Hyper-V при совместной работе vGate и средства антивирусной защиты Kaspersky Endpoint Security 11 может потребоваться отключение контроля портов 80 и 443 в настройках Kaspersky Endpoint Security.

Внимание! Для корректной установки ПО vGate на компьютеры с ОС Windows необходимо на время установки отключить самозащиту в Kaspersky Endpoint Security.

Обеспечение совместимости агента аутентификации с ПО Континент

Поддерживается совместная работа ПО vGate 4.4 и ПО Континент на одном компьютере.

Для обеспечения корректной работы агента аутентификации vGate требуется разрешить обмен данными клиента ПО Континент с сервером авторизации vGate по протоколу AH (IP-протокол 51).

Для организации обмена данными в ПО Континент 3.9.1:

1. В Программе управления сервером доступа Континент создайте правила фильтрации, обеспечивающие прохождение пакетов протокола AH от клиента Континента (абонентского пункта) к серверу авторизации vGate.

   В правилах фильтрации укажите следующие значения:

Поле	Значение
Отправитель	IP-адрес клиента Континента
Получатель	IP-адрес сервера авторизации vGate
Сервисы	Протокол AH (IP-протокол 51)
Действие	Пропустить пакет

2. Добавьте созданные правила фильтрации в список правил учетной записи пользователя Континент.

Для организации обмена данными в ПО Континент 4.0.3 и 4.1:

1. На панели навигации Менеджера конфигурации выберите подраздел "Контроль доступа | Межсетевой экран" и создайте правило фильтрации, указав необходимые параметры (см. выше).
2. Вызовите контекстное меню параметра "Сервис" и выберите пункт "Добавить...".
3. Нажмите кнопку "Создать" в появившемся окне.

   Откроется окно "Сервис".
4. В поле "Протокол" укажите значение "51". Заполните поле "Название" и нажмите кнопку "ОК".
5. Вызовите контекстное меню параметра "Действие" и выберите пункт "Пропустить".
6. Сохраните изменения в конфигурации Центра управления сетью. Для применения изменений в конфигурации узла безопасности установите политику на требуемые компоненты комплекса.

Если после установки политики, содержащей правило фильтрации комплекса, пакеты протокола AH не проходят, нужно разорвать существующие соединения на необходимых узлах безопасности.

Примечание.

- Чтобы разорвать существующие соединения в ПО Континент 4.0.3, необходимо в настройках узла безопасности выбрать пункт "Разорвать без учета исключений". Если в дальнейшем данная настройка не требуется, необходимо установить ее начальное значение.
- Для разрыва существующих соединений в ПО Континент 4.1 на панели навигации Менеджера конфигурации выберите подраздел "Структура". В списке узлов безопасности выберите нужный компонент и нажмите кнопку "Сбросить сессии" на панели инструментов.

Обеспечение совместимости агента аутентификации с ViPNet

Поддерживается совместная работа ПО vGate и ViPNet 4.3.

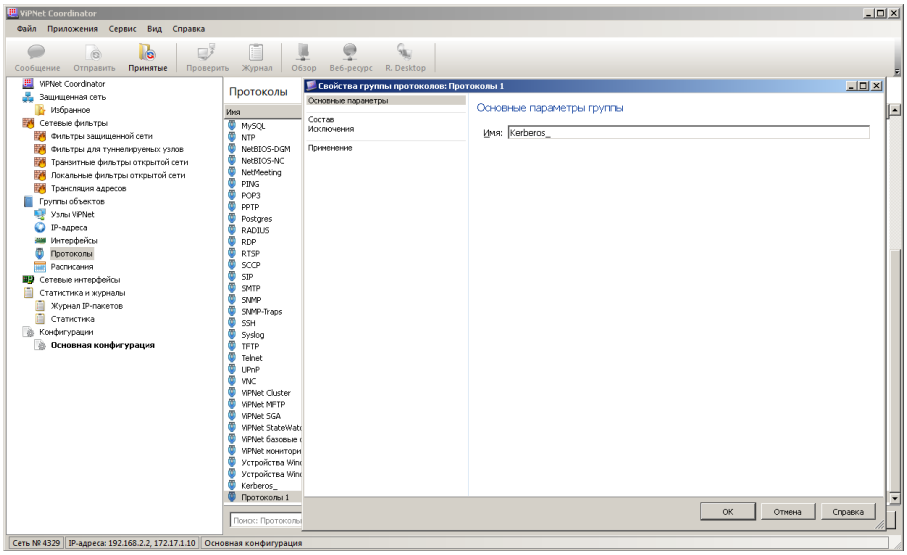
В примерах ниже рассматривается настройка ПО ViPNet следующих версий:

- Client 4.3 (4.53803);
- Coordinator 4.3 (2.37189).

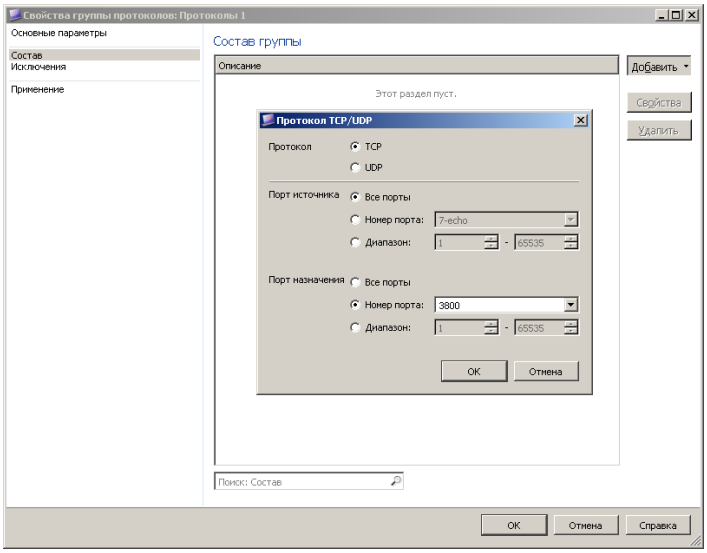
Вариант 1

Для настройки ViPNet:

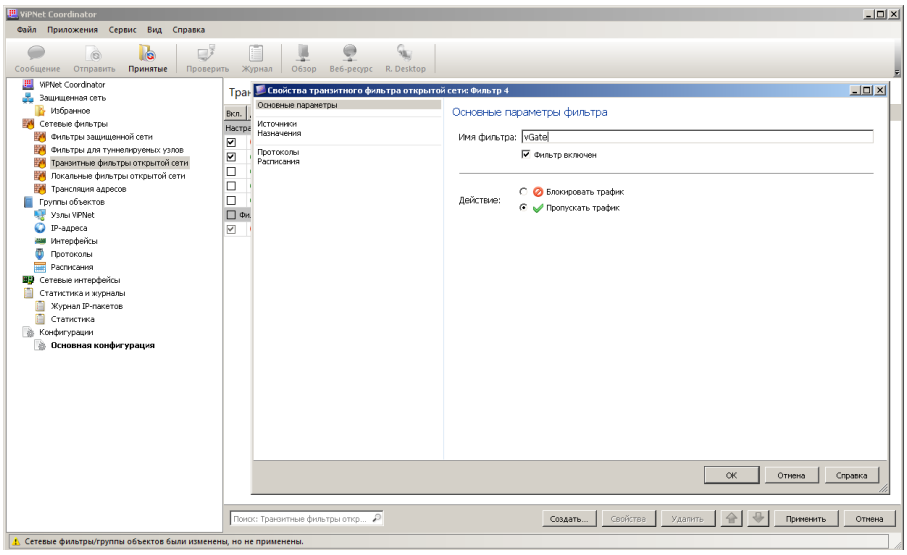
1. В меню ViPNet Coordinator выберите пункт "Группы объектов", затем "Протоколы" и создайте новую группу протоколов.



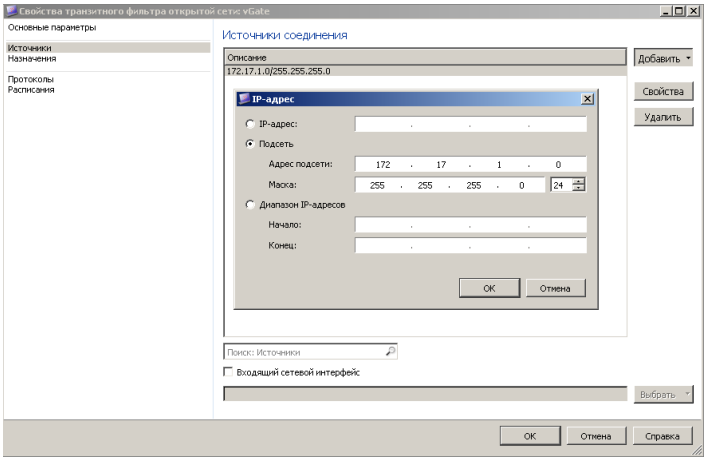
2. В окне добавления группы перейдите на вкладку "Состав", затем нажмите кнопку "Добавить" и добавьте следующие протоколы и порты Kerberos:
   - UDP 3800;
   - UDP 750;
   - UDP 88;
   - TCP 3800;
   - TCP 3801;
   - UDP 3801;
   - TCP 3808.



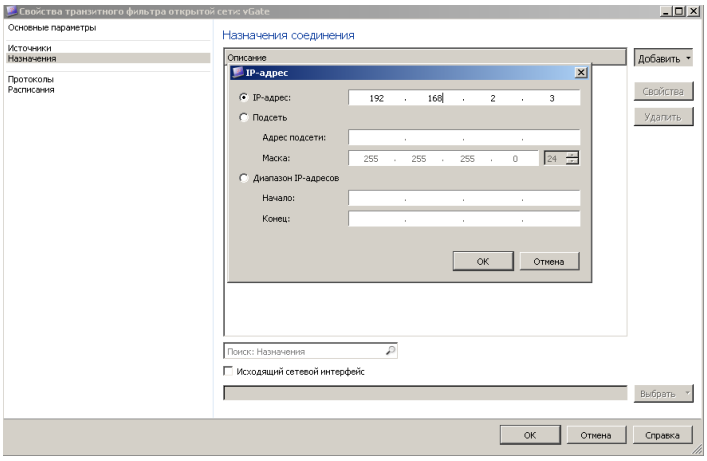
3. В меню ViPNet Coordinator выберите пункт "Сетевые фильтры", затем "Транзитные фильтры открытой сети" и создайте новый фильтр.



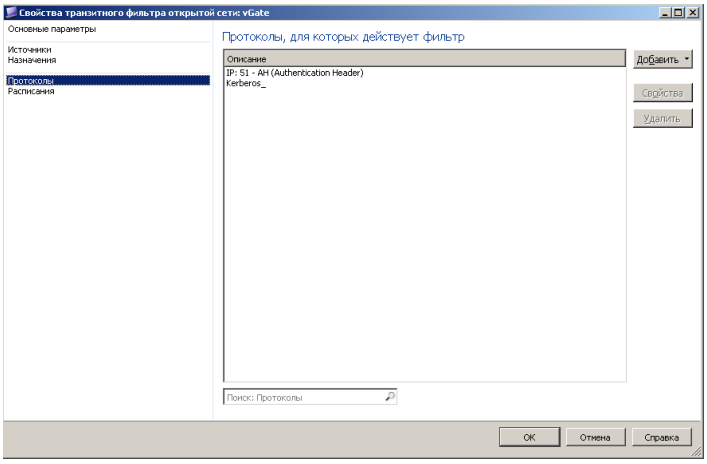
4. В окне создания фильтра перейдите на вкладку "Источники" и нажмите кнопку "Добавить", выберите "IP-адрес или группа адресов", а затем "Подсеть". Укажите адрес клиентской подсети.



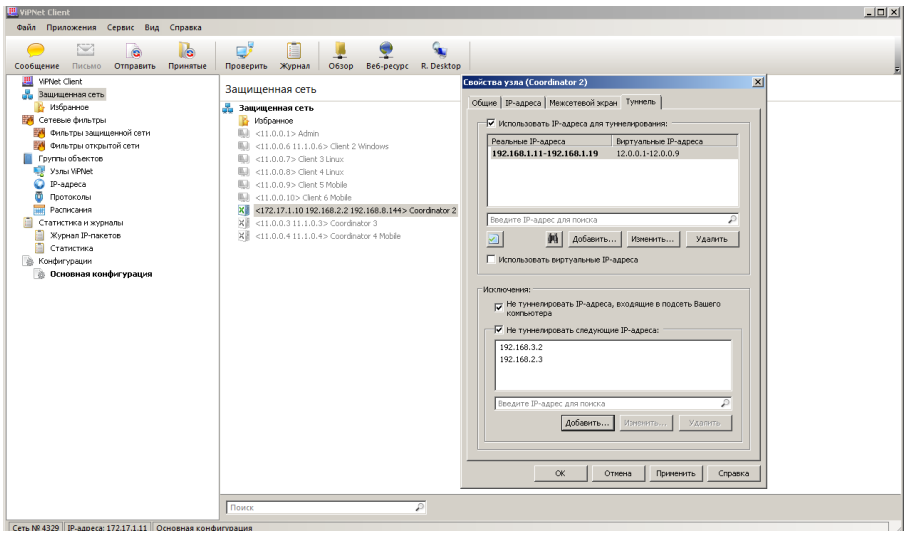
5. Перейдите на вкладку "Назначения" и нажмите кнопку "Добавить", выберите "IP-адрес или группа адресов", а затем "IP-адрес". Укажите внешний адрес сервера авторизации vGate.



6. Перейдите на вкладку "Протоколы" и нажмите кнопку "Добавить". Добавьте созданную в пп. 1, 2 группу протоколов Kerberos и IP-протокол AH, нажмите кнопку "ОК".



7. При необходимости настройте туннелирование в ViPNet Client. Для этого выберите в меню "Защищенная сеть" и перейдите в свойства узла (ViPNet Coordinator), дважды щелкнув элемент. Откройте вкладку "Туннель", отметьте "Не туннелировать следующие IP-адреса" и добавьте внешний IP-адрес сервера авторизации vGate и адреса защищенной подсети.



Вариант 2

Для настройки ViPNet:

1. Выполните действия из пп. 1–6 варианта 1 (см. выше) для ViPNet Coordinator 1.
2. Выполните действия из пп. 1–6 варианта 1 (см. выше) для ViPNet Coordinator 2.
3. При необходимости настройте туннелирование в ViPNet Client. Для этого выполните действия из п. 7 варианта 1 (см. выше).

Обеспечение совместимости агента аутентификации с МЭ

В случае эксплуатации агента аутентификации vGate совместно с межсетевыми экранами сторонних производителей (далее — МЭ) для работы vGate требуется в настройках МЭ создать правила, разрешающие исходящие соединения на следующие порты:

- порт TCP 3801;
- порт UDP 3801;
- порт TCP 3800;
- порт UDP 3800;
- порт UDP 750;
- порт UDP 88;
- порт TCP 3802;
- порт TCP 3803;
- порт TCP 3902;
- порт TCP 3906;
- порт TCP 3908;
- порт TCP 135;
- порт TCP 2179;
- порт TCP 3910.

Также может потребоваться создать разрешающее правило для протокола 51 и включить в список доверенных сетей все подсети защищаемого периметра, а также все IP-адреса основного и резервного серверов авторизации.

Настройки Windows Firewall

При установке ПО vGate на компьютере, предназначенном для сервера авторизации, в настройках Windows Firewall будут созданы разрешения для входящих соединений по следующим портам.

Порт	Протокол	Назначение
0	TCP	Служба развертывания vGate
88	UDP	vGate Kerberos IV KDC Service
443	TCP	Служба проксирования трафика vGate
750	UDP	vGate Kerberos V5 KDC Service
3800	TCP	Служба аутентификации vGate
3800	UDP	Служба аутентификации vGate
3801	UDP	Конфигурация службы аутентификации vGate
3801	TCP	Служба управления пользователями vGate
3802	TCP	Служба удаленного управления vGate
3803	TCP	Статус асинхронных операций службы удаленного управления vGate
3805	UDP	Служба аудита vGate
3806	TCP	Порт gRPC для vGate
3808	TCP	Порт для резервирования сервера авторизации vGate
3809	TCP	Служба аудита vGate (порт gRPC)
3814	TCP	Порт gRPC для vGate
3815	TCP	Порт gRPC для бэкенда vGate
5432	TCP	Порт для репликации PostgreSQL

Порт	Протокол	Назначение
3902	TCP	Служба аутентификации vGate
3904	TCP	vGate Hyper-V Rhuid for ConfigSrv
3906	TCP	vGate Hyper-V Rhuid for Client
3907	TCP	vGate Hyper-V Rhuid for ConfigSrv (Service port)
3908	TCP	vGate Hyper-V Rhuid for Client (Service port)
3915	TCP	vGate Hyper-V Rhuid for Backend (gRPC port)
135	TCP	Доступ к службе Microsoft RPC на сервере Hyper-V
2179	TCP	Доступ к консоли виртуальной машины Hyper-V
3910	TCP	Доступ к службе WMI
3912	TCP	Доступ к службам кластера
3911	TCP	Доступ к компоненту защиты Hyper-V

При эксплуатации сервера авторизации vGate совместно с межсетевыми экранами сторонних производителей также следует открыть указанные выше порты.

На компьютере, предназначенном для сервера авторизации/резервного сервера авторизации, рекомендуется отключать межсетевые экраны сторонних производителей.

Во время установки компонента защиты Hyper-V в настройках Windows Firewall будут созданы разрешения для входящих соединений по следующим портам:

Порт	Протокол	Назначение
3805	TCP	Служба аудита vGate
3809	TCP	Служба аудита vGate (порт gRPC)
3910	TCP	Доступ к службе WMI - Hyper-V Agent (TCP)
5985	TCP	Доступ к службе WinRM - Hyper-V Agent (TCP)

При эксплуатации компонента защиты Hyper-V совместно с межсетевыми экранами сторонних производителей также следует открыть указанные выше порты.

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