КОД безопасности

Средство защиты информации

vGate R2

Руководство администратора

Установка, настройка и эксплуатация

RU.88338853.501410.012 91 2-1

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**https://www.securitycode.ru**

Оглавление

Список сокращений

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
vCenter	Централизованное средство управления ESXi-серверами и виртуальными машинами
vCSA	vCenter Server Appliance — виртуальный модуль с установленным сервером vCenter и связанными с ним службами
PSC	Platform Services Controller — компонент, обеспечивающий работу служб виртуальной инфраструктуры VMware
АВИ	Администратор виртуальной инфраструктуры
АИБ	Администратор информационной безопасности
АС	Автоматизированная система
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 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. • Linux Альт 8 СП, ядро версии 4.4.211. 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
Средство просмотра отчетов	• 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 ESXi	• VMware vSphere 6.5 (VMware ESXi Server 6.5). • VMware vSphere 6.7 (VMware ESXi Server 6.7). • VMware vSphere 7.0 (VMware ESXi Server 7.0). Работа ПО vGate на кастомных образах vSphere (от производителей серверов HP, IBM и др.) не гарантируется
Компонент защиты vCenter (vCSA)	• Windows Server 2012 R2 + Update KB2999226. • Windows Server 2016 x64. • Photon OS. • VMware vSphere 6.5 (VMware vCenter Server 6.5). • VMware vSphere 6.7 (VMware vCenter Server 6.7). • VMware vCenter Server Appliance 6.5. • VMware vCenter Server Appliance 6.7. • VMware vCenter Server Appliance 7.0. Для компонента защиты vCenter требуется 200 МБ на жестком диске. Работа ПО vGate на кастомных образах vSphere (от производителей серверов HP, IBM и др.) не гарантируется
Компонент защиты PSC	• Platform Services Controller 6.7. • Platform Services Controller Appliance 6.7
Сервер мониторинга	VMware ESXi Server, удовлетворяющий минимальным требованиям: • процессор — 2 ядра; • 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 компонента защиты vCenter 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.

ESXi-серверы 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.**17**) и не менее двух Ethernet-интерфейсов при использовании сервера авторизации для маршрутизации трафика (см. стр.**22**).

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.**13**
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. • Устанавливается консоль управления vGate и средство просмотра отчетов (следует выполнить, если предполагается, что на сервере авторизации у АИБ будет основное или дополнительное рабочее место)	См. стр.**16**
	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 консоль управления и средство просмотра отчетов (следует выполнить, если предполагается, что на сервере авторизации у АИБ будет основное или дополнительное рабочее место). • Устанавливается компонент "Резервирование конфигурации". Резервный сервер: • Выполняется установка резервного сервера авторизации. • Выполняется первоначальная настройка в процессе установки ПО. • Устанавливаются консоль управления и средство просмотра отчетов (при необходимости)	См.стр.**28**
3	**Установка компонентов защиты виртуальной инфраструктуры**	В консоли управления выполняется установка компонентов защиты: • на сервер vCenter (vCSA), если он присутствует в конфигурации; • на ESXi-серверы	См. стр.**98**
4	**Установка и настройка сервера мониторинга**	Выполняется развертывание компонентов ПО vGate, обеспечивающих работу мониторинга безопасности, в следующем порядке: • выполняется развертывание и настройка сервера мониторинга; • выполняется настройка подключения к vCenter; • в веб-консоли vGate выполняется настройка подключения к серверу мониторинга	См. стр.**54**

№	Шаг установки	Особенности	Описание
5	**Установка ПО на компьютер АИБ**	• Устанавливаются агент аутентификации, консоль управления и средство просмотра отчетов. Этот шаг следует пропустить, если рабочее место АИБ на сервере авторизации	См. стр.49
6	**Установка ПО на компьютер АВИ**	Устанавливается агент аутентификации	См.стр.49
7	**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.49

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 ESXi-серверы, серверы vCenter и другие элементы виртуальной инфраструктуры) рекомендуется отделить от сети виртуальных машин и других сетей виртуальной инфраструктуры.
- Если в виртуальной инфраструктуре используются функции vMotion и Fault Tolerance, рекомендуется организовать отдельную сеть репликации виртуальных машин, отделив ее от сетей администрирования и сетей виртуальных машин.
- Если данные виртуальных машин хранятся за пределами ESXi-серверов в отдельной системе хранения, рекомендуется создать сеть передачи данных на основе технологии Ethernet (iSCSI) или Fiber channel. При необходимости сеть передачи данных и сеть репликации виртуальных машин могут быть совмещены.

Для работы в сети, сконфигурированной таким образом, ESXi-серверы 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.

Примечание. После установки сервера авторизации vGate, агента аутентификации или компонента защиты vCenter в списке компонентов (в свойствах сетевого адаптера) появится сетевая служба "Security Code vGate NDIS 6.0 network filter driver".

Перед конфигурированием локальной сети рекомендуется ознакомиться с документацией к продуктам VMware.

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

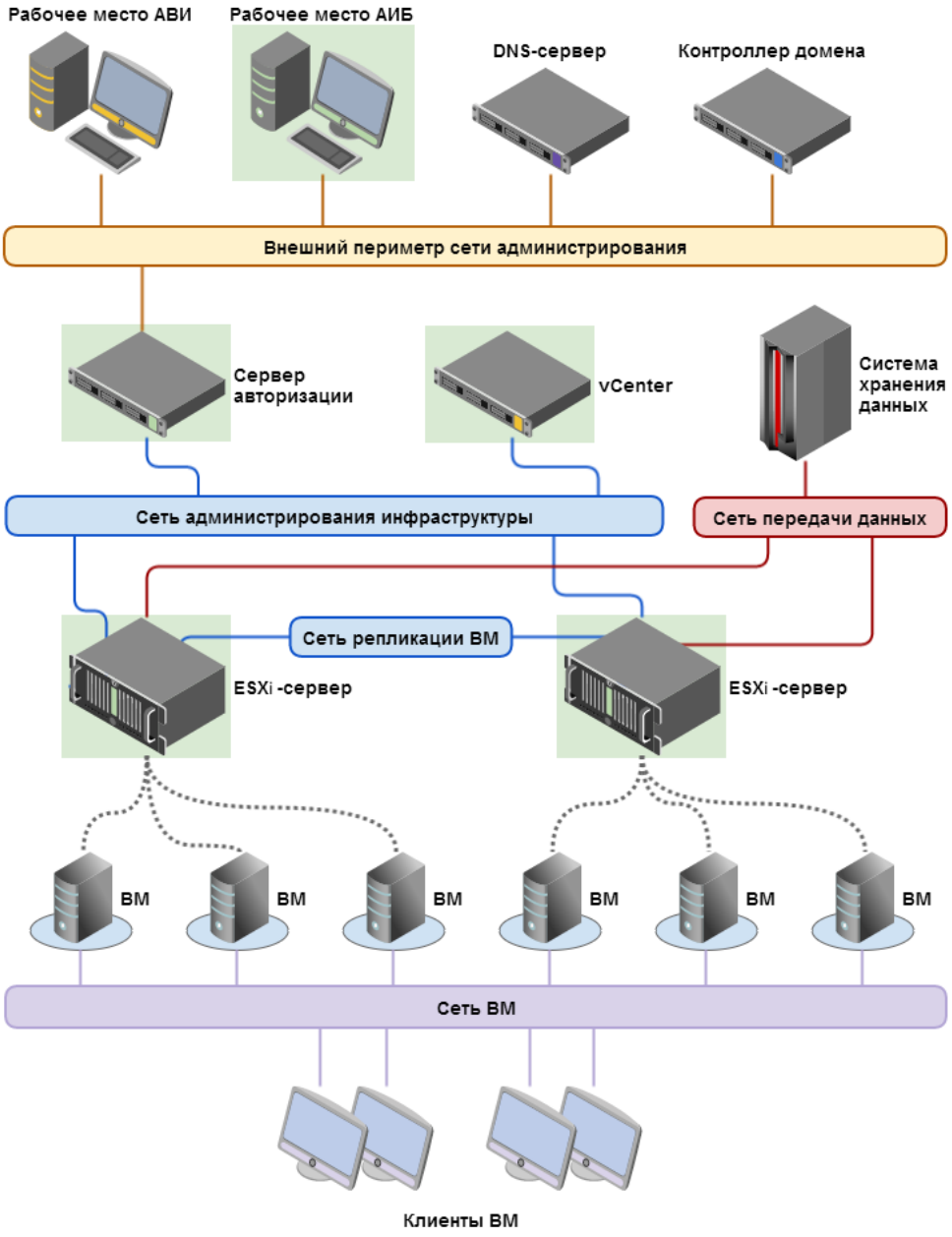


Рис.1 Архитектура сети и размещение компонентов (маршрутизацию трафика выполняет сервер авторизации vGate)

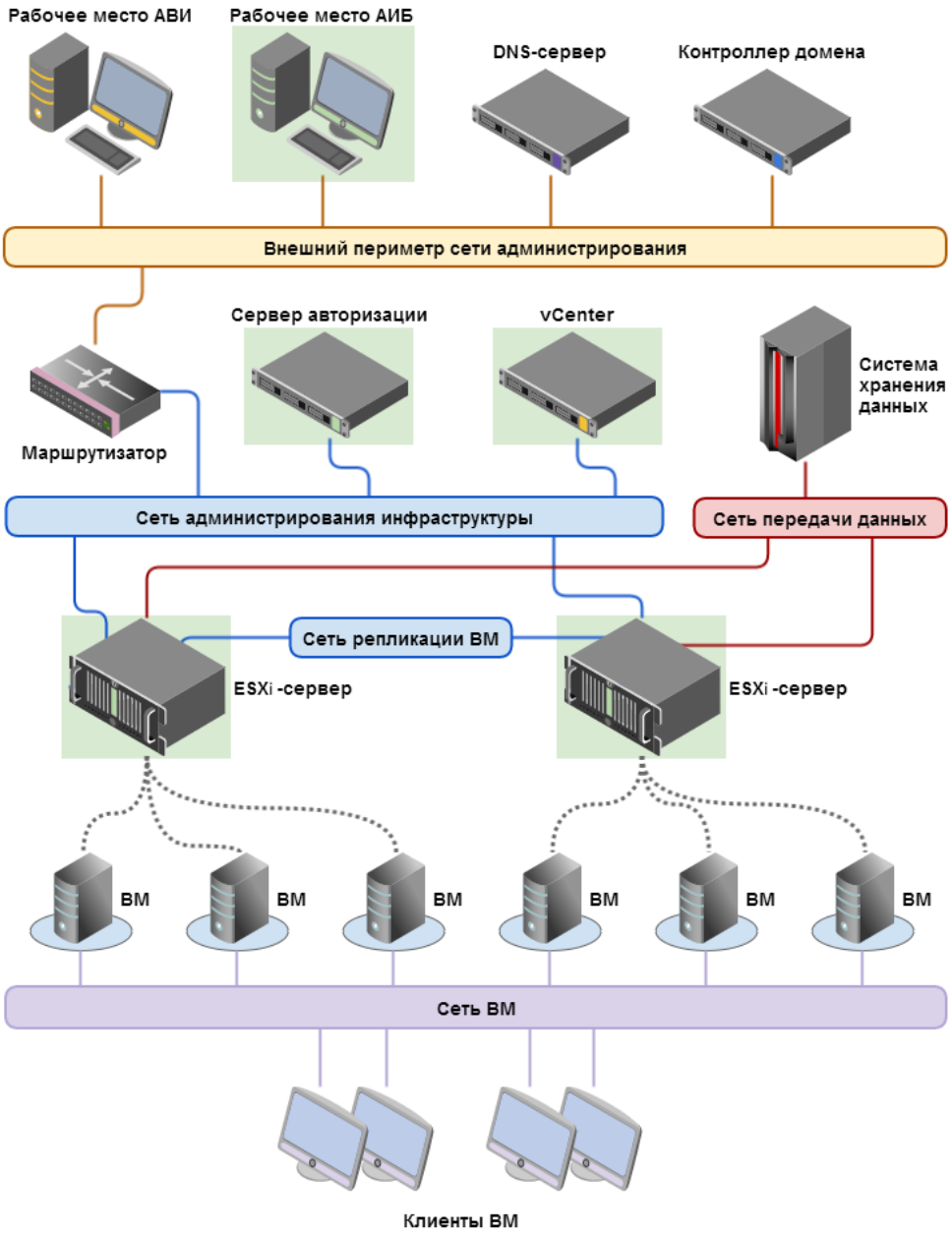


Рис.2 Архитектура сети и размещение компонентов (маршрутизация с помощью существующего маршрутизатора в сети)

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 (ESXi-серверы, vCenter) 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 (ESXi-серверы, vCenter) 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.**84**). 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.**17**).

  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.**15**). 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.**240**.

- С помощью сервера авторизации vGate (см. стр.**22**).

  При выборе этого способа защищаемые серверы должны быть расположены в отдельной подсети. На всех компьютерах защищаемого периметра сети администрирования (ESXi-серверы и серверы vCenter) 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.85).

Внимание! Если на компьютере, предназначенном для сервера авторизации, предполагается использовать компонент "Средство просмотра отчетов", необходимо предварительно установить Microsoft Report Viewer 2010 SP1 Redistributable Package. Для установки запустите с установочного диска из каталога \Redistributables\Microsoft Report Viewer Redistributable 2010 файл ReportViewer.exe и следуйте указаниям мастера установки.

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 ESXi-серверами и vCenter 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 VMware vSphere" стартового диалога программы установки.

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

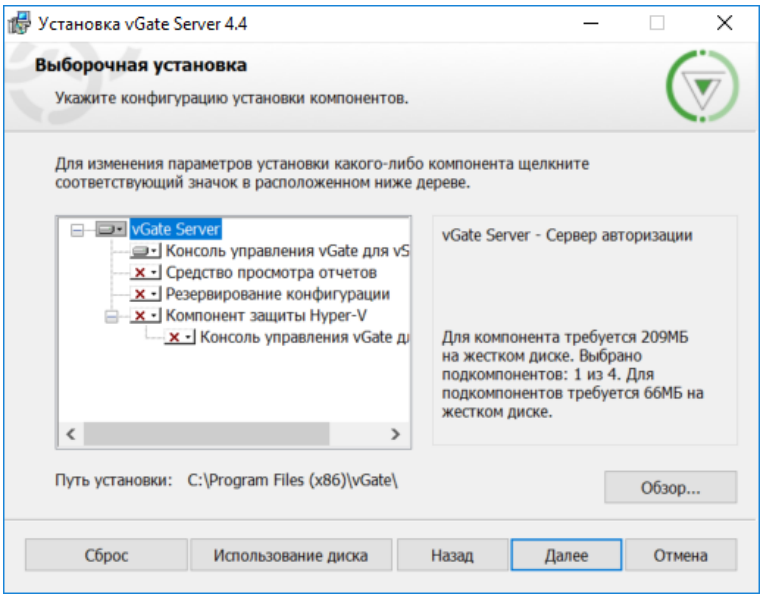
   Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.
4. Нажмите кнопку "Далее".

   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.

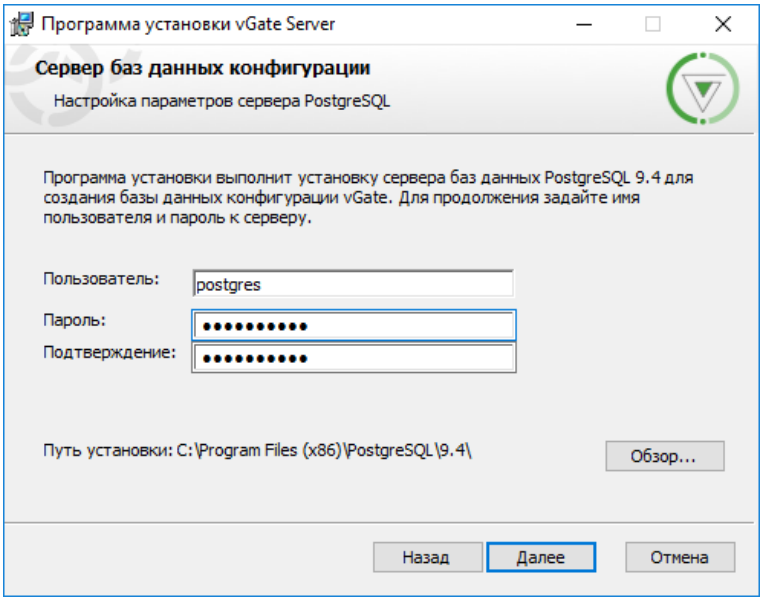
- Выберите для установки компонент "Консоль управления vGate". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Компоненты "Резервирование конфигурации" и "Средство просмотра отчетов" по умолчанию не устанавливаются. Если предполагается использовать резервирование конфигурации (см. стр. 28) или средство просмотра отчетов, выберите эти компоненты для установки. Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".
- "Компонент защиты Hyper-V" устанавливается для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V и не требуется для защиты VMware vSphere.

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.

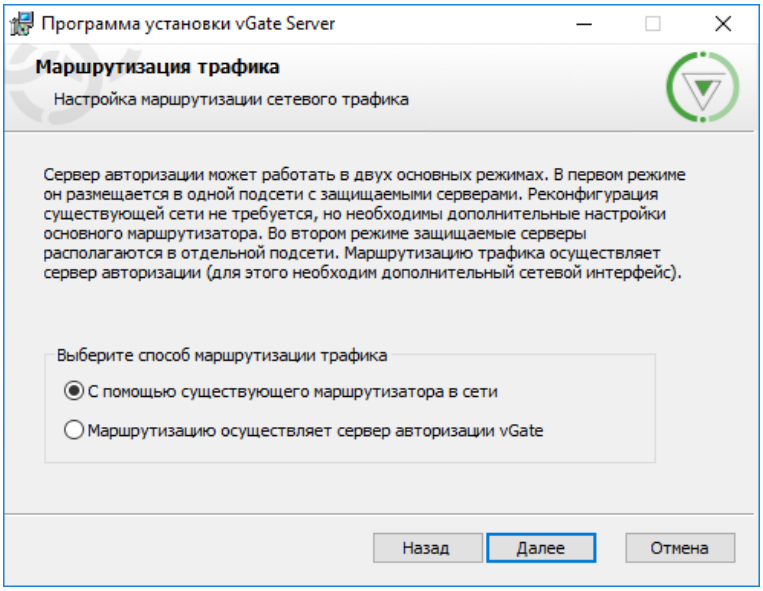


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

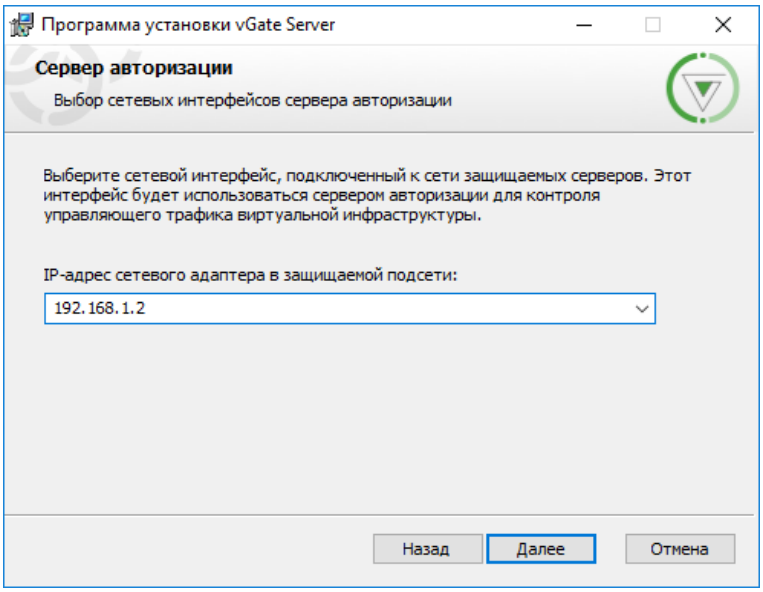
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для 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.



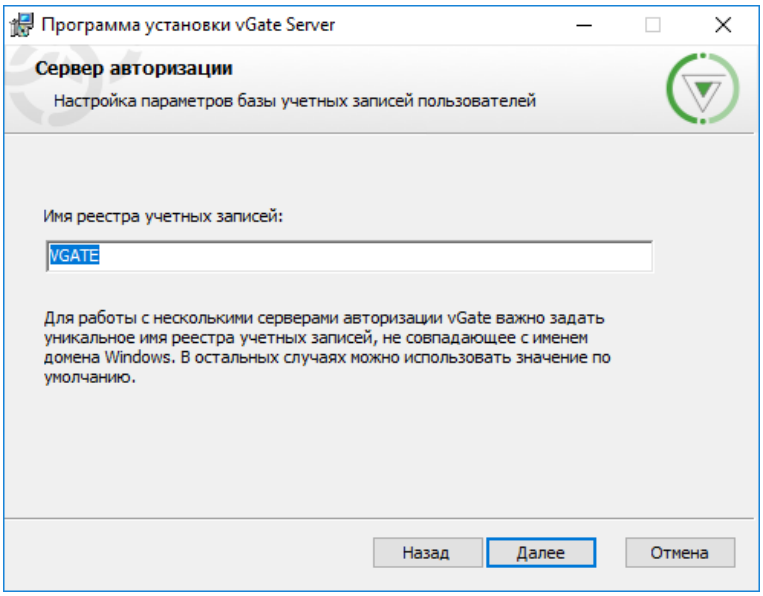
9. Выберите способ маршрутизации трафика "С помощью существующего маршрутизатора в сети" и нажмите кнопку "Далее".

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".

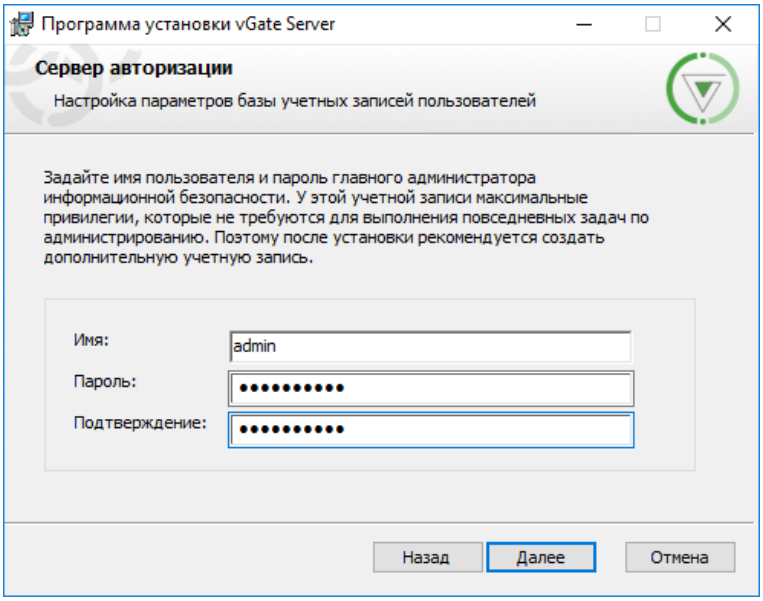
На экране появится следующий диалог.



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

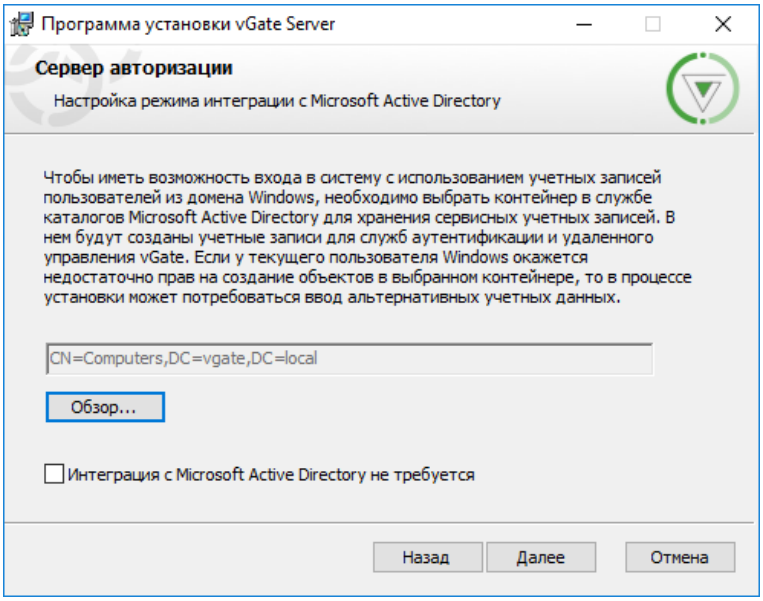
11. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

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.**13**) 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 ESXi-серверами и vCenter 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 VMware vSphere" 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.

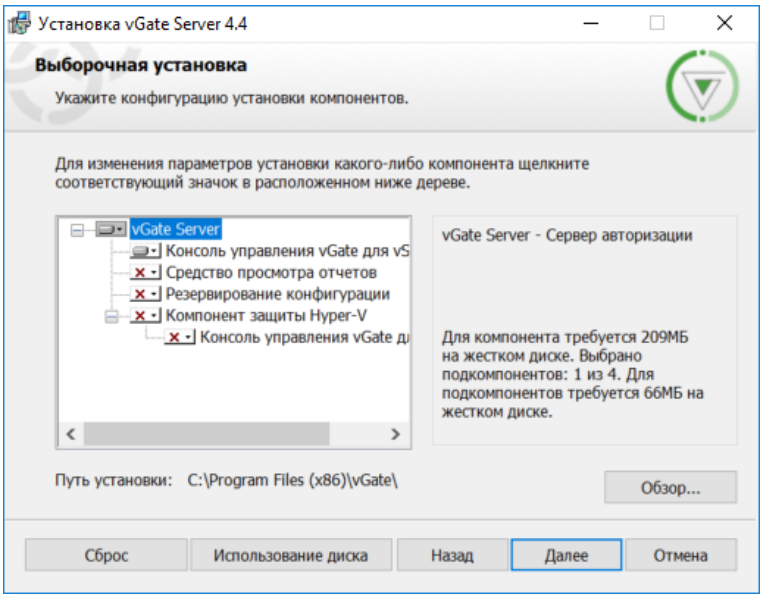
4. Нажмите кнопку "Далее".

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.

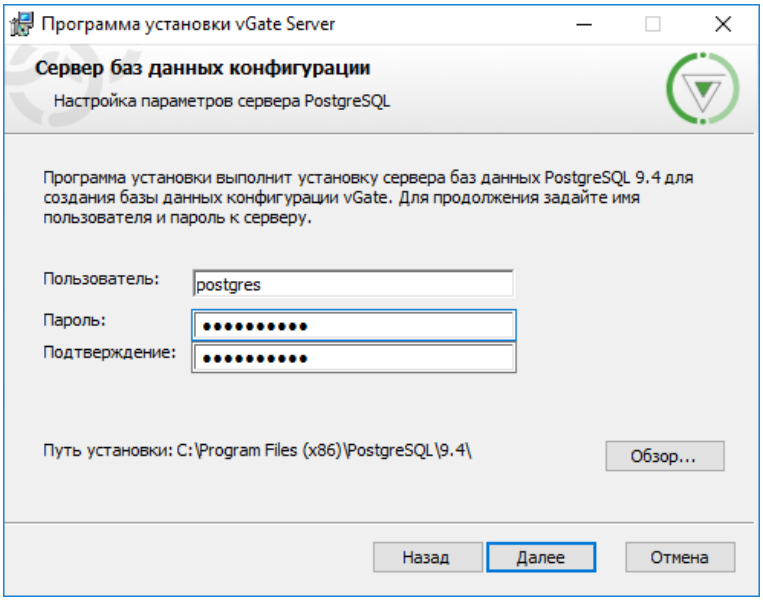
- Выберите для установки компонент "Консоль управления vGate". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Компоненты "Резервирование конфигурации" и "Средство просмотра отчетов" по умолчанию не устанавливаются. Если предполагается использовать резервирование конфигурации (см. стр. 28) или средство просмотра отчетов, выберите эти компоненты для установки. Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".
- "Компонент защиты Hyper-V" устанавливается для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V и не требуется для защиты VMware vSphere.

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.

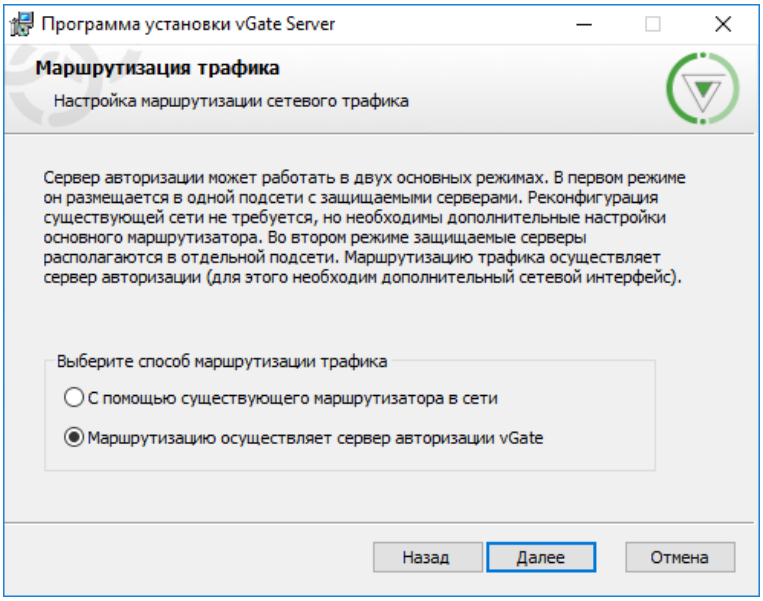


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

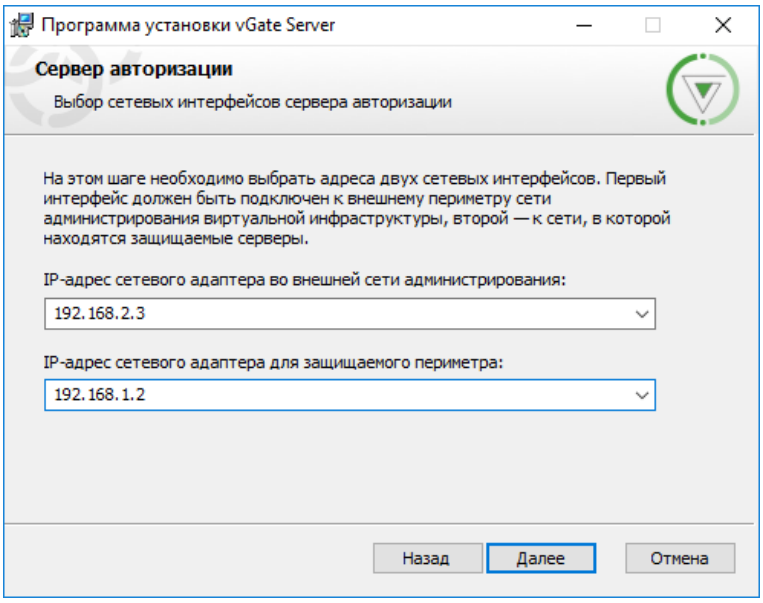
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для 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".

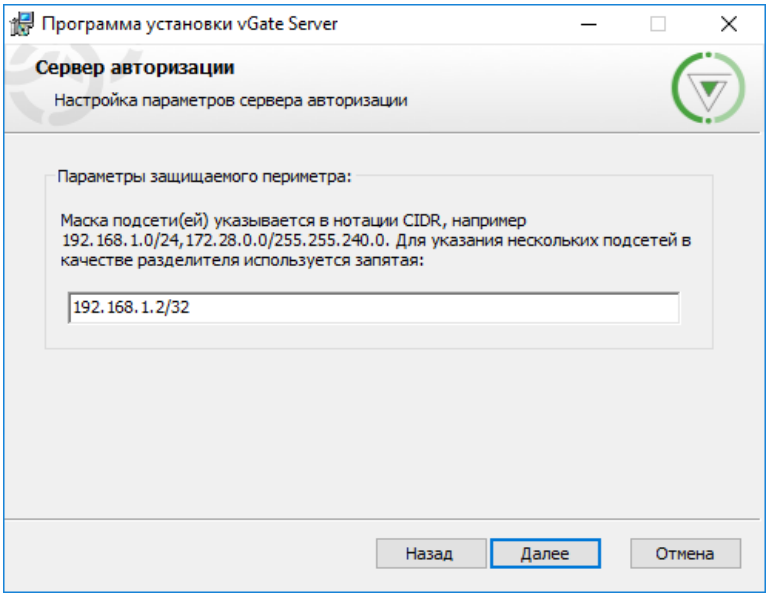
На экране появится следующий диалог.



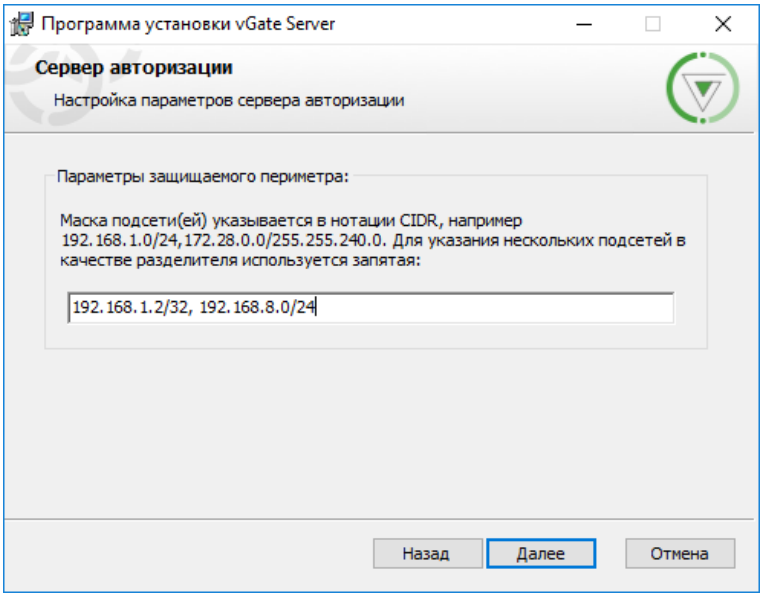
10. Укажите сетевые параметры сервера авторизации и нажмите кнопку "Далее".

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.



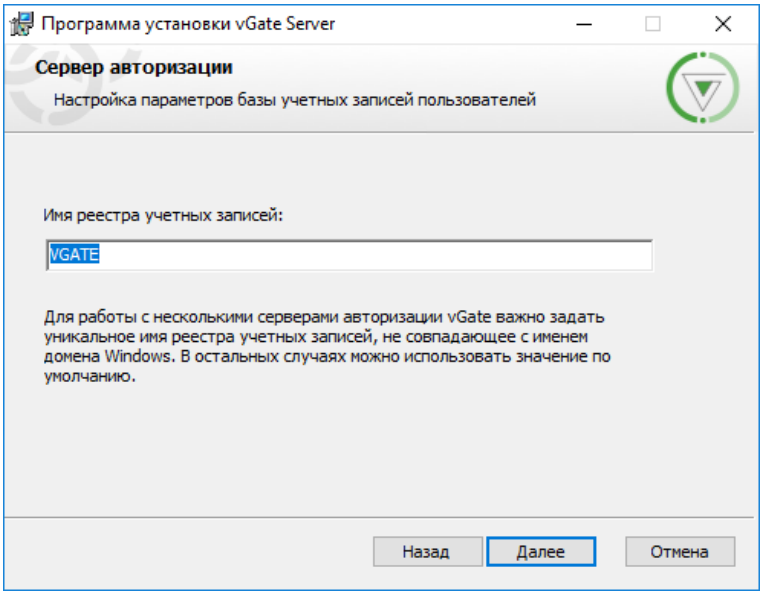
11. Если защищаемый периметр сети администрирования состоит из нескольких сетей, укажите их IP-адреса в текстовом поле, используя запятую в качестве разделителя.



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 ESXi-серверы, и нажмите кнопку "Далее".

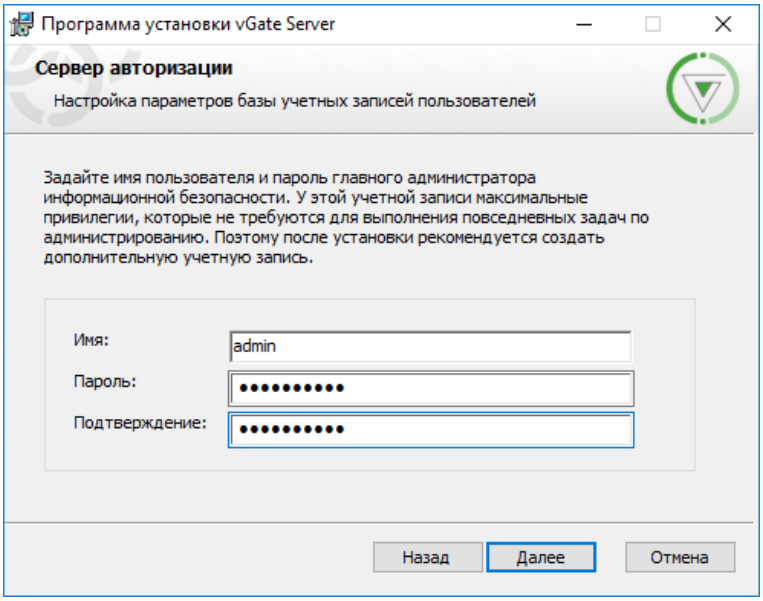
На экране появится следующий диалог.



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

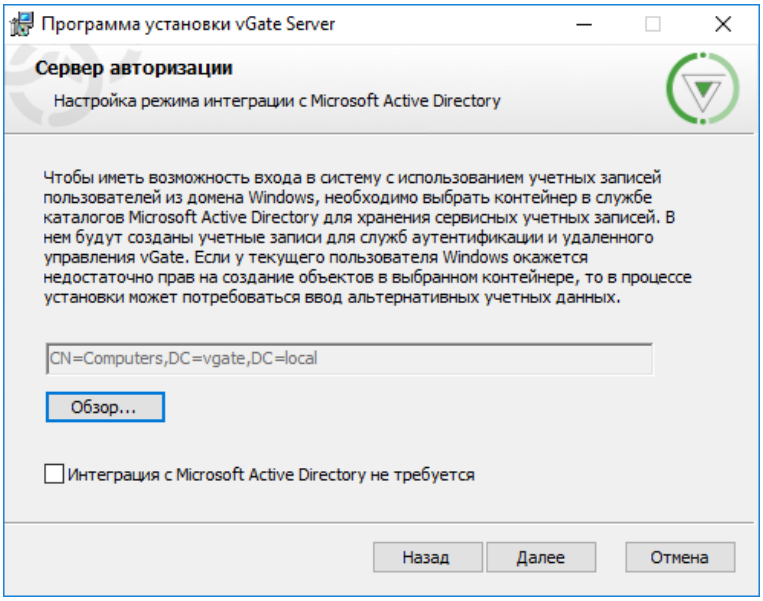
13. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

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.**13**) 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.**76**).

> **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.**29**).

  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.**15**). 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.**240**.

- С помощью сервера авторизации vGate (см. стр.**38**).

  При выборе этого способа защищаемые серверы должны быть расположены в отдельной подсети. На всех компьютерах защищаемого периметра сети администрирования (ESXi-серверы и серверы vCenter) 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.**85**).

Внимание! Если на компьютерах, предназначенных для основного и резервного серверов авторизации, предполагается использовать компонент "Средство просмотра отчетов", необходимо предварительно установить Microsoft Report Viewer 2010 SP1 Redistributable Package. Для установки запустите с установочного диска из каталога \Redistributables\Microsoft Report Viewer Redistributable 2010 файл ReportViewer.exe и следуйте указаниям мастера установки.

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 ESXi-серверами и vCenter 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 ESXi-серверами и vCenter 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 VMware vSphere" стартового диалога программы установки.

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

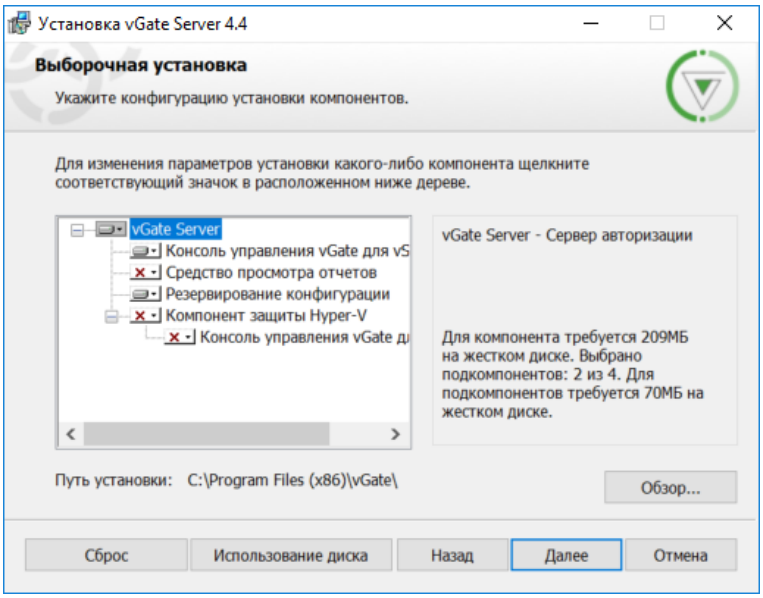
   Программа начнет выполнение подготовительных действий, по окончании которых на экран будет выведен диалог приветствия программы установки.
4. Нажмите кнопку "Далее".

   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.

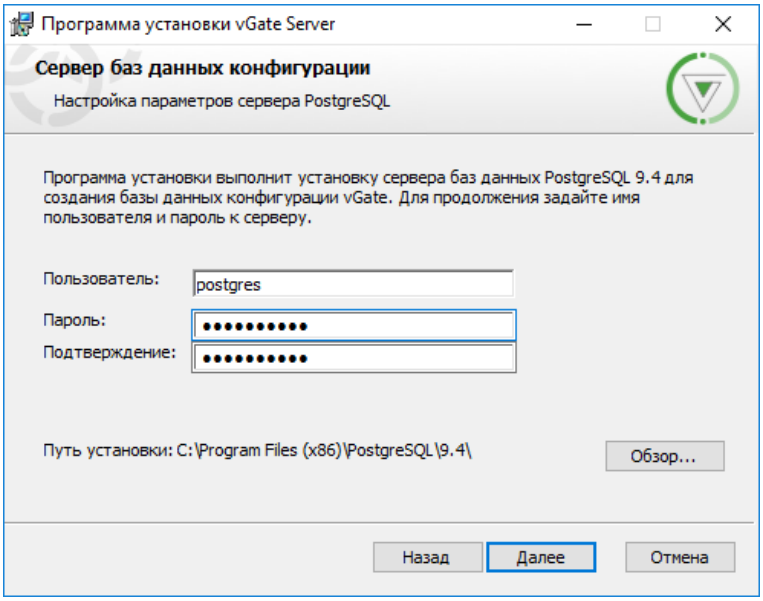
- Выберите для установки компонент "Консоль управления vGate". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Выберите для установки компонент "Резервирование конфигурации".
- Компонент "Средство просмотра отчетов" по умолчанию не устанавливается. Для установки нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск". Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".
- "Компонент защиты Hyper-V" устанавливается для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V и не требуется для защиты VMware vSphere.

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.

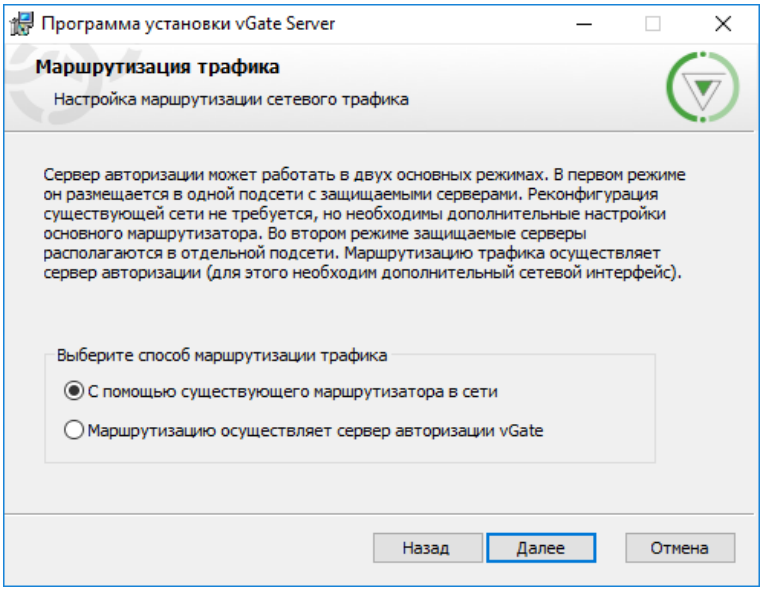


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

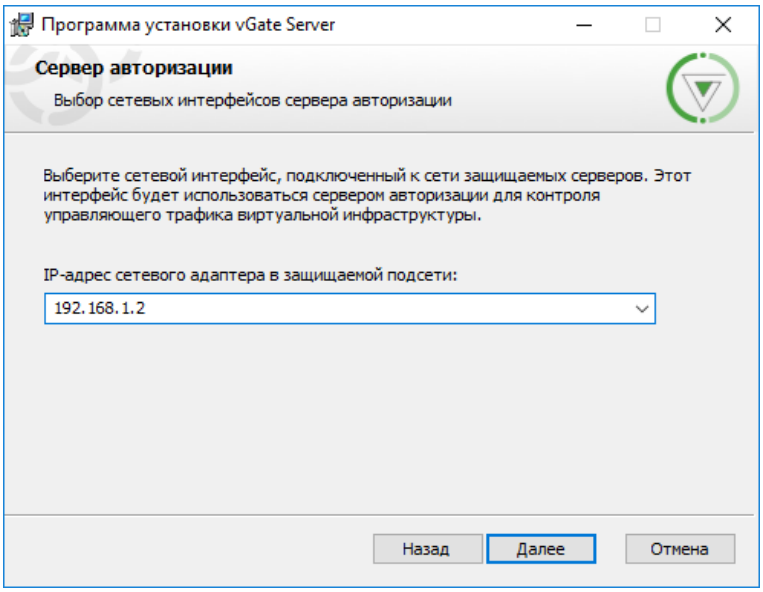
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для 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.



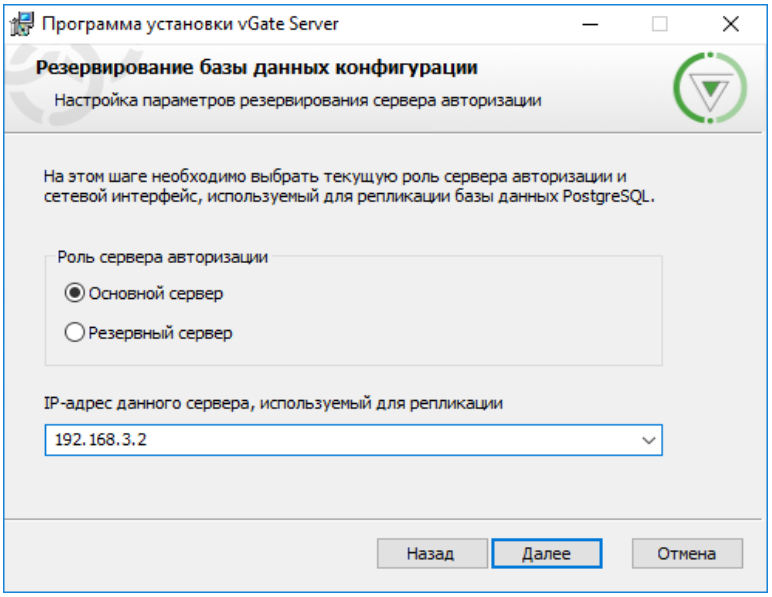
9. Выберите способ маршрутизации трафика "С помощью существующего маршрутизатора в сети" и нажмите кнопку "Далее".

На экране появится следующий диалог.



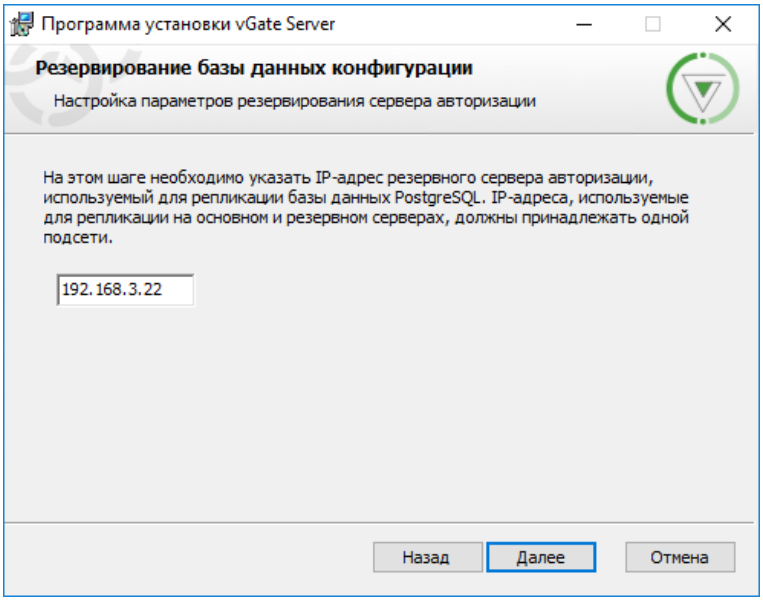
10. Укажите IP-адрес адаптера 1 сервера авторизации, через который будут проходить маршруты в защищаемый периметр сети администрирования инфраструктуры и из него, и нажмите кнопку "Далее".

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



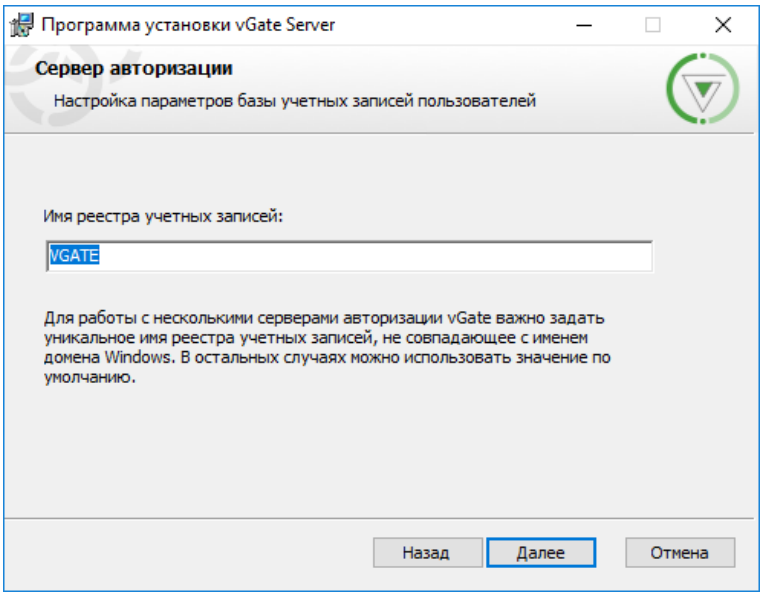
11. Выберите роль сервера авторизации "Основной сервер", укажите IP-адрес этого сервера, используемый для репликации данных между основным и резервным серверами авторизации в сети резервирования, и нажмите кнопку "Далее".

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".

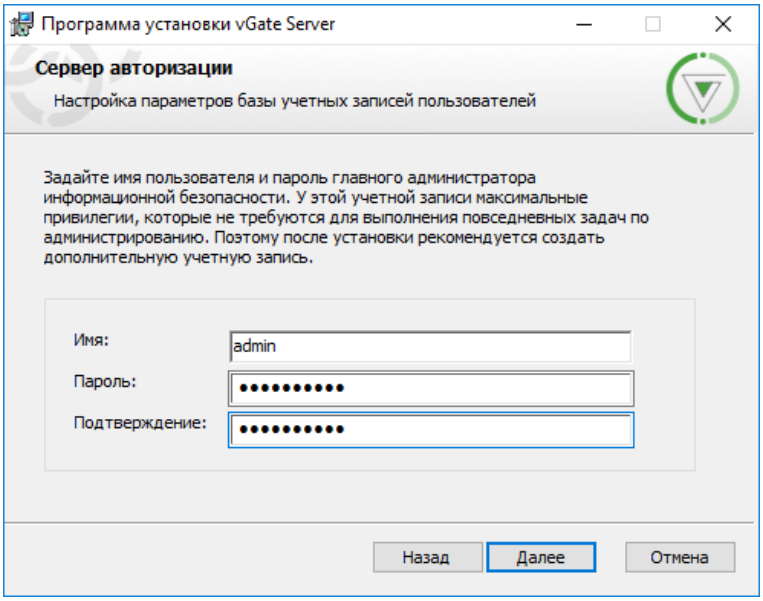
На экране появится следующий диалог.



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

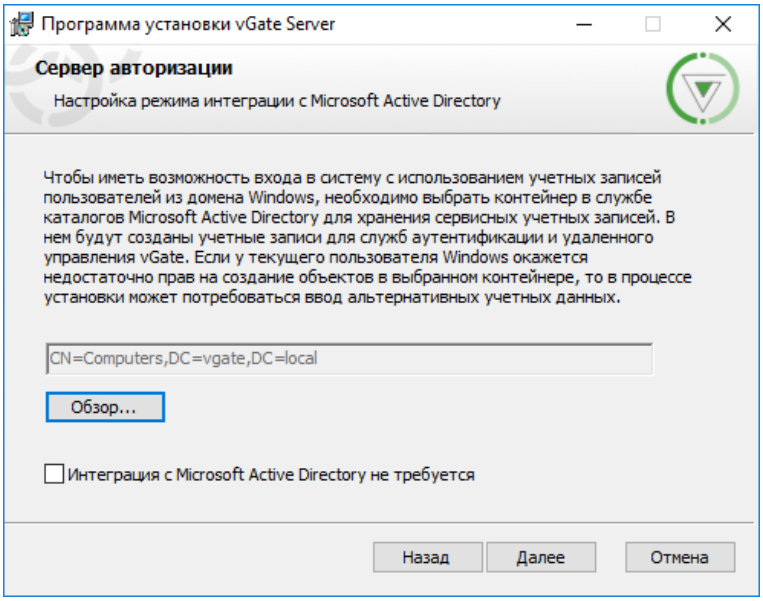
13. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

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.**13**) 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".

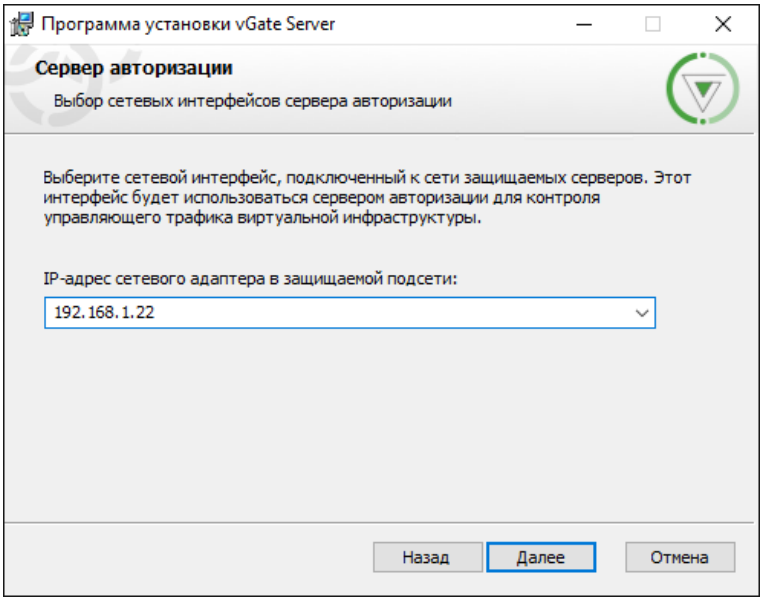
На экране появится диалог установки сервера баз данных PostgreSQL.

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.

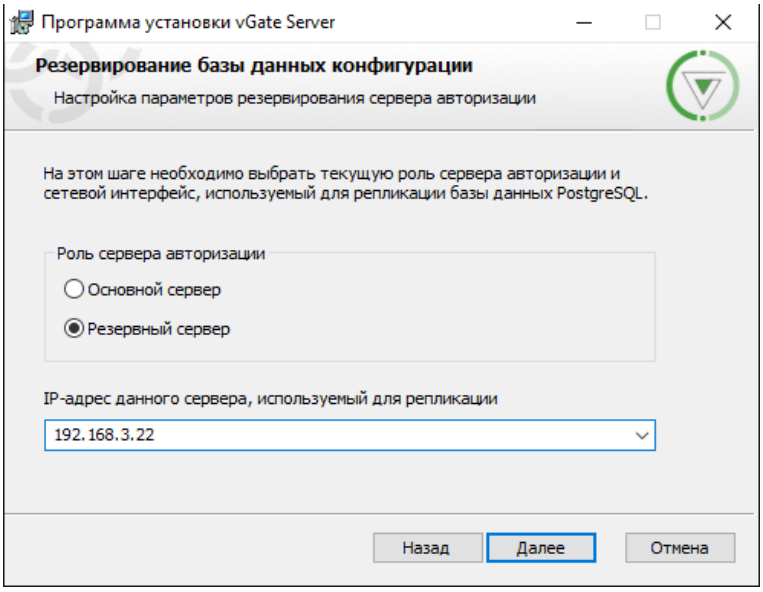
8. Выберите способ маршрутизации трафика "С помощью основного маршрутизатора" и нажмите кнопку "Далее".

На экране появится диалог настройки сетевых параметров.



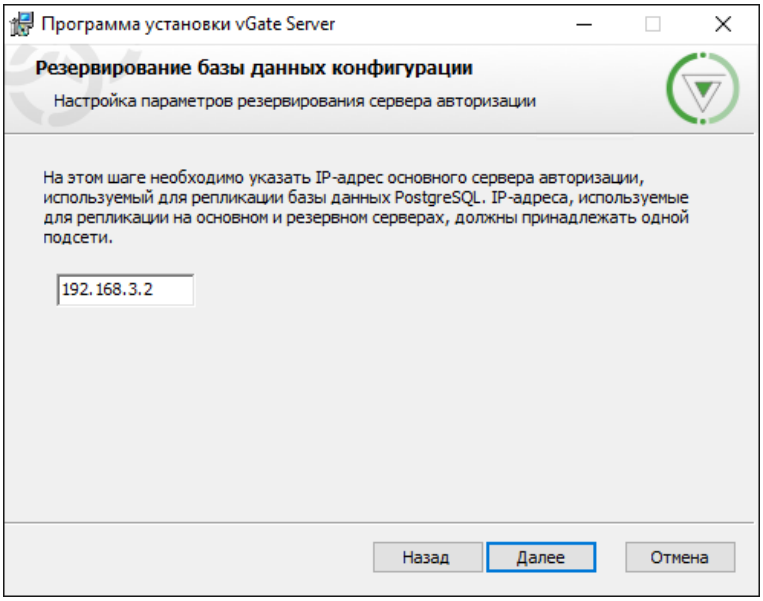
9. Укажите IP-адрес сетевого адаптера резервного сервера авторизации и нажмите кнопку "Далее".

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 настройки параметров входа в систему для службы проксирования трафика vGate (vcp.exe).

12. Укажите параметры учетной записи службы проксирования трафика vGate (vcp.exe), которая будет использоваться для подключения к виртуальной инфраструктуре, и нажмите кнопку "Далее".

На экране появится диалог с сообщением о готовности к установке.

13. 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.

14. 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.**61**.

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 ESXi-серверами и vCenter 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 ESXi-серверами и vCenter 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 VMware vSphere" 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.

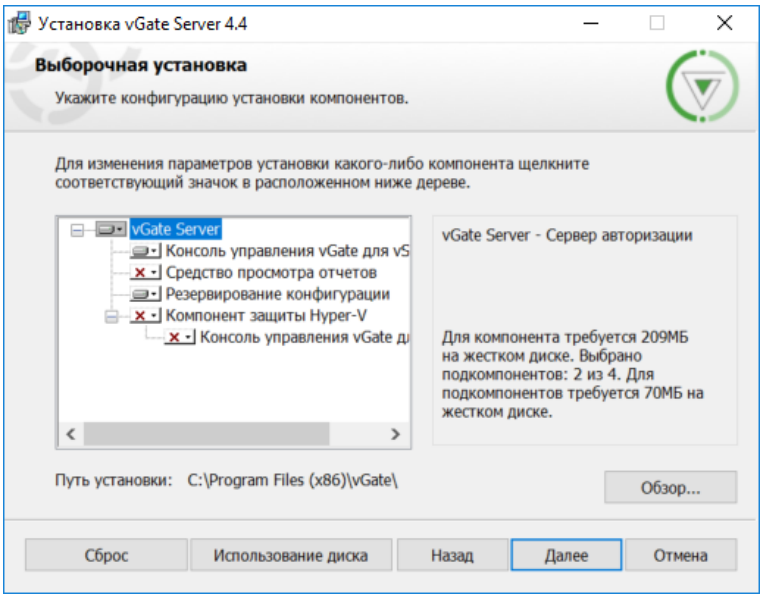
4. Нажмите кнопку "Далее".

   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.

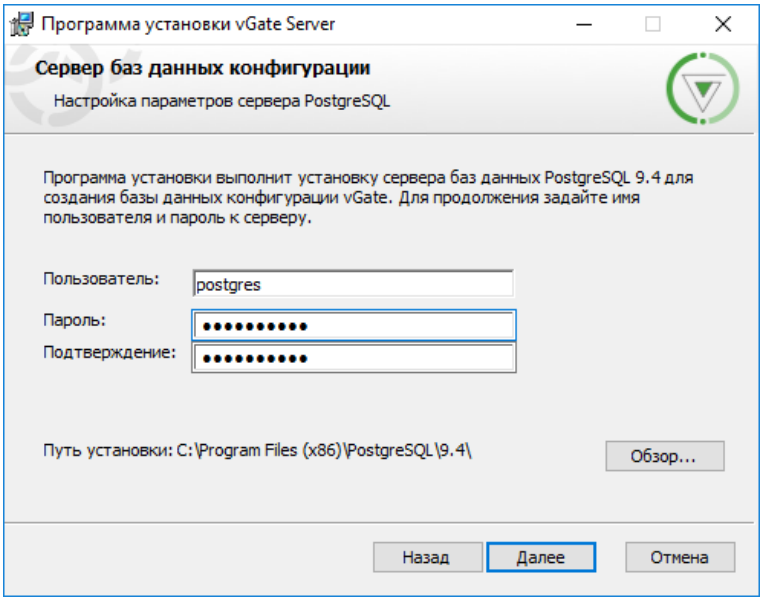
- Выберите для установки компонент "Консоль управления vGate". Для этого нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск".
- Выберите для установки компонент "Резервирование конфигурации".
- Компонент "Средство просмотра отчетов" по умолчанию не устанавливается. Для установки нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск". Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".
- "Компонент защиты Hyper-V" устанавливается для защиты виртуальной инфраструктуры на платформе Microsoft Hyper-V и не требуется для защиты VMware vSphere.

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.

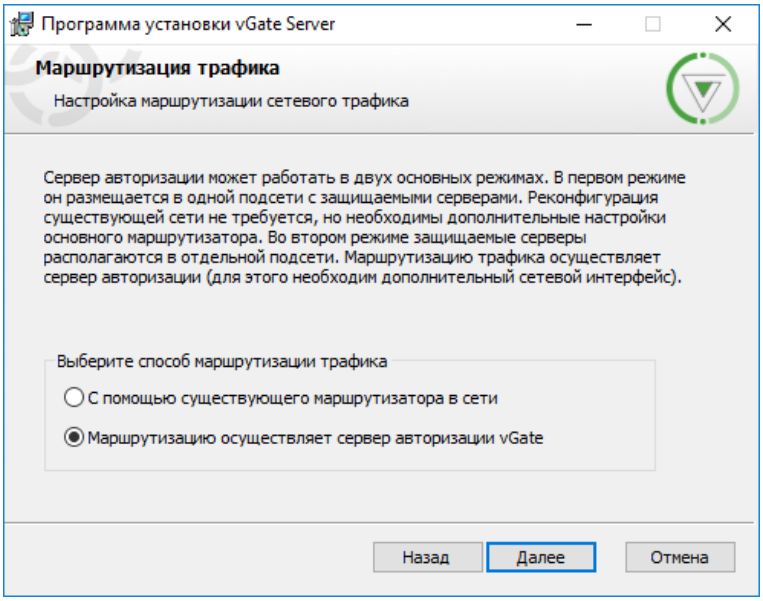


8. Укажите имя и пароль пользователя сервера баз данных PostgreSQL, при необходимости измените путь к папке установки базы данных и нажмите кнопку "Далее". При установке vGate с резервированием имена пользователя PostgreSQL на основном и резервном серверах должны совпадать.

Примечание.

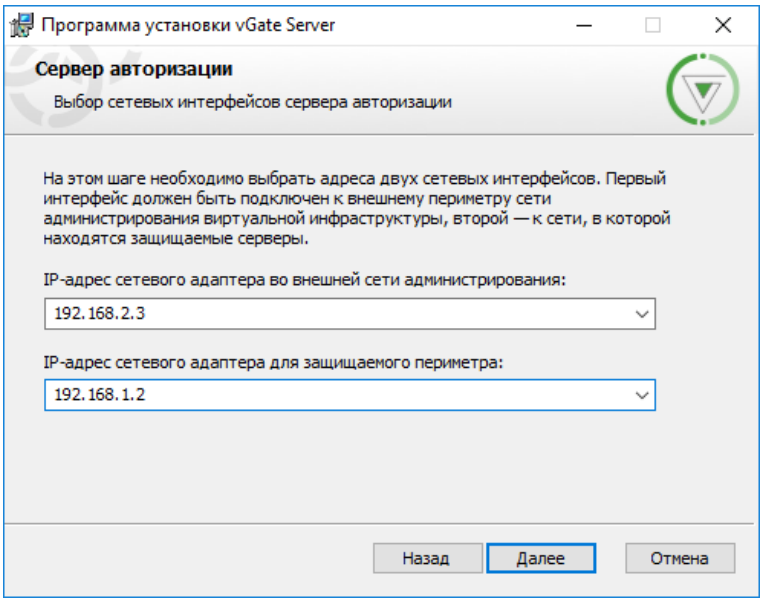
- Сервер баз данных PostgreSQL 9.4 будет установлен автоматически при установке vGate, и на нем будет создана база данных конфигурации vGate. В случае если сервер PostgreSQL уже установлен на компьютере, программа установки предложит использовать его для создания базы данных конфигурации vGate.
- Для 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".

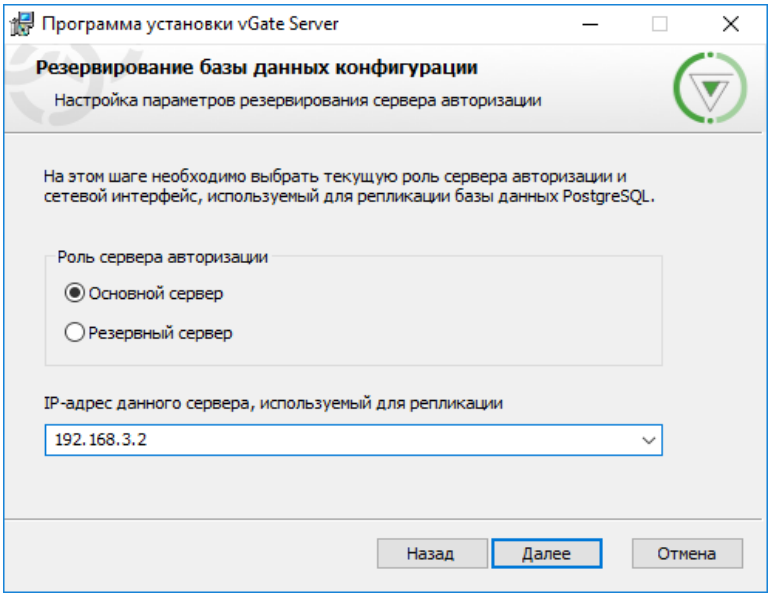
На экране появится следующий диалог.



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

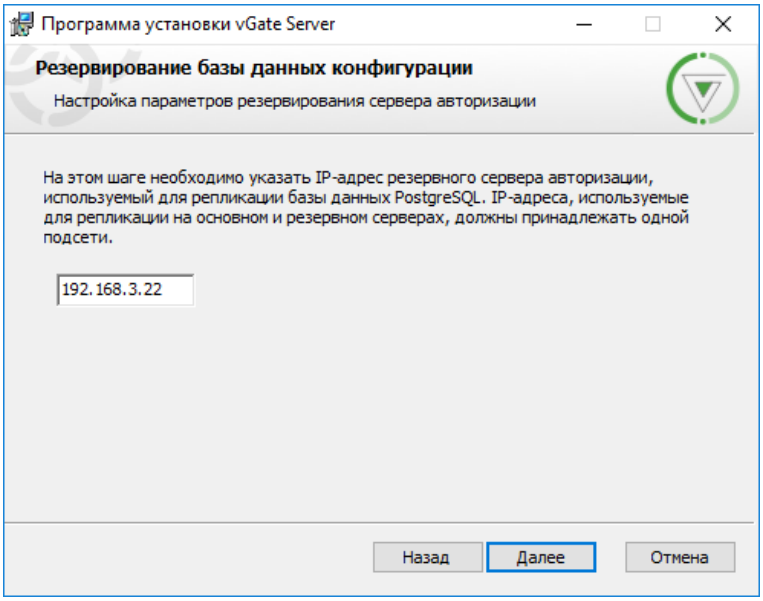
Параметр	Описание
IP-адрес сетевого адаптера во внешней сети администрирования	IP-адрес сервера во внешнем периметре сети администрирования инфраструктуры (подсети, в которой размещены рабочие места АИБ и АВИ)
IP-адрес сетевого адаптера для защищаемого периметра	IP-адрес сервера в защищаемом периметре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



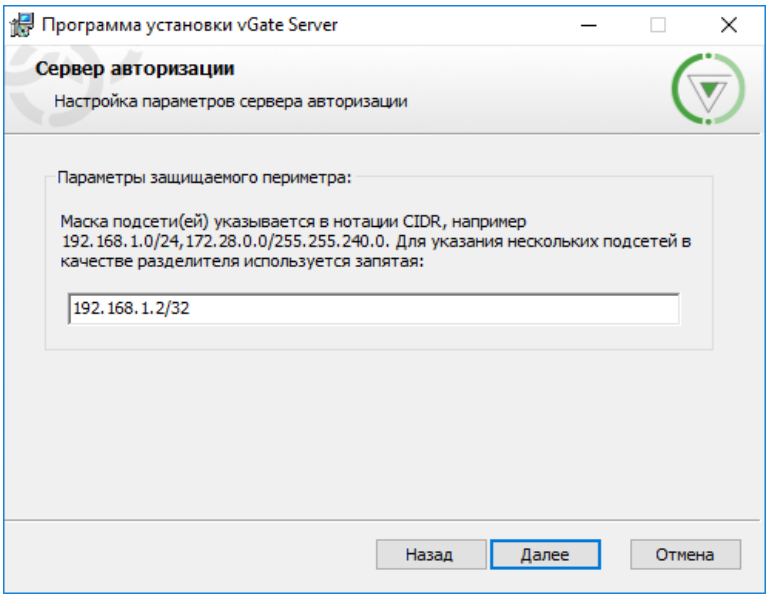
11. Выберите роль сервера авторизации "Основной сервер", укажите IP-адрес этого сервера, используемый для репликации данных между основным и резервным серверами авторизации в сети резервирования, и нажмите кнопку "Далее".

На экране появится диалог настройки параметров резервного сервера.

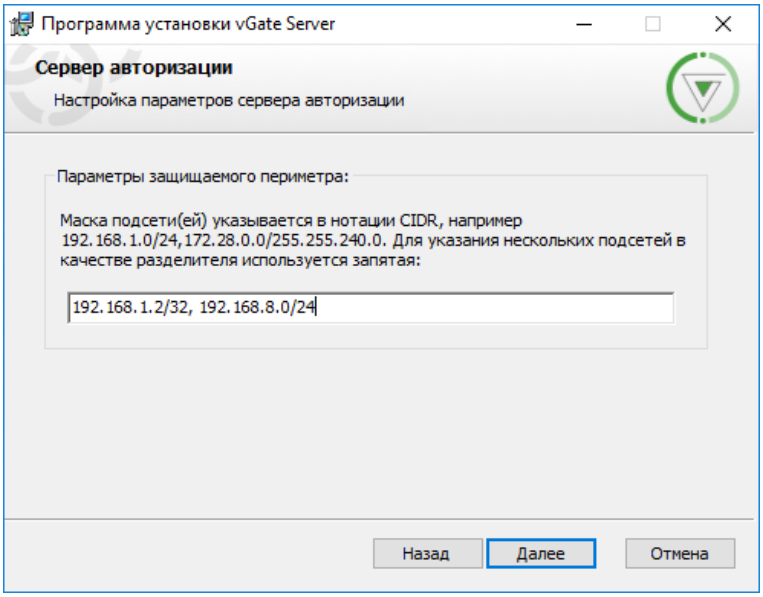


12. Укажите IP-адрес резервного сервера авторизации в сети резервирования, используемый для репликации, и нажмите кнопку "Далее".

На экране появится следующий диалог.



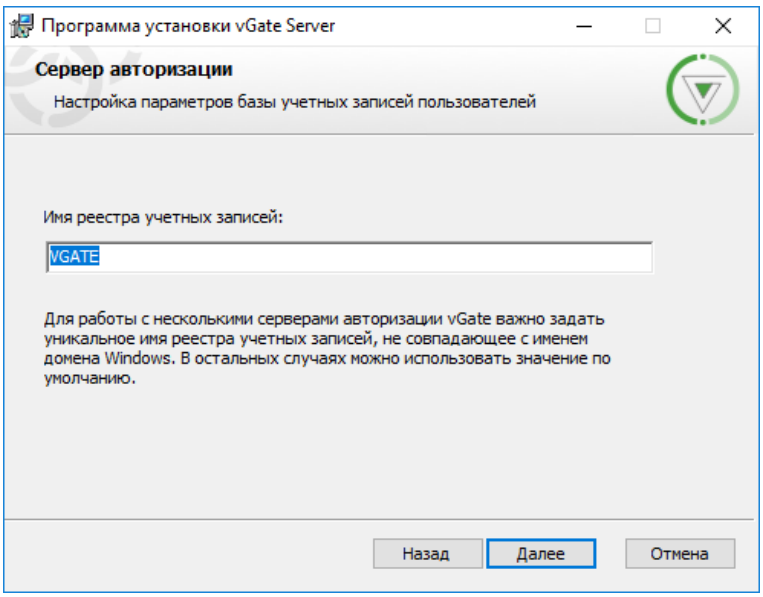
13. Если защищаемый периметр сети администрирования состоит из нескольких сетей, укажите их IP-адреса в текстовом поле, используя запятую в качестве разделителя.



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 ESXi-серверы, и нажмите кнопку "Далее".

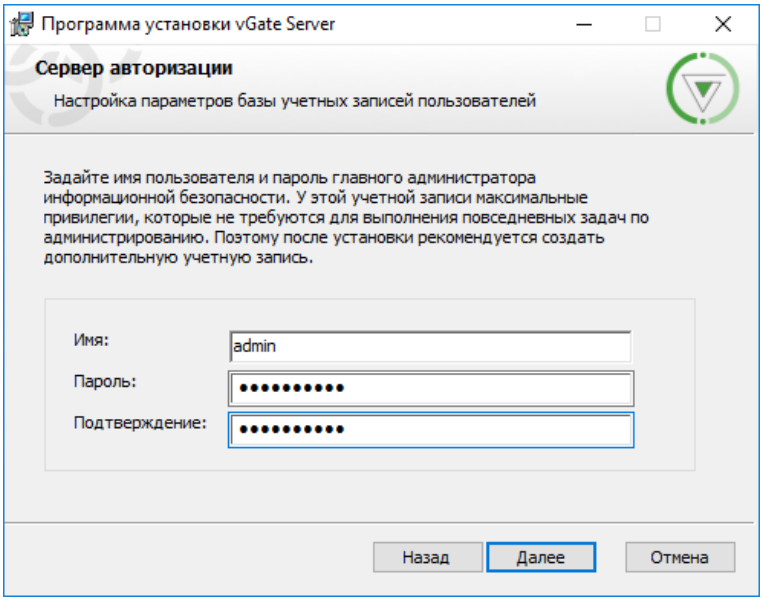
На экране появится следующий диалог.



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

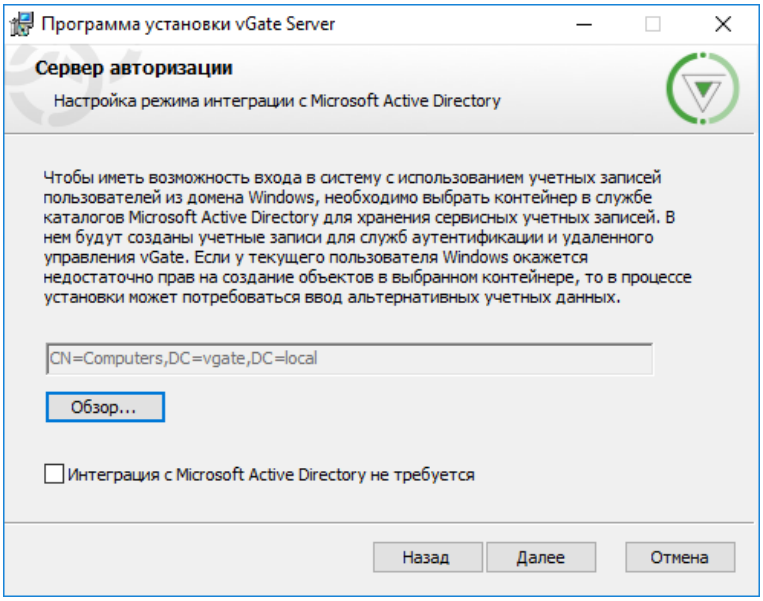
15. Укажите имя реестра учетных записей vGate и нажмите кнопку "Далее".

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.**13**) 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".

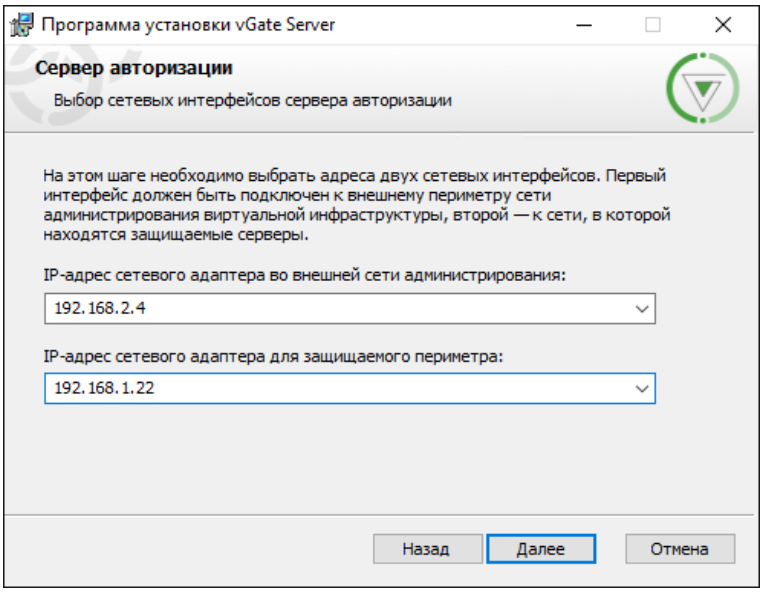
На экране появится диалог установки сервера баз данных PostgreSQL.

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".

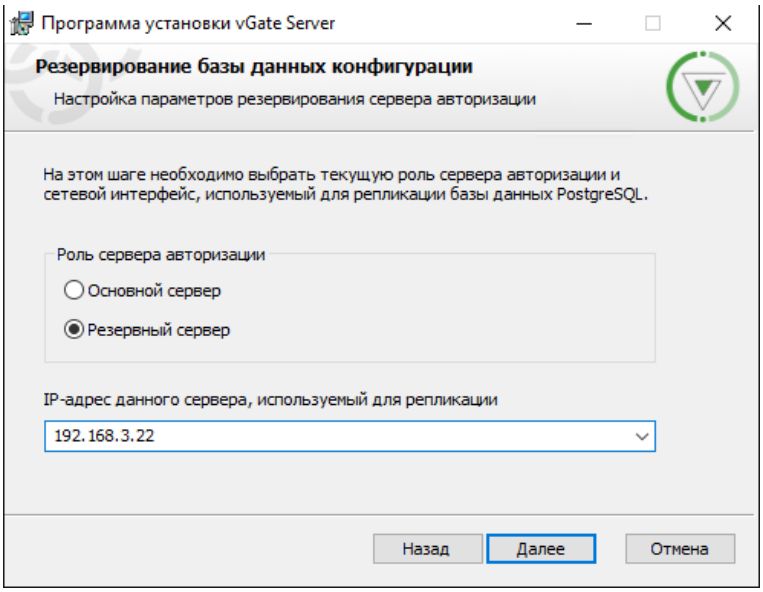
На экране появится диалог настройки сетевых параметров.



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

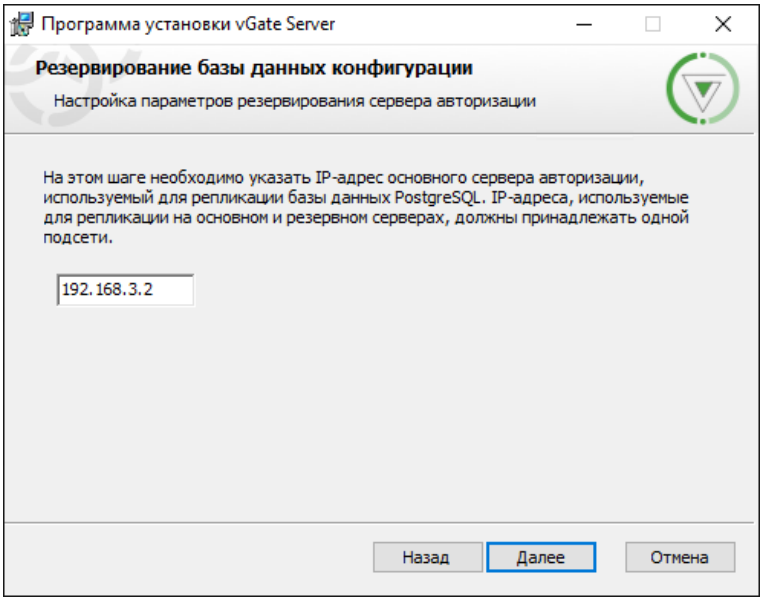
Параметр	Описание
IP-адрес сетевого адаптера во внешней сети администрирования	IP-адрес резервного сервера во внешнем периметре сети администрирования инфраструктуры
IP-адрес сетевого адаптера для защищаемого периметра	IP-адрес резервного сервера в сети администрирования инфраструктуры

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 настройки параметров входа в систему для службы проксирования трафика vGate (vcp.exe).

12. Укажите параметры учетной записи службы проксирования трафика vGate (vcp.exe), которая будет использоваться для подключения к виртуальной инфраструктуре, и нажмите кнопку "Далее".

На экране появится диалог с сообщением о готовности к установке.

13. 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.

14. 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.**61**.

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 ESXi-сервер, 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 ESXi-сервере 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.**16** и стр.**28**).

Примечание. В случае развертывания vGate 4.4 с установкой сервера авторизации на виртуальной машине, для этой ВМ поддерживается использование политики безопасности "Доверенная загрузка виртуальных машин" (см. стр.**118**).

Подготовка сервера виртуализации к установке vGate с резервированием

При использовании маршрутизатора:

1. Создайте на ESXi-сервере виртуальный коммутатор (vSwitch1) с привязкой к физическому сетевому адаптеру (vmnic0), подключенному к физической сети, которая используется как сеть защищаемых серверов.
2. Создайте на виртуальном коммутаторе (vSwitch1) группу портов ВМ (VMNetwork1).
3. Создайте на ESXi-сервере виртуальный коммутатор (vSwitch2) с привязкой к физическому сетевому адаптеру (vmnic1), подключенному к физической сети, которая используется как сеть резервирования.
4. Создайте на виртуальном коммутаторе (vSwitch2) группу портов ВМ (VMNetwork2).
5. Создайте на ESXi-сервере две виртуальные машины (VM1 и VM2) и добавьте каждой из них две ранее созданные группы портов (VMNetwork1 и VMNetwork2).
6. Установите на обе ВМ гостевую операционную систему из списка поддерживаемых сервером авторизации vGate.
7. В гостевых операционных системах ВМ настройте сетевые адаптеры и выполните установку сервера авторизации vGate с резервированием (см. стр.**28**).

При маршрутизации трафика с использованием сервера авторизации:

1. Создайте на ESXi-сервере виртуальный коммутатор (vSwitch1) с привязкой к физическому сетевому адаптеру (vmnic0), подключенному к физической сети, которая используется как сеть администрирования инфраструктуры.
2. Создайте на виртуальном коммутаторе (vSwitch1) группу портов ВМ (VMNetwork1).
3. Создайте на ESXi-сервере виртуальный коммутатор (vSwitch2) с привязкой к физическому сетевому адаптеру (vmnic1), подключенному к физической сети, которая используется как сеть резервирования.
4. Создайте на виртуальном коммутаторе (vSwitch2) группу портов ВМ (VMNetwork2).
5. Создайте на ESXi-сервере 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).
6. Создайте на виртуальном коммутаторе (vSwitch3) группу портов ВМ (VMNetwork3).
7. Создайте две ВМ (VM1, VM2) и добавьте каждой из них три ранее созданные группы портов (VMNetwork1, VMNetwork2 и VMNetwork3).
8. Установите на обе ВМ гостевую операционную систему из списка поддерживаемых сервером авторизации vGate.
9. В гостевых операционных системах ВМ настройте сетевые адаптеры и выполните установку сервера авторизации vGate с резервированием

   (см. стр.**28**).

Установка агента аутентификации на ОС Windows

Внимание! Если на компьютере предполагается использовать компонент "Средство просмотра отчетов", необходимо предварительно установить Microsoft Report Viewer 2010 SP1 Redistributable Package. Для установки запустите с установочного диска из каталога \Redistributables\Microsoft Report Viewer Redistributable 2010 файл ReportViewer.exe и следуйте указаниям мастера установки.

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.**102**).

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.

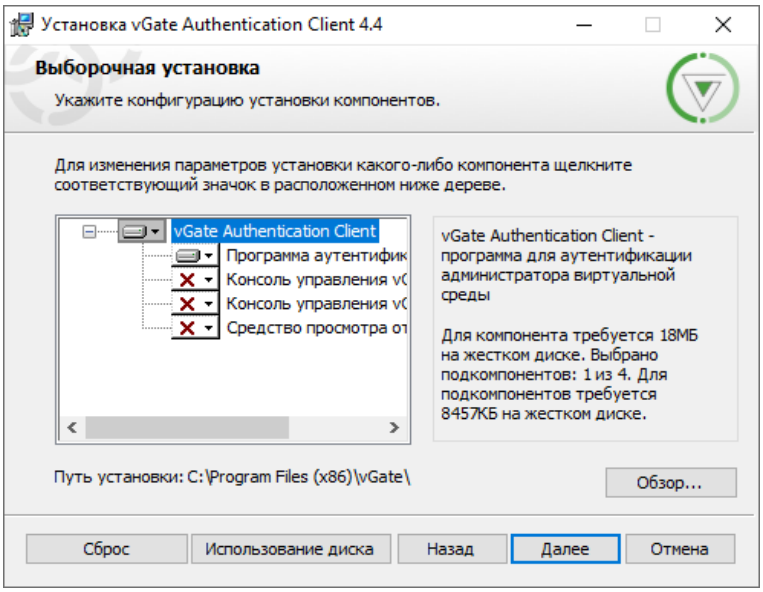
   Программа установки выполнит подготовительные действия и выведет на экран диалог приветствия.
4. Нажмите кнопку "Далее".

   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 и средство просмотра отчетов. Для их установки раскройте дерево компонентов, нажмите мышью на значок слева от названия компонента и в раскрывающемся меню выберите нужный пункт.

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 агента аутентификации на ОС Linux

Установка агента аутентификации на ОС Linux производится с помощью RPM Package Manager.

Внимание! Установку агента аутентификации необходимо запускать от имени администратора. Также нужно разрешить SELinux выполнять скрипты RPM-пакетов с помощью правил SELinux или перевести SELinux в режим работы Permissive, или отключить SELinux на время установки пакетов.

Для установки агента аутентификации введите команду:

```
rpm -iv /tmp/vgclient_4.4.211.std.def.alt0.M80C.1-4.4.4021.0-0.x86_64.rpm
```

Во время установки RPM-пакета будет проверено соответствие версий ядра и дистрибутива версиям, для которых собран пакет.

Если установка RPM-пакета завершилась с ошибкой, необходимо удалить из системы агент аутентификации (см. стр.**60**).

Примечание. Файл конфигурации устанавливается с минимальными параметрами. Например, в нем отсутствуют подключения к серверам авторизации vGate, которые пользователю нужно будет добавить с помощью программы аутентификации (см. раздел "Работа агента аутентификации в ОС Linux" в документе [**4**]).

Установка компонента защиты vCenter Server

Установка компонента защиты сервера vCenter (VMware vSphere 6.5 или 6.7), развернутого на ОС Windows, выполняется во время настройки vGate в консоли управления (см. стр.**98**). При необходимости компонент может быть установлен с помощью программы установки vGate непосредственно на ПК с установленным VMware vCenter.

vGate Standard позволяет осуществлять защиту только одного сервера vCenter. Если в компании эксплуатируются несколько серверов vCenter, объединенных с помощью режима VMware vCenter Linked Mode, необходимо установить компонент защиты vGate на каждый из них. Эта функция доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Если на компьютере, предназначенном для компонента защиты vCenter, эксплуатируется ПО Secret Net Studio, перед началом установки необходимо отключить межсетевой экран Secret Net Studio.

Для установки компонента защиты vCenter:

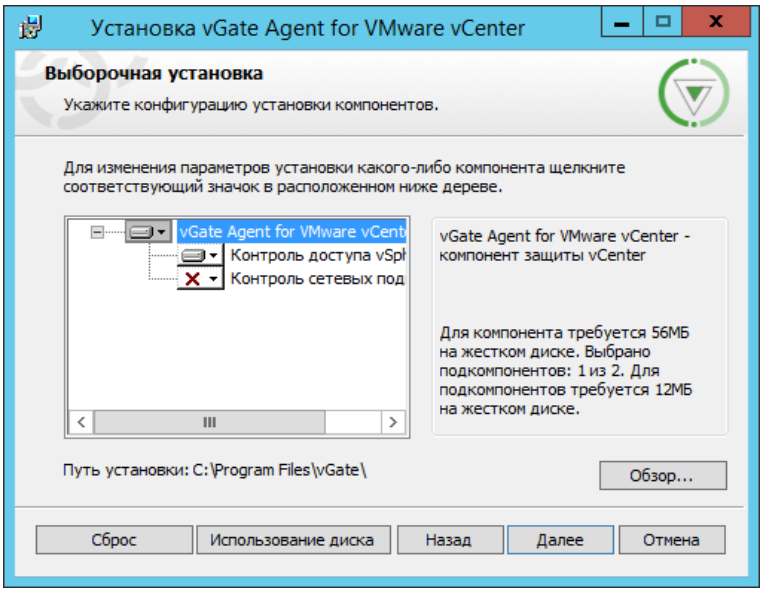
1. Войдите в систему с правами администратора компьютера.
2. Поместите установочный диск в устройство чтения компакт-дисков.
3. Запустите на исполнение файл vGateVpxAgent.msi, находящийся на установочном диске.

   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.

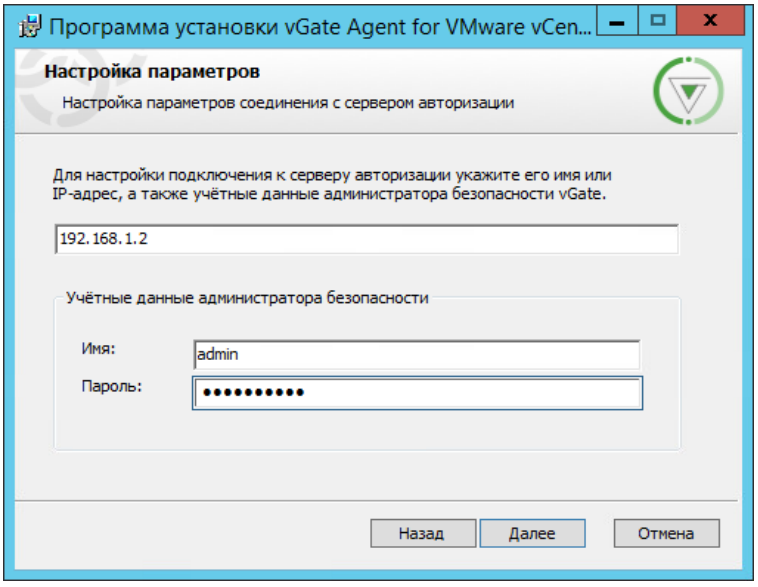


Пояснение. Компонент "Контроль сетевых подключений" по умолчанию не устанавливается. Если компонент выбран для установки, то после установки компонента защиты vCenter на сервере vCenter будут ограничены входящие сетевые соединения. Подробнее о настройке фильтрации соединений с vCenter см. стр.143.

Совет. Чтобы выбрать компонент для установки, нажмите мышью на значок слева от названия компонента и в раскрывшемся меню выберите пункт "Будет установлен на локальный жесткий диск". Для запрета установки компонента нажмите мышью на значок и в раскрывшемся меню выберите пункт "Компонент будет полностью недоступен".

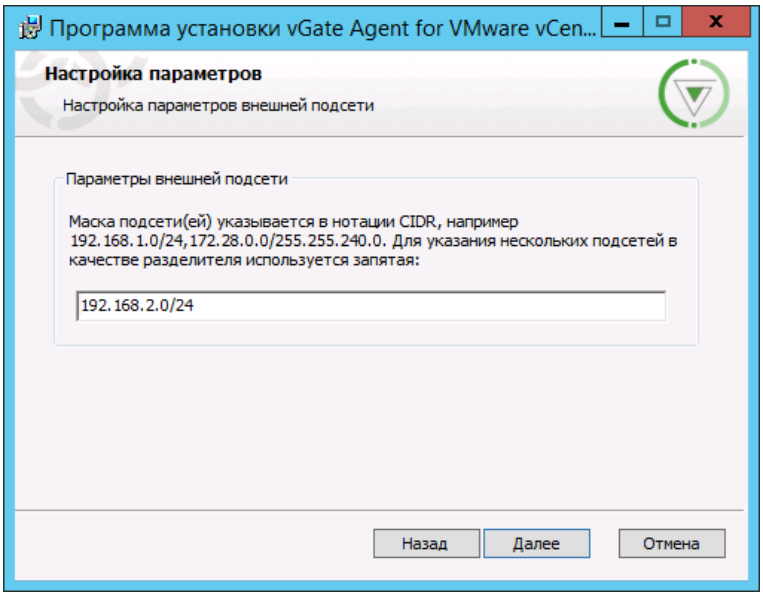
6. При необходимости укажите другую папку для размещения файлов и нажмите кнопку "Далее".

   На экране появится следующий диалог.



7. Укажите имя или IP-адрес сервера авторизации, а также учетные данные администратора информационной безопасности и нажмите кнопку "Далее".

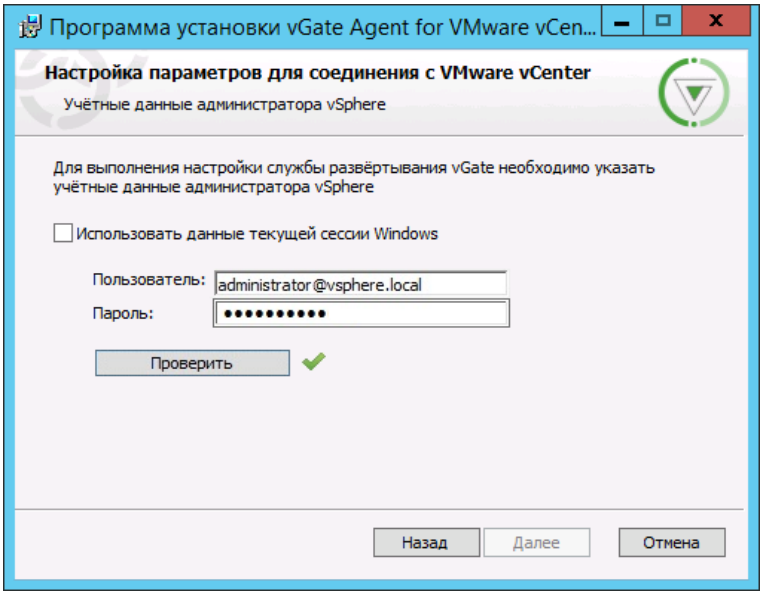
Если на шаге **5** для установки был выбран компонент "Контроль сетевых подключений", на экране появится следующий диалог.



8. Укажите параметры внешней подсети (подсетей) администрирования виртуальной инфраструктуры, в которой расположены рабочие места АИБ и АВИ, и нажмите кнопку "Далее".

Соединение с vCenter будет разрешено только в том случае, если IP-адрес рабочего места администратора соответствует одной из указанных подсетей.

На экране появится следующий диалог.



9. Укажите учетные данные администратора для выполнения настройки службы развертывания vGate и нажмите кнопку "Далее".
   - При выборе системной учетной записи нажмите кнопку "Далее".
   - При выборе учетной записи из домена Windows:
     - укажите имя и пароль учетной записи;
     - нажмите кнопку "Проверить" для проверки параметров учетной записи;

       На экране появится сообщение о результатах проверки. Нажмите кнопку "ОК" в окне сообщения.

     - в случае успешной проверки нажмите кнопку "Далее" для продолжения установки.

   На экране появится диалог с сообщением о готовности к установке.
10. 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.
11. 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 мониторинга

Для работы функции мониторинга безопасности (см. стр.**191**) необходимо развернуть в сети сервер мониторинга.

Для развертывания сервера мониторинга:

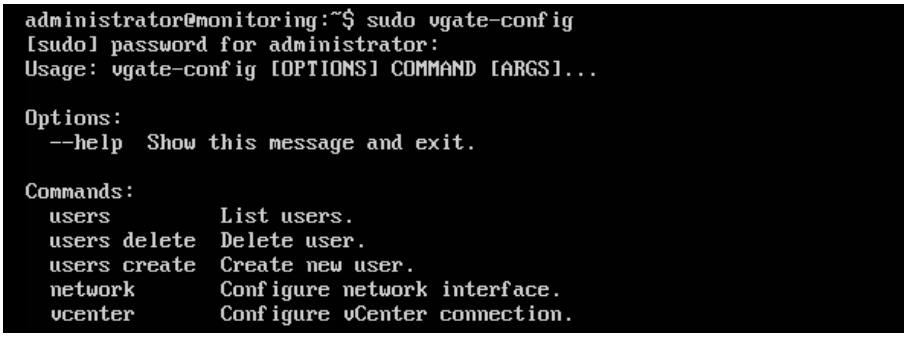
1. В VMware vCenter выполните импорт виртуальной машины из OVF шаблона, расположенного на установочном диске vGate в каталоге \monitoring\Monitoring.ovf.
2. После запуска ВМ введите следующие учетные данные:

   Monitoring login: administrator

   Password: qwe
3. Выполните команду:

```
sudo vgate-config
```

   На экране появится список доступных команд:



4. Для настройки сетевого интерфейса выполните команду:

```
sudo vgate-config network
```

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

```
administrator@monitoring:~$ sudo vgate-config network
Configuring network interface: eth0
IP Address: 192.168.2.150
Netmask: 255.255.255.0
Default gateway: 192.168.2.10
DNS Nameservers []: 192.168.2.2

Network interface has been configured successfully.
```

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

6. При наличии в виртуальной инфраструктуре сервера vCenter настройте подключение сервера мониторинга к нему.

   Для этого выполните команду:

```
sudo vgate-config vcenter
```

```
administrator@monitoring:~$ sudo vgate-config vcenter
vCenter address: 192.168.2.61
Username: administrator@vsphere.local
Password:

vCenter has been configured successfully.
```

Внимание! Для VMware vCenter Server for Windows в консоли управления vGate необходимо создать правило, разрешающее доступ с IP-адреса сервера мониторинга к серверу vCenter. Для корректного сбора сообщений аудита необходимо указать учетные данные АВИ через TCP-порт 443 (см. стр.143). Также необходимо убедиться в том, что vCenter Firewall не блокирует порт 443.

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.**191**).

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.**56**
2	**Экспорт конфигурации vGate**	Экспорт конфигурации vGate версий 4.2 и 4.3 производится в консоли управления vGate	См. стр.**87**
3	**Удаление ПО vGate 4.2 и 4.3**	Выполняется удаление ПО сервера авторизации vGate, агента аутентификации, компонента защиты для vCenter, а также PostgreSQL 9.4 (x86). При использовании функции мониторинга безопасности необходимо выполнить удаление сервера мониторинга	См. стр.**58**
4	**Установка ПО vGate 4.4**	Выполняется установка ПО сервера авторизации vGate, агента аутентификации, компонента защиты для vCenter. При использовании функции мониторинга безопасности необходимо также выполнить установку и настройку сервера мониторинга	См. стр.**12**
5	**Импорт конфигурации vGate**	В консоли управления выполняется импорт конфигурации vGate, полученной на шаге 2	См. стр.**87**

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.**76**).

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.**59**).
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.**76**), 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.**76**).

   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.**236**).

Глава 3
Переустановка и удаление vGate

Программы установки сервера авторизации vGate, агента аутентификации, компонента защиты для vCenter 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:

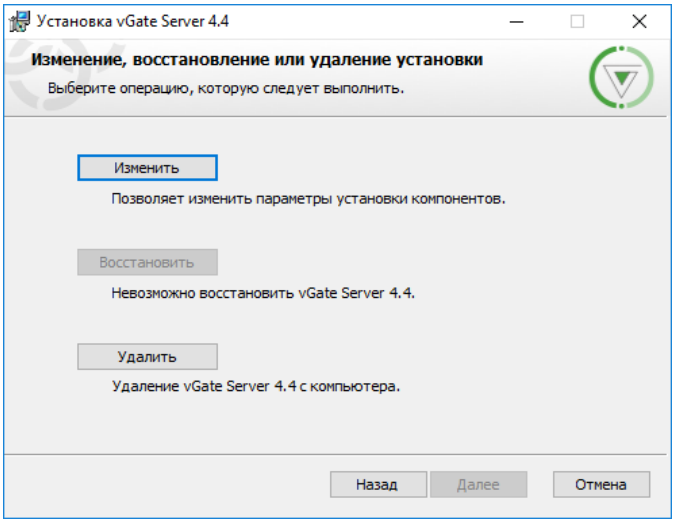
1. Запустите соответствующую программу установки.

   Совет. Это можно сделать двумя способами:
   - Запустите на исполнение файл vGateServer.msi, vGateClient.msi, vGateVpxAgent.msi из каталога \vGate\ на установочном компакт-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 Agent for VMware vCenter 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:

- установить или удалить консоль управления на компьютере, на котором установлен сервер или агент аутентификации;
- добавить или удалить компонент "Резервирование конфигурации" на сервере авторизации;
- установить или удалить компонент "Контроль сетевых подключений" на компьютере, на котором установлен компонент защиты vCenter;
- установить или удалить компонент "Средство просмотра отчетов" на компьютере, где установлен сервер авторизации или агент аутентификации.

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.**59**) 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.**59**) 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.**28**).

Удаление

Внимание!

- Перед удалением сервера авторизации vGate необходимо удалить компоненты защиты со всех ESXi-серверов, а также компоненты защиты vCenter с помощью консоли управления (см. стр.**98**).
- Для удаления компонента защиты vGate с ESXi-сервера версии 7.0 необходимо предварительно выключить виртуальные машины с ОС, исполняемые на этом сервере.
- 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".

Развернутые на ESXi-серверах модули защиты vGate версии 2.4 и выше также можно удалить вручную.

Для удаления компонентов защиты ESXi-серверов вручную:

1. На ESXi-сервере откройте сервисную консоль и выполните команду для вывода на экран номера версии агента vGate:

   ```
   esxcli software vib list | grep sc-vgate-agent
   ```

2. Выполните команду для удаления модулей защиты:

   ```
   esxcli software vib remove –n sc-vgate-agent
   ```

   или

   ```
   esxcli software vib remove --vibname=sc-vgate-agent
   ```

Удаление агента аутентификации на ОС Linux

Удаление агента аутентификации на ОС Linux производится с помощью RPM Package Manager.

Внимание! Удаление агента аутентификации необходимо запускать от имени администратора. Также нужно разрешить SELinux выполнять скрипты RPM-пакетов с помощью правил SELinux или перевести SELinux в режим работы Permissive, или отключить SELinux на время удаления пакетов.

Для удаления агента аутентификации выполните команду:

```
rpm -ev vgclient_4.4.211.std.def.alt0.M80C.1-4.4.4021.0-
0.x86_64.rpm
```

При удалении программного обеспечения удаляются бинарные файлы и файлы конфигурации. Лог-файлы и конфигурационный файл службы аутентификации vGate (aupa.exe) не будут удалены.

Чтобы просмотреть информацию об установленном ПО, выполните команду:

```
rpm -qa vgclient*
```

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.**35** или стр.**45** (в зависимости от выбранного способа маршрутизации трафика)
3.	**Настройка правил фильтрации сетевых подключений к vCenter**	Выполняется в консоли управления или с помощью утилиты drvmgr	См. стр.**62**

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.**29** (при использовании стороннего маршрутизатора) или на стр.**38** (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.**35** (при использовании маршрутизатора) или на стр.**45** (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.**49**.

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 ESXi-серверами и vCenter 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 ESXi-серверами и vCenter 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.

Настройка правил фильтрации сетевых подключений к vCenter

Если при установке компонента защиты vCenter был выбран пункт "Контроль сетевых подключений", то доступ к vCenter будет разрешен только с основного IP-адреса защищаемого периметра сервера авторизации. Для корректной работы функции резервирования сервера авторизации, где используются два IP-адреса защищаемого периметра, необходимо добавить правила доступа для дополнительного IP-адреса основного сервера авторизации, а также для IP-адреса защищаемого периметра резервного сервера авторизации.

Эти правила доступа можно настроить в консоли управления или с помощью утилиты drvmgr. Подробнее о настройке правил доступа для vCenter и формате утилиты drvmgr см. стр.**143** и стр.**238**.

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.**76**).

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.**76**). 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.**76**) 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.**28**).

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, vcp.exe, vgate.webapp на основном сервере не работает.
2. После заданного количества неудачных попыток соединения со службами (см. стр.**76**) 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.**62**).

Передача управления резервному серверу авторизации

1. Отключите питание на основном сервере.
2. Запустите консоль управления vGate на резервном сервере от имени администратора (см. стр.**67**), перейдите в раздел "Конфигурация", откройте группу параметров "Сервер авторизации" и нажмите кнопку-ссылку "Назначить основным". В появившемся окне нажмите кнопку "Сменить роль".

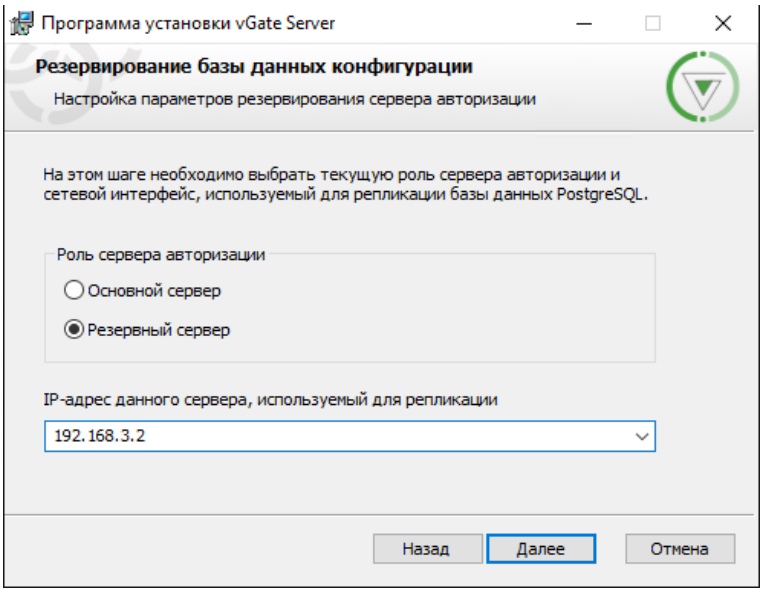
   Резервному серверу будет назначен основной IP-адрес основного сервера (192.168.1.2), а его собственный IP-адрес (192.168.1.22) станет дополнительным.
3. В DNS измените настройки псевдонима, настроив ссылку на полное доменное имя (FQDN) резервного сервера.
4. Если маршрутизацию трафика выполняют серверы 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.**29** или стр.**38** 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.**35** или стр.**45** 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.**28**).

Переустановка основного сервера авторизации

Для переустановки основного сервера авторизации рекомендуется выполнить те же действия, что при замене основного сервера при сбое (см. стр.**64**).

Глава 5
Настройка конфигурации

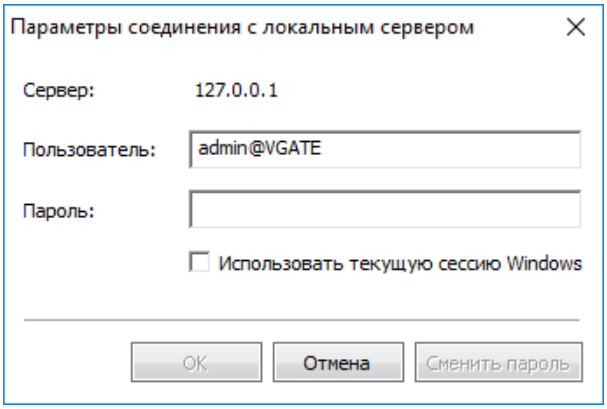
Консоль управления

Для запуска консоли управления:

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

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

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	Сетевое 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)

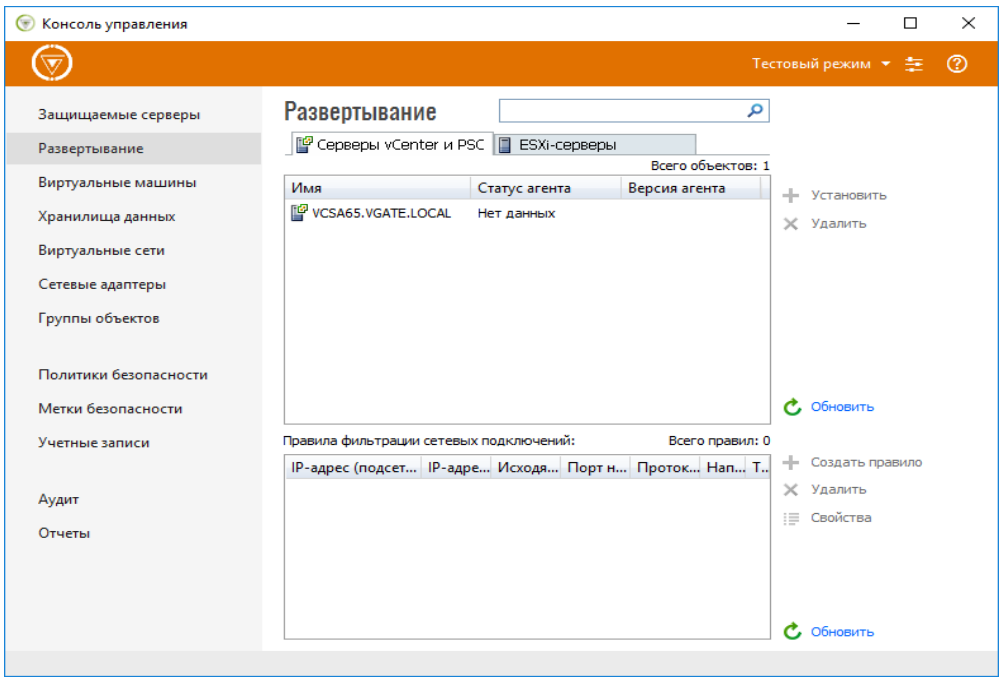
Совет. Для изменения пароля АИБ нажмите кнопку "Сменить пароль".

На экране появится консоль управления vGate.

Примечание. Во время первого запуска консоли управления на экране появится мастер первоначальной настройки (см. стр. 68). После завершения работы мастера откроется окно консоли управления для установки агентов на серверы vCenter.

Окно консоли управления имеет три рабочие области:

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

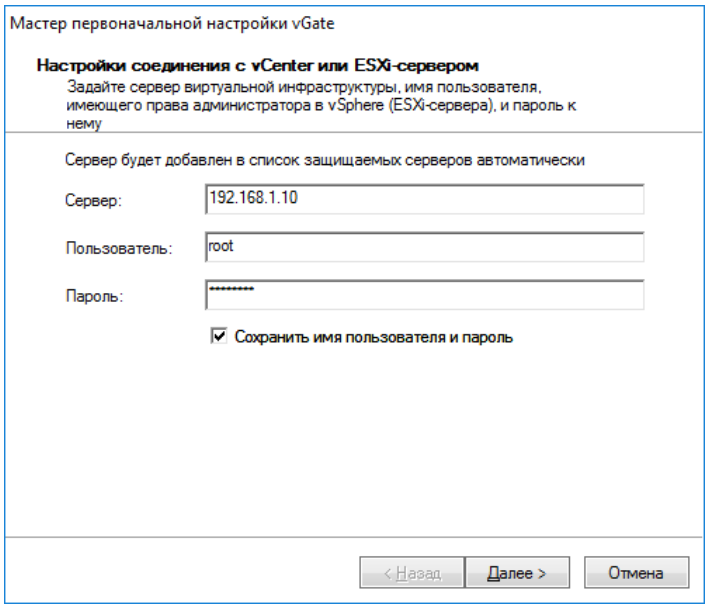


В области параметров отображаются объекты, связанные с выбранной функцией. Для выполнения доступных операций в правой части области параметров находятся кнопки-ссылки. Для поиска объектов по названию в верхней части окна располагается форма поиска.

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.72).

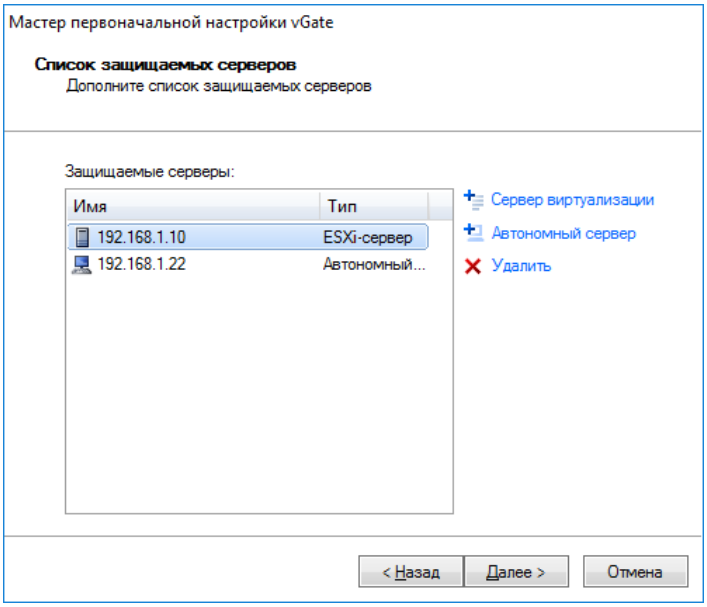
Для первоначальной настройки vGate:

1. Укажите сетевое имя либо IP-адрес сервера ESXi или vCenter, а также имя и пароль администратора для данного сервера и нажмите кнопку "Далее".

   Примечание. Поле "Сохранить имя пользователя и пароль" отмечено по умолчанию. Сохраненные параметры соединения с сервером ESXi или vCenter будут использоваться в дальнейшем при запуске консоли управления текущим пользователем на данном компьютере. Если поле не отмечено, параметры соединения будут использованы только в рамках текущей сессии работы в консоли управления, а некоторые операции в виртуальной инфраструктуре не будут контролироваться vGate (подробнее см. стр.77).

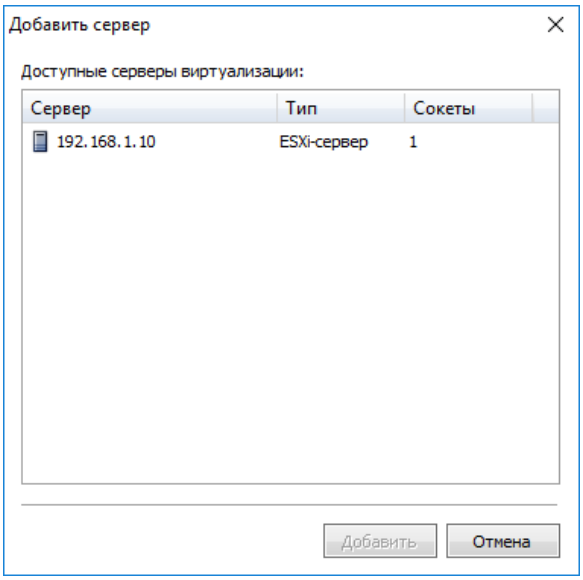
   Указанный сервер будет добавлен в список защищаемых серверов автоматически.

   На экране появится диалог выбора защищаемых серверов.



2. Чтобы добавить сервер vCenter, все относящиеся к нему ESXi-серверы и сервер Platform Services Controller (VMware vSphere 6.7) в список защищаемых серверов, нажмите кнопку-ссылку "Сервер виртуализации".

На экране появится диалог добавления серверов.



Пояснение. В зависимости от заданных параметров соединения (см. стр.77) список будет содержать либо один сервер виртуализации, либо сервер vCenter и все управляемые им серверы виртуализации. Для выбора нескольких элементов используйте клавиши <Shift> и <Ctrl>.

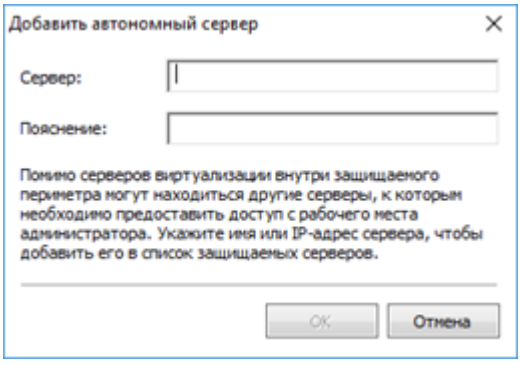
3. Выберите защищаемые серверы и нажмите кнопку "Добавить".

Примечание. Если в компании эксплуатируются несколько серверов vCenter, объединенных с помощью режима VMware vCenter Linked Mode, то после добавления одного из серверов в список защищаемых объектов все связанные с ним серверы будут отображаться в списке доступных серверов виртуализации. Если объединение серверов не используется, то для защиты периметра каждого сервера vCenter необходимо развернуть отдельный сервер авторизации и соответствующим образом его настроить.

Помимо ESXi и vCenter защищаемыми серверами могут быть и другие элементы виртуальной инфраструктуры, имеющие сетевой IP-адрес и находящиеся в защищаемом периметре сети администрирования (например, СХД, DNS, AD). Их также необходимо добавить в список защищаемых серверов.

4. Нажмите кнопку-ссылку "Автономный сервер".

На экране появится следующий диалог.

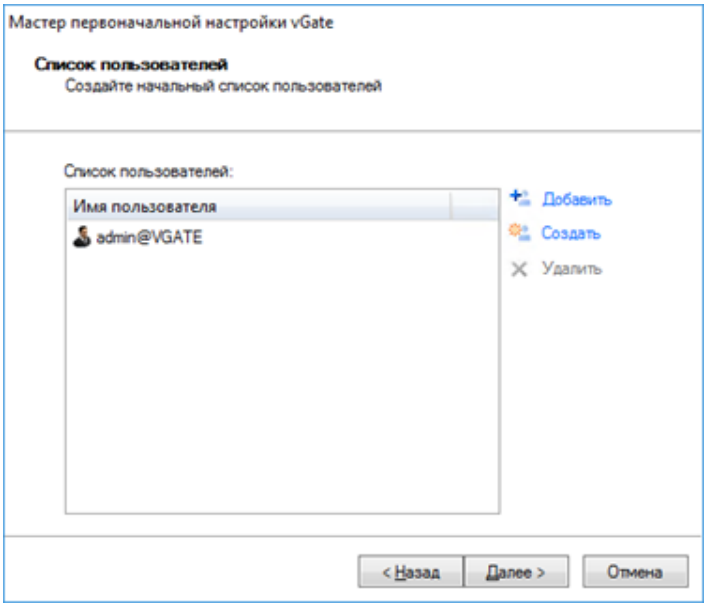


5. Укажите сетевое имя или IP-адрес сервера, при необходимости введите комментарий и нажмите кнопку "OK".

В списке защищаемых серверов появятся новые записи.

6. Нажмите кнопку "Далее".

   На экране появится диалог добавления учетных записей пользователей.

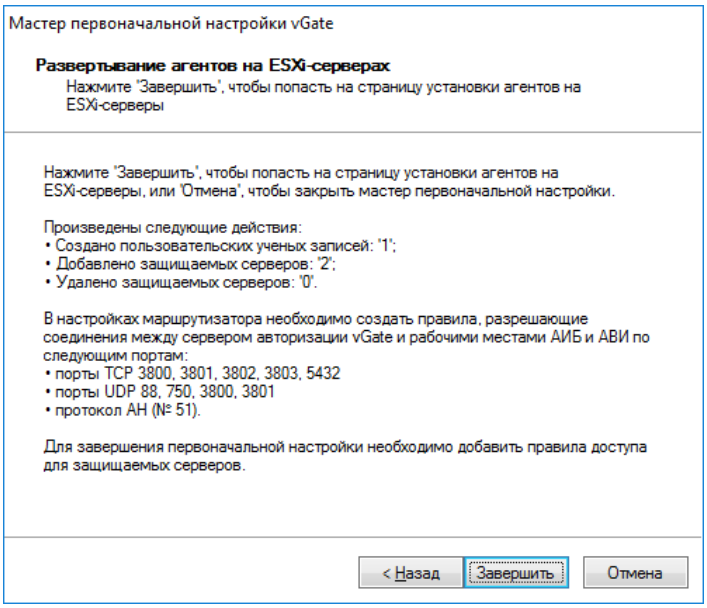


   По умолчанию список пользователей уже содержит учетную запись главного АИБ (см. стр.**102**).

7. Чтобы добавить пользователя из Active Directory, нажмите кнопку-ссылку "Добавить" и зарегистрируйте существующую учетную запись (см. стр.**102**). Для создания нового пользователя нажмите кнопку-ссылку "Создать" (см. стр.**104**).

8. Нажмите кнопку "Далее".

   На последнем шаге мастер отобразит сведения о совершенных действиях.

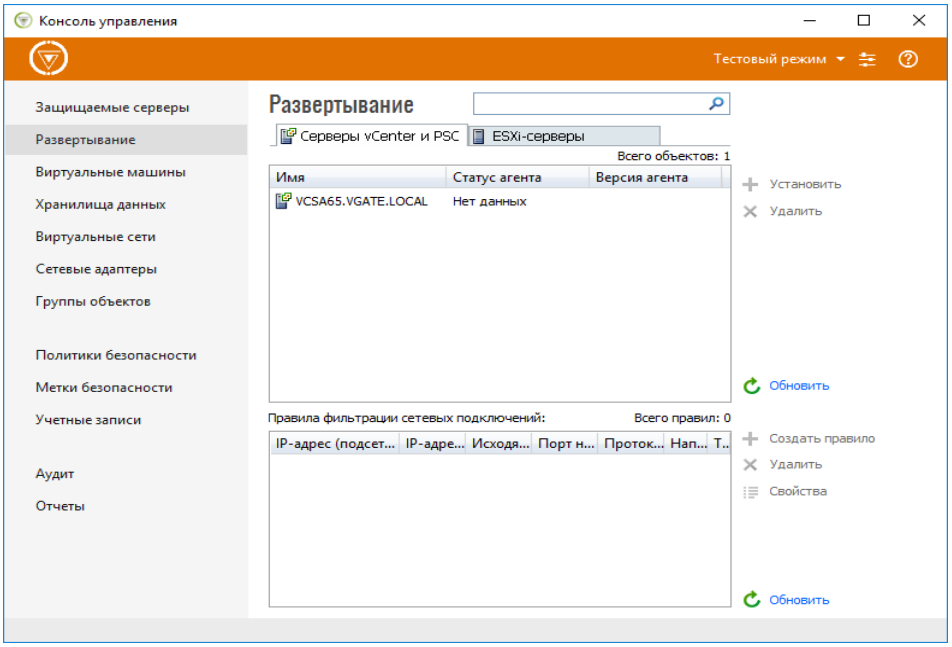


Если при установке vGate был выбран способ маршрутизации трафика с помощью существующего маршрутизатора в сети, то на последнем шаге мастер также отобразит напоминание о необходимости настройки маршрутизатора. В настройках маршрутизатора следует создать разрешающие правила для соединения между сервером авторизации и рабочими местами АИБ и АВИ по следующим портам:

- порты TCP 3800, 3801, 3802, 3803, 5432;
- порты UDP 88, 750, 3800, 3801;
- протокол AH (№ 51).

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

   На экране появится окно установки агентов на серверы vCenter.



Общий порядок настройки

Порядок настройки vGate для конфигурации с сервером vCenter и без него имеет некоторые отличия.

Если первоначальная настройка конфигурации не была выполнена с помощью мастера, выполните ее самостоятельно (действия **1–3**).

План настройки для конфигурации с vCenter

1. Нажмите кнопку  в области главного меню консоли управления и зарегистрируйте имеющуюся лицензию на использование vGate для защиты ESXi-серверов (см. стр.**73**).
2. Нажмите кнопку  и настройте параметры соединения с сервером vCenter (см. стр.**77**).

   Пояснение. После этого все ВМ, относящиеся к данному vCenter, появятся в списке защищаемых ВМ.

3. Выберите функцию "Защищаемые серверы". Добавьте в список защищаемых серверов vCenter, все относящиеся к нему ESXi-серверы и сервер Platform Services Controller (VMware vSphere 6.7). Для этого используйте кнопку "Сервер виртуализации" (см. стр.**97**).

   Примечание. Если в сети администрирования виртуальной инфраструктуры кроме серверов ESXi и vCenter 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".

4. Выберите функцию "Развертывание" и установите на всех добавленных серверах vCenter и ESXi компоненты защиты vGate (см. стр.**98**).
5. 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.**102**).

6. Выберите функцию "Защищаемые серверы" и настройте для каждого пользователя необходимые правила доступа к компонентам управления виртуальной инфраструктурой (см. стр.**96** и стр.**111**).

Внимание! После предоставления пользователям доступа к защищаемым серверам необходимо перевести vGate из тестового в штатный режим работы (см. стр.**93**).

7. Настройте остальные функции при необходимости.

Примечание. Если в компании эксплуатируются несколько серверов vCenter, объединенных с помощью режима VMware vCenter Linked Mode, то после добавления одного из серверов в список защищаемых объектов все связанные с ним серверы будут отображаться в списке доступных серверов виртуализации. Если объединение серверов не используется, то для защиты периметра каждого сервера vCenter необходимо развернуть отдельный сервер авторизации и соответствующим образом его настроить.

План настройки для конфигурации без vCenter

1. Нажмите кнопку  в области главного меню консоли управления и зарегистрируйте имеющуюся лицензию на использование vGate для защиты ESXi-серверов (см. стр.**73**).
2. Нажмите кнопку  в области главного меню. Если для соединения с защищаемыми серверами используется общая учетная запись, настройте параметры соединения с ESXi-сервером (см. стр.**77**).
3. Выберите функцию "Защищаемые серверы" и добавьте данный ESXi-сервер в список защищаемых серверов. Для этого используйте кнопку "Сервер виртуализации" (см. стр.**97**).

   Пояснение. Список найденных при обзоре ESXi-серверов будет содержать только один сервер, параметры соединения с которым заданы при выполнении действия **2**.

   Примечание. Если в сети администрирования виртуальной инфраструктуры кроме серверов ESXi 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".
4. Выберите функцию "Развертывание" и установите на данном ESXi-сервере компонент защиты vGate (см. стр.**100**).
5. Повторите действия **2**–**4** для всех защищаемых ESXi-серверов.

   Пояснение. В дальнейшем настройка параметров соединения с ESXi-сервером потребуется только для пересчета контрольных сумм ВМ, размещенных на данном ESXi-сервере.
6. 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.**102**).
7. Выберите функцию "Защищаемые серверы" и настройте для каждого пользователя необходимые правила доступа к компонентам управления виртуальной инфраструктурой (см. стр.**137**).

Внимание! После предоставления пользователям доступа к защищаемым серверам необходимо перевести vGate из тестового в штатный режим работы (см. стр.**93**).

8. Настройте остальные функции при необходимости.

Регистрация лицензии

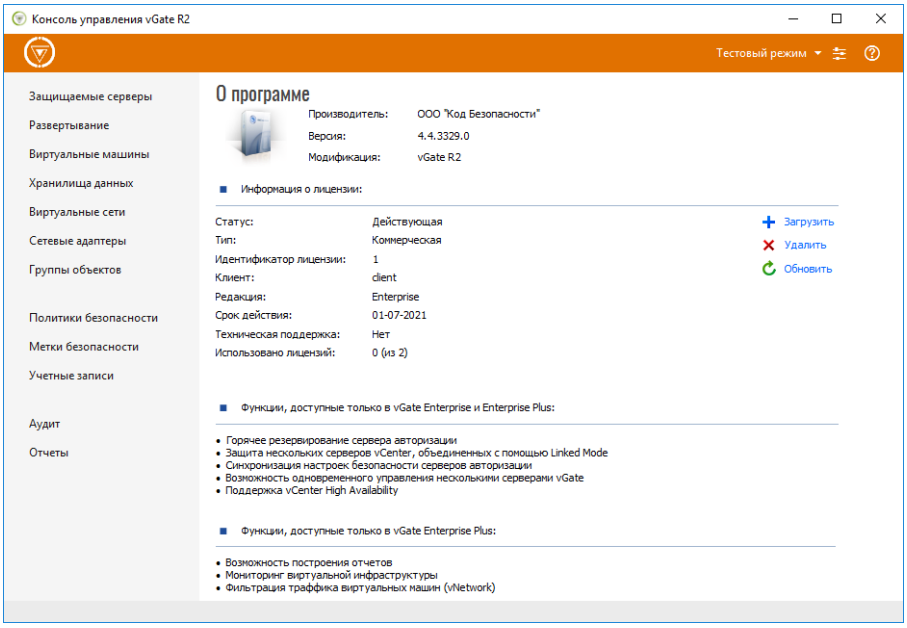
Для ознакомления с ПО vGate в демонстрационном режиме необходим ключ активации (см. раздел "Правила использования лицензий" в документе [1]). Демонстрационный режим работы vGate поддерживает выполнение всех функций, доступных в редакции Enterprise Plus (см. раздел "Функциональные возможности" в документе [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.

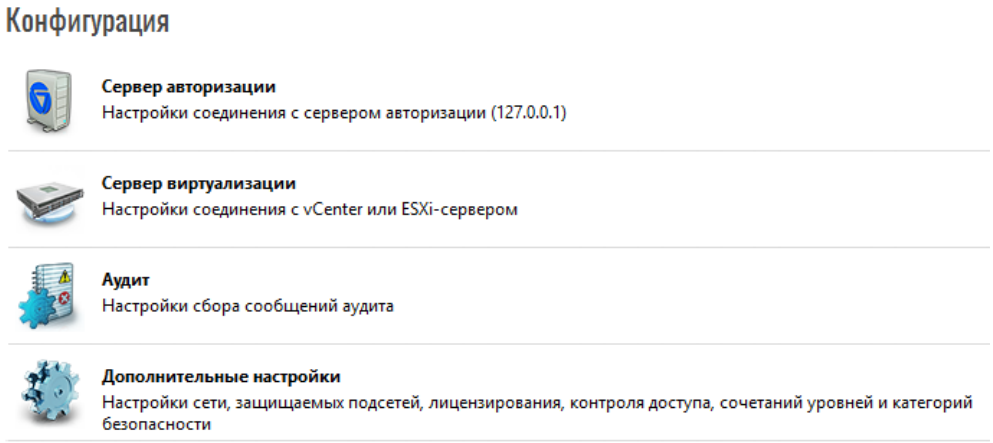
Примечание. Чтобы обновить информацию о лицензии, нажмите кнопку-ссылку "Обновить". Для удаления лицензионного ключа используется кнопка-ссылка "Удалить".

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.**59**).

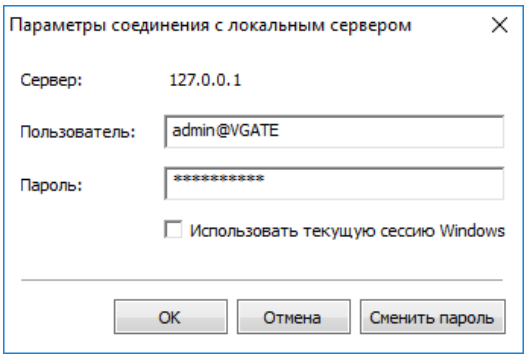
Повторное подключение к серверу авторизации

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.

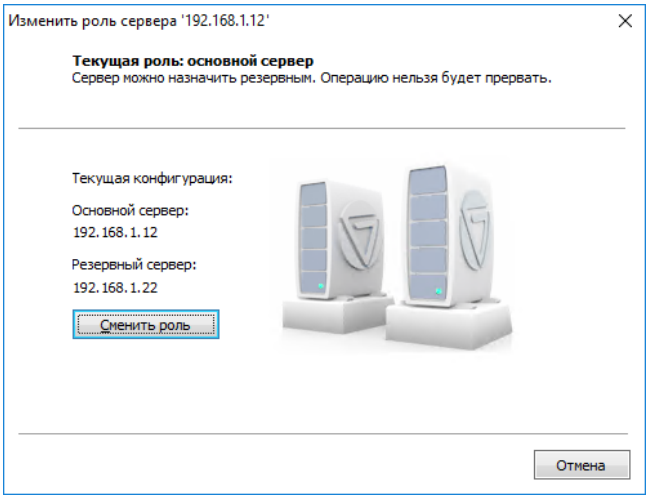
Функция резервирования сервера авторизации доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

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.**61**).

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]).

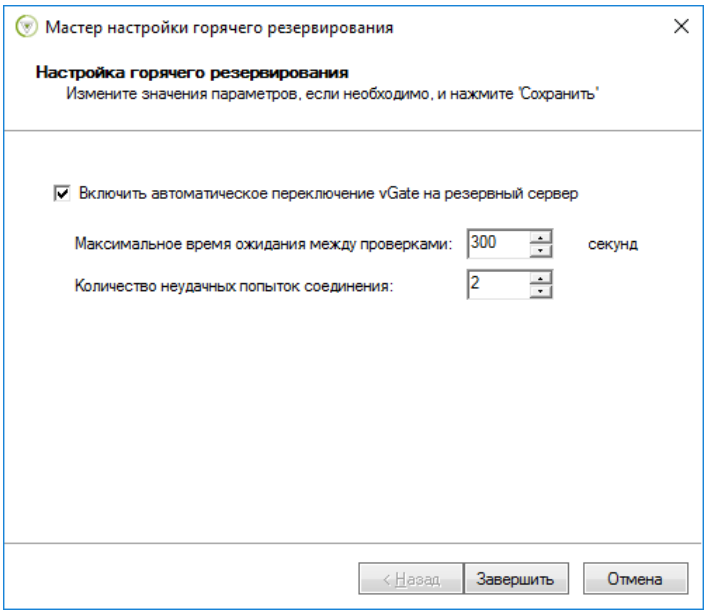
Внимание! Для доступа к функции горячего резервирования необходимо ввести в эксплуатацию резервный сервер авторизации (см. стр.**61**).

Внимание! Если на защищаемые серверы vCenter установлен компонент vGate "Контроль сетевых подключений", то для корректной работы функции автоматического переключения на резервный сервер авторизации необходимо добавить правила доступа, разрешающие подключение с IP-адреса резервного сервера к серверам vCenter по протоколу TCP и любому порту (см. стр.**143**).

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 vCenter или ESXi-сервером

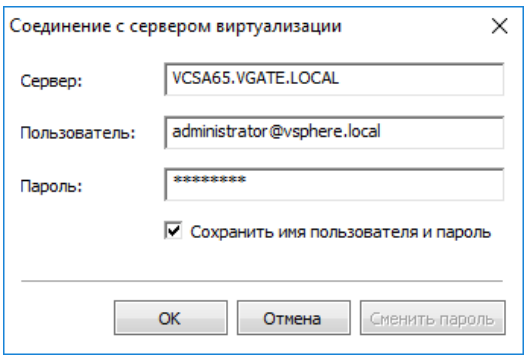
В зависимости от конфигурации виртуальной инфраструктуры необходимо использовать различные варианты соединения:

- Если для управления виртуальной инфраструктурой используется vCenter, то указываются параметры соединения с ним.
- Если в виртуальной инфраструктуре отсутствует vCenter и при этом используются несколько ESXi-серверов, то указываются параметры соединения с одним из них. В этом случае только подключенный ESXi-сервер будет виден в списке "Добавить ESXi-серверы" при регистрации защищаемых серверов. Для настройки vGate потребуется последовательно для каждого из защищаемых ESXi-серверов выполнить соединение с ним и добавить его в список защищаемых серверов (см. стр. **73**, план настройки для конфигурации без vCenter). В дальнейшем последовательное подключение к ESXi-серверам потребуется только для пересчета контрольных сумм ВМ и шаблонов ВМ, размещенных на данном ESXi-сервере. Для управления правами доступа пользователей этого не потребуется.

Для изменения параметров соединения:

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

   На экране появится диалог изменения параметров соединения.



3. Укажите сетевое имя или IP-адрес сервера ESXi или vCenter, а также имя и пароль администратора данного сервера ESXi или vCenter.

   Внимание! При указании параметров соединения с сервером vCenter используйте данные учетной записи администратора vSphere.

   Примечание. Поле "Сохранить имя пользователя и пароль" отмечено по умолчанию. Сохраненные параметры соединения с сервером ESXi или vCenter будут использоваться в дальнейшем при запуске консоли управления текущим пользователем на данном компьютере. Если поле не отмечено, параметры соединения будут использованы только в рамках текущей сессии работы в консоли управления, а некоторые операции в виртуальной инфраструктуре не будут контролироваться vGate.

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

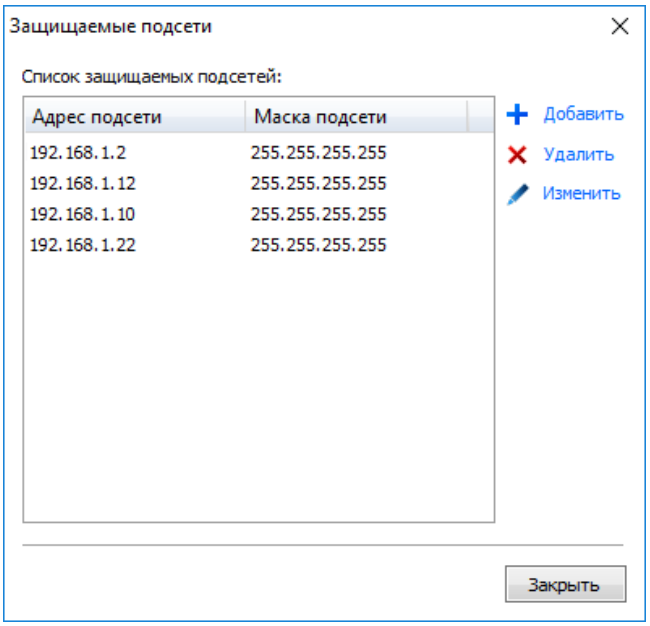
Добавление защищаемых подсетей

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:

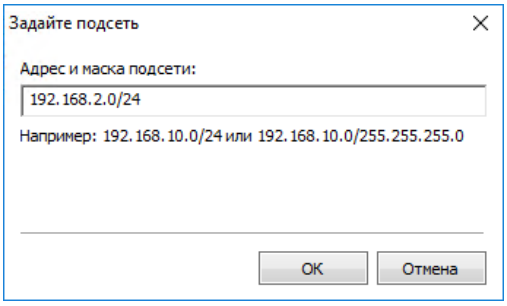
1. В разделе "Конфигурация" откройте группу параметров "Дополнительные настройки".
2. В области параметров нажмите кнопку-ссылку "Защищаемые подсети".

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".

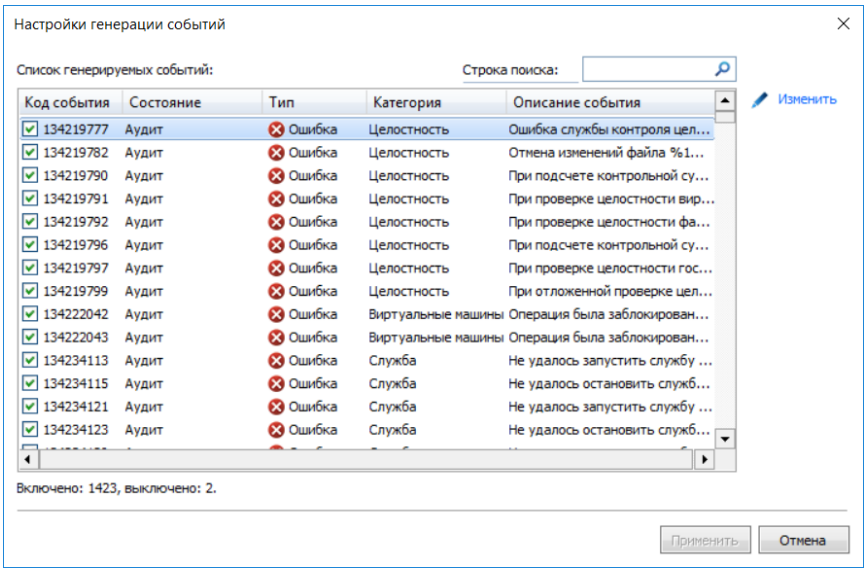
Настройка аудита событий

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".

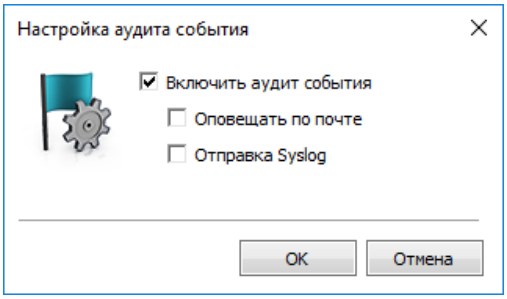
На экране появится следующий диалог.



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.**81**
Отправка Syslog	Включение отправки выбранного сообщения аудита на сервер Syslog

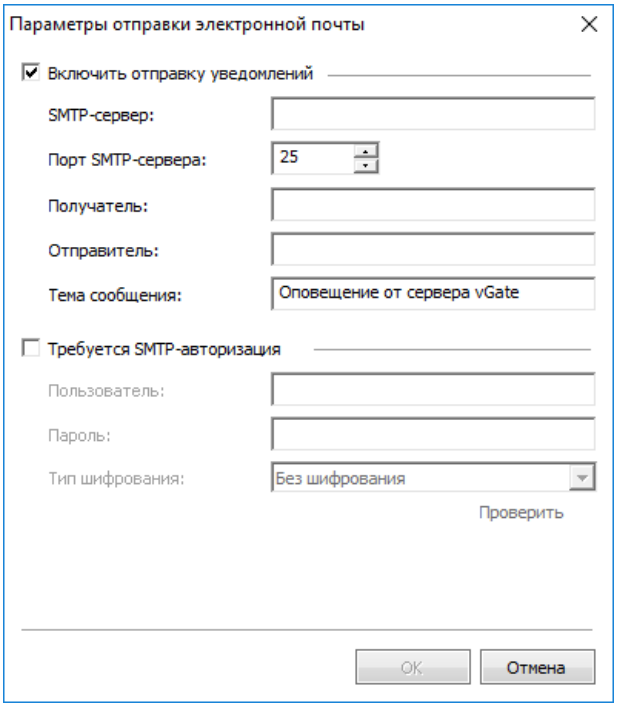
Настройка отправки уведомлений о событиях по SMTP

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".

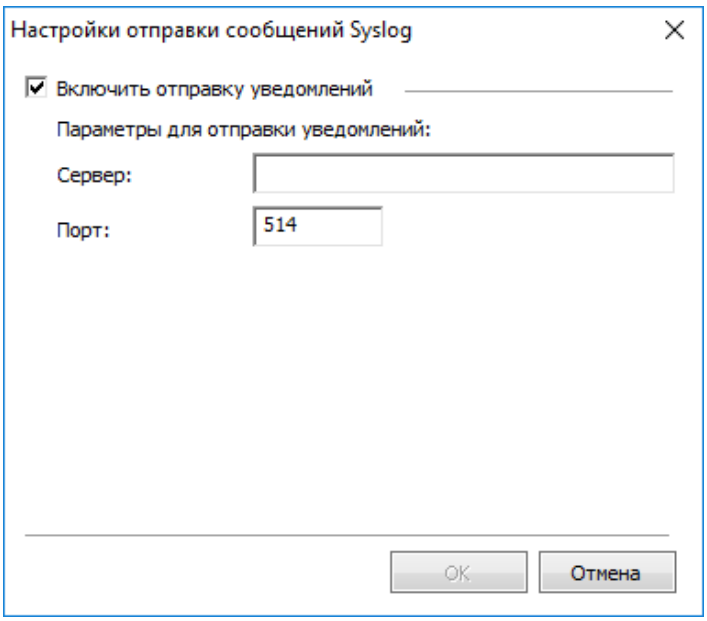
Настройка отправки уведомлений о событиях по протоколу Syslog

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

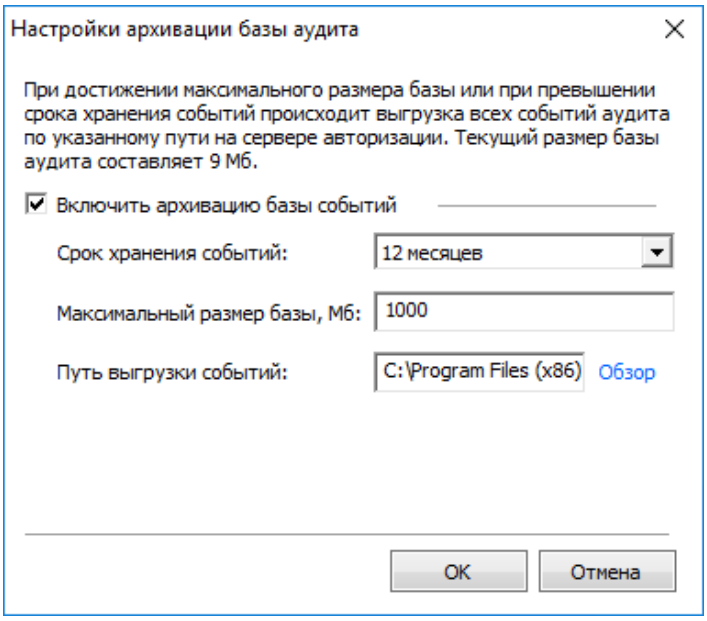
Настройка архивации базы аудита

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

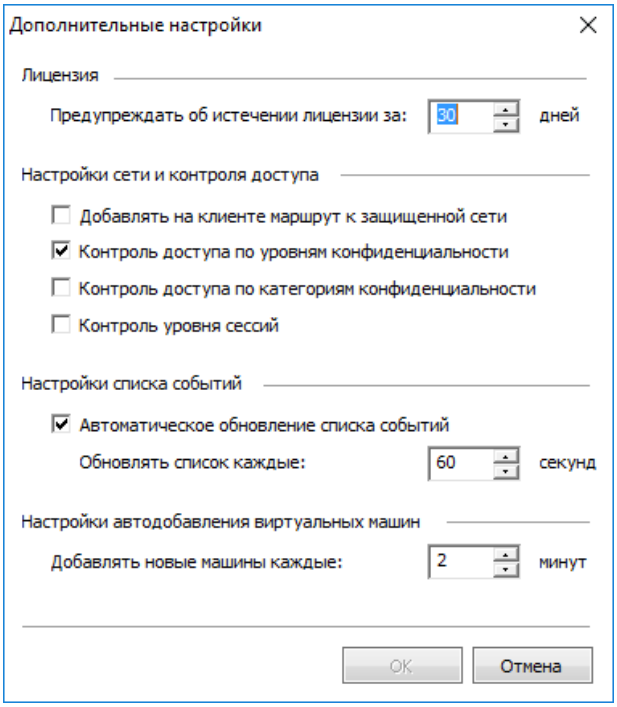
Изменение периода предупреждения об истечении лицензии

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.**13**.

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.**144**). 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.**225**.

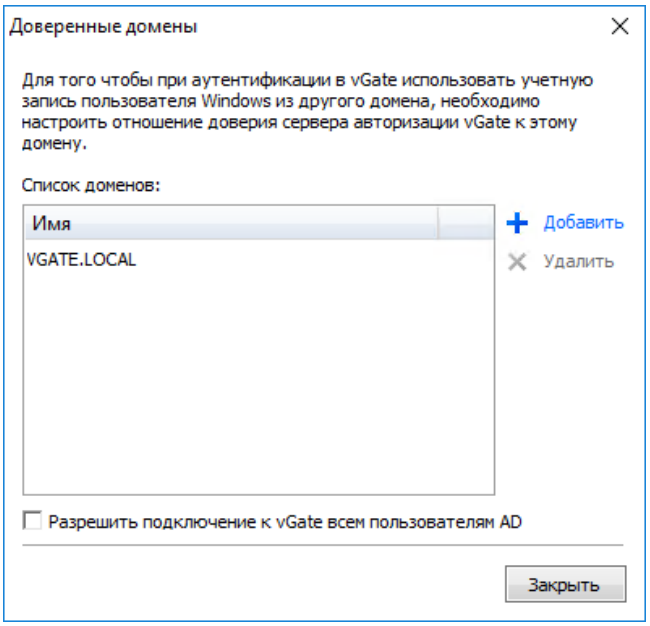
Добавление доверенных доменов

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".

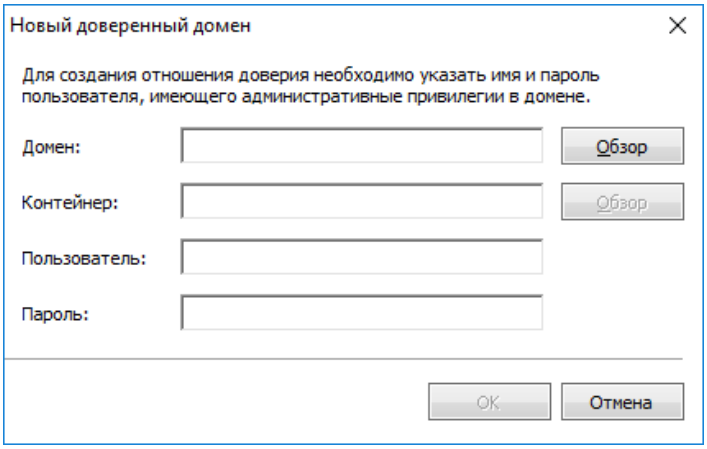
На экране появится диалог для добавления и удаления доверенных доменов.



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".

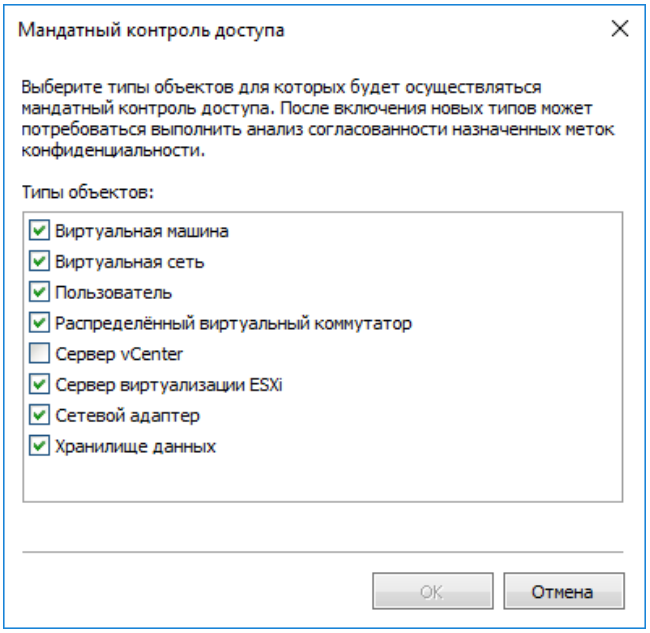
Настройка полномочного управления доступом по типам объектов

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 (ESXi-серверов и vCenter), 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 при одновременном выполнении следующих условий:

- консоль управления запущена с использованием данных учетной записи главного АИБ;
- в параметрах соединения с сервером виртуализации (см. стр.77) указаны данные учетной записи администратора vSphere (или администратора ESXi-сервера при использовании конфигурации без vCenter).

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.

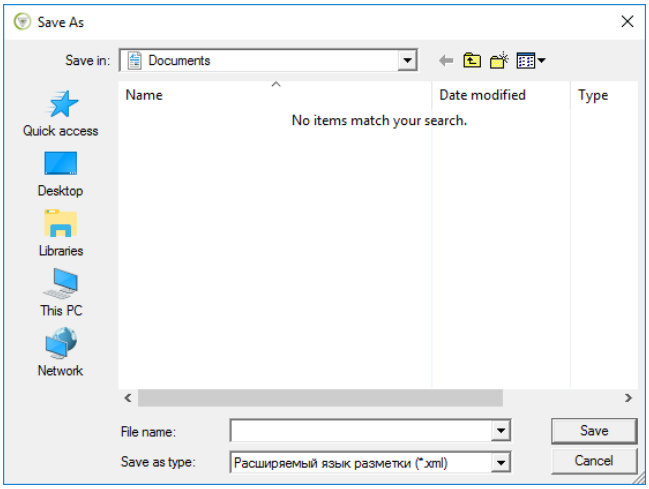
Файл конфигурации содержит информацию о следующих объектах:

- общая информация о системе (версия vGate, режим работы);
- настроенные наборы политик безопасности;
- настроенные уровни и категории конфиденциальности;
- настройки сегментирования;
- 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) 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 отчетов);
- 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.

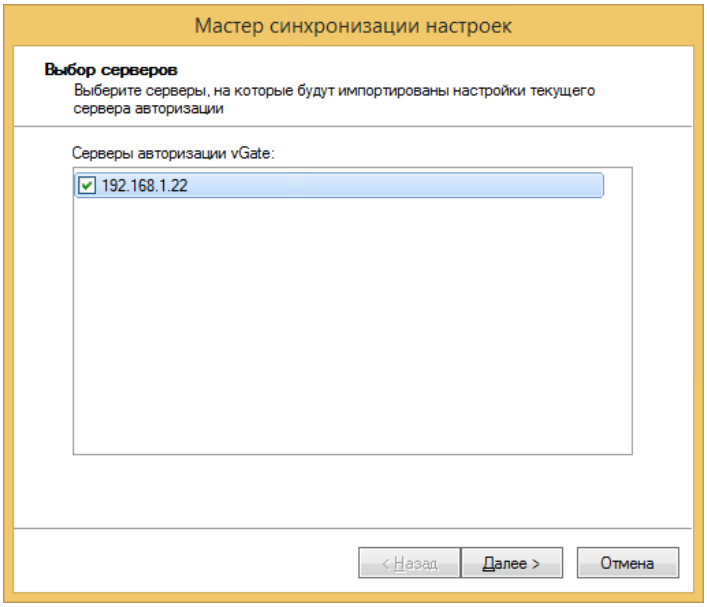
При запуске мастера синхронизации настроек выполняется проверка параметров лицензий на серверах авторизации, к которым подключен агент аутентификации. Для корректной работы мастера необходимо выполнение следующих условий:

- 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.

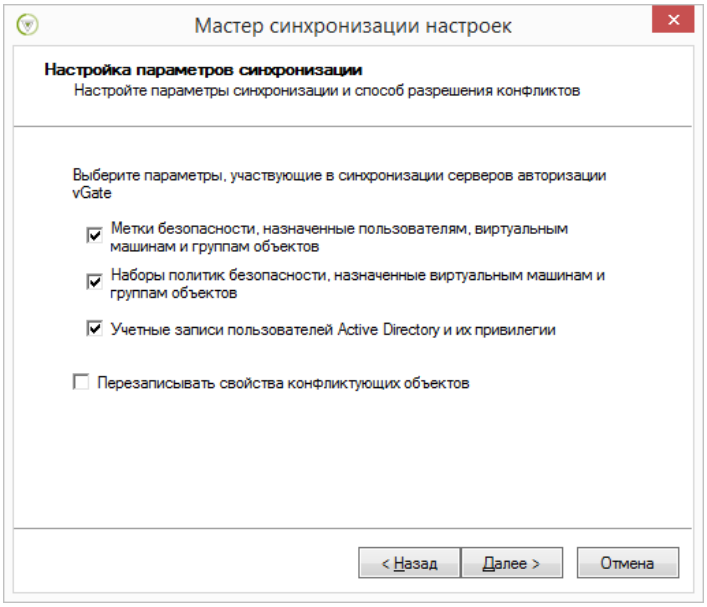


В списке серверов авторизации vGate находятся те серверы, к которым выполнено подключение агента аутентификации.

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.



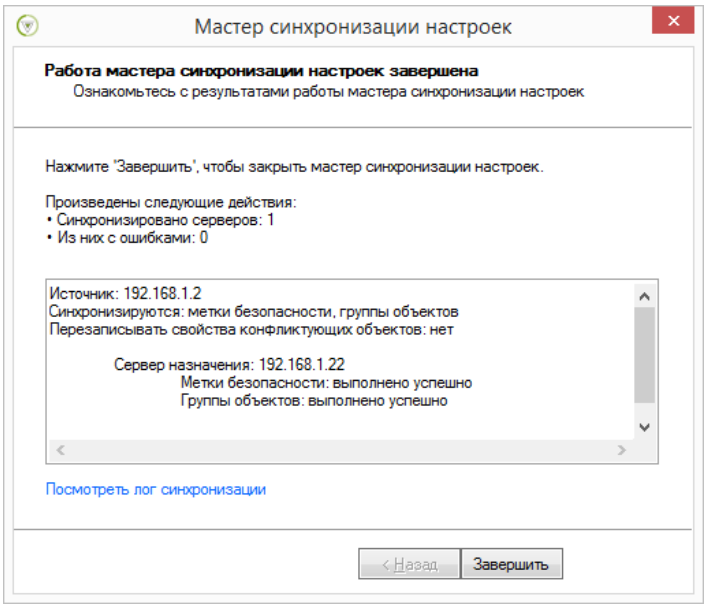
4. Укажите настройки, которые необходимо импортировать на выбранные серверы авторизации, и нажмите "Далее".

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"; • "Контроль целостности шаблонов виртуальных машин"; • "Синхронизация времени"; • "Настроить централизованное хранилище для сбора дампов памяти ESXi-сервера с помощью ESXi Dump Collector"; • "Контроль за доступом через VMSafe CPU/Mem API"; • "Запрет доступа к VMSafe Network API"; • "Отсылка событий сервера виртуализации на syslog-сервер"; • "Проверка настроек SNMP-агента"; • "Настройка брандмауэра ESXi-сервера для ограничения доступа к службам, работающим на сервере"; • "Настройка постоянного журналирования на ESXi-сервере". 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
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.84).

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.**95**). 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.238).

- 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.

Внимание! Если в инфраструктуре присутствует сервер vCenter с установленным компонентом защиты vGate, при переключении режима требуется, чтобы настройки подключения к серверу виртуализации были сохранены (см. стр.77).

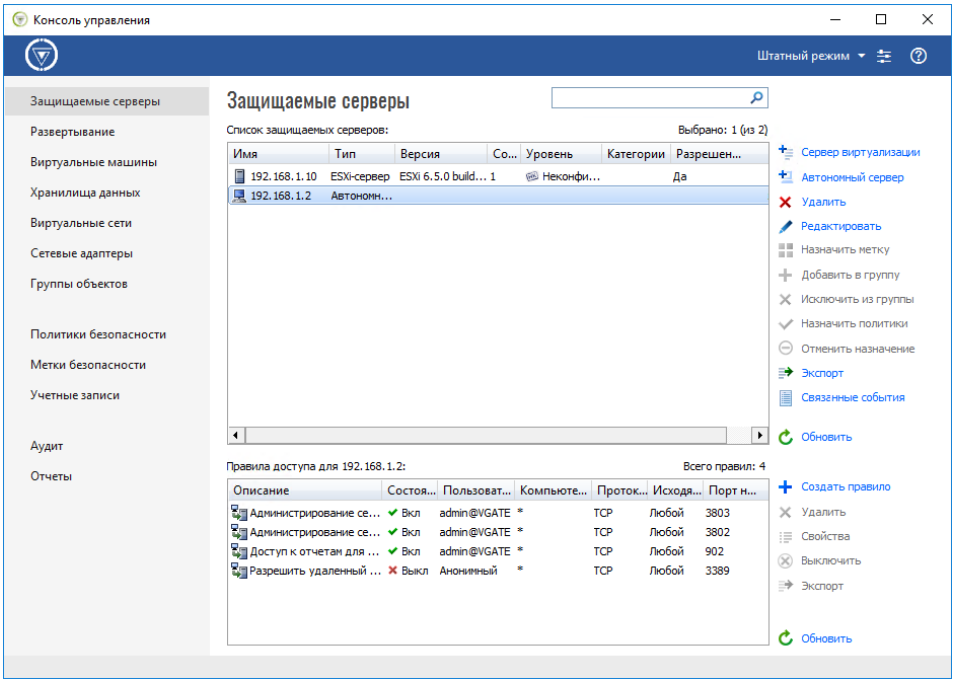
Для переключения vGate в штатный режим:

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.**137**).

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.

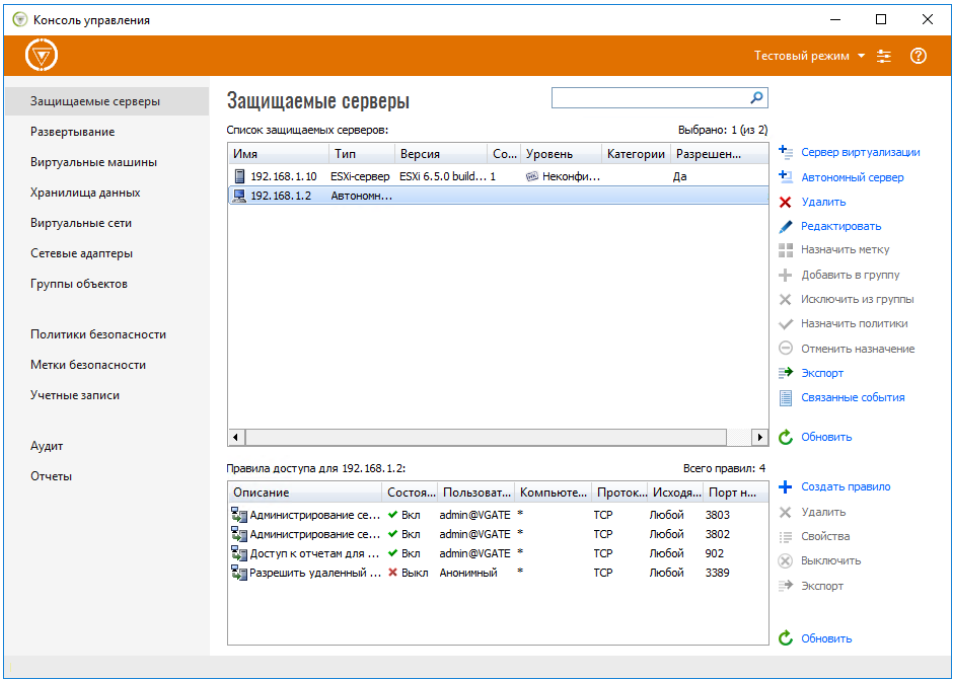
Для переключения vGate в тестовый режим:

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 (ESXi-серверов и vCenter);
- действие политик безопасности;
- действие правил разграничения доступа к защищаемым серверам и правил фильтрации сетевых подключений к vCenter;
- 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 ESXi-серверов и vCenter (подробнее о событиях аудита см. стр.167).

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

Внимание! Если в инфраструктуре присутствует сервер vCenter с установленным компонентом защиты vGate, при переключении режима требуется, чтобы настройки подключения к серверу виртуализации были сохранены (см. стр.77).

Для переключения vGate в аварийный режим:

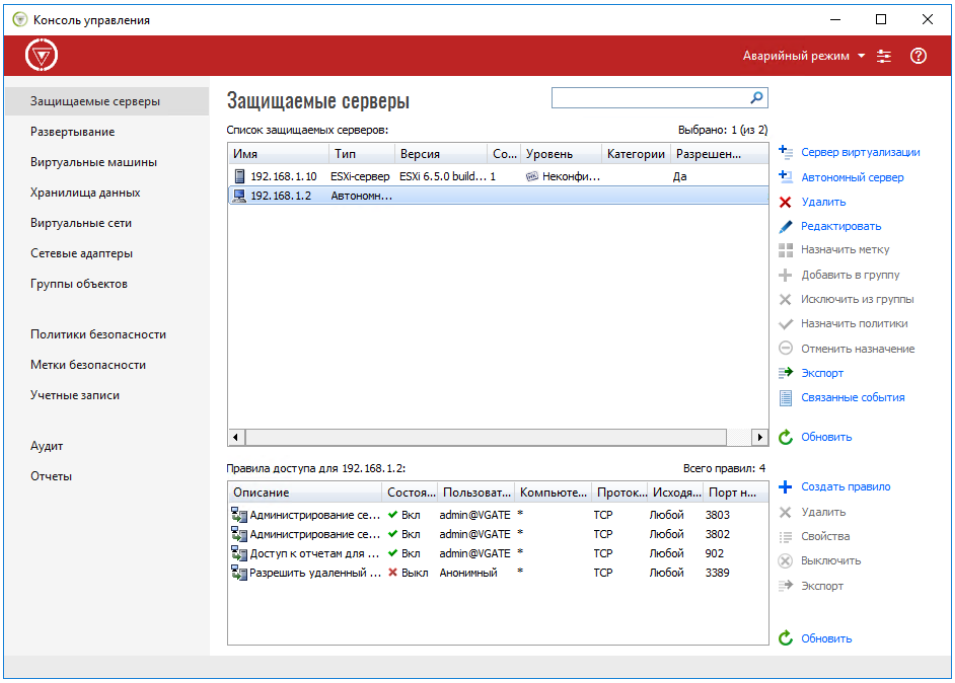
1. В области главного меню консоли управления нажмите кнопку-ссылку с названием текущего режима работы (в обычном случае — "Штатный режим") и выберите в раскрывающемся списке вариант "Аварийный режим".

   На экране появится предупреждение о переключении vGate в аварийный режим.

Примечание. Будут запрошены учетные данные для доступа к защищаемым vGate серверам ESXi в случае, если они не находятся под управлением сервера vCenter (vCSA), и серверу PSC (VMware vSphere 6.7).

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.72).

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.

   Примечание. Будут запрошены учетные данные для доступа к ESXi- серверам в случае, если они не находятся под управлением сервера vCenter (vCSA), и к серверу PSC (VMware vSphere 6.7).

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".

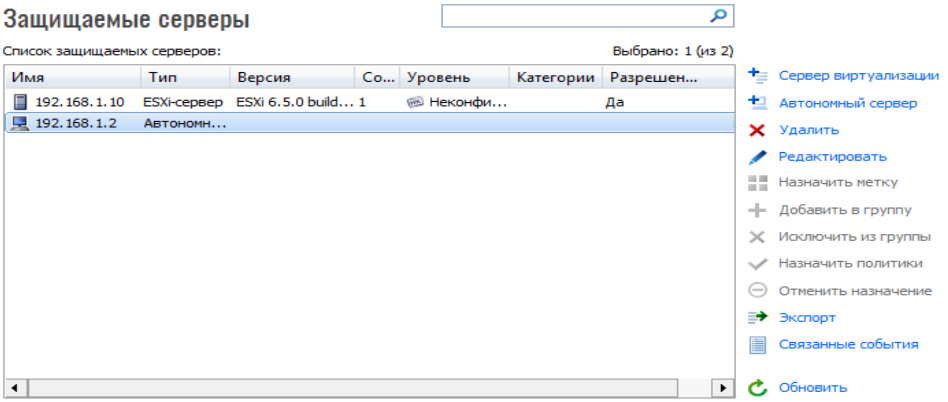
Регистрация защищаемых серверов

Защищаемыми серверами могут быть ESXi-серверы, серверы vCenter, Platform Services Controller или другие элементы виртуальной инфраструктуры, имеющие IP-адрес и находящиеся в защищаемом периметре сети администрирования (например, DNS).

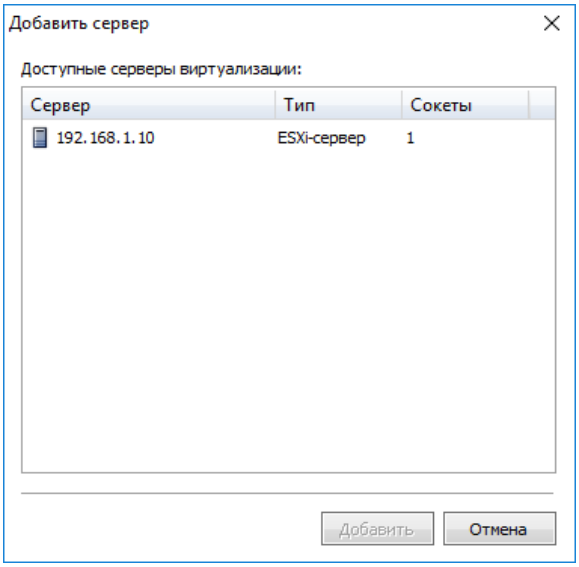
Внимание! vGate Standard позволяет осуществлять защиту только одного сервера vCenter. Если в компании эксплуатируются несколько серверов vCenter, объединенных с помощью режима VMware vCenter Linked Mode, необходимо установить компонент защиты vGate на каждый из них. Эта функция доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Для регистрации сервера ESXi, vCenter или PSC:

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 диалог со списком серверов.



Пояснение. В зависимости от заданных параметров соединения (см. стр.77) список будет содержать либо один сервер виртуализации, либо сервер vCenter и все управляемые им серверы виртуализации.

3. Выберите нужные серверы и нажмите кнопку "Добавить".

Совет. Для выбора нескольких элементов в списке используйте клавиши <Shift> и <Ctrl>.

Примечание. Поле "Сохранить имя пользователя и пароль" отмечено по умолчанию. Сохраненные параметры соединения с сервером ESXi или vCenter будут использоваться в дальнейшем при запуске консоли управления текущим пользователем на данном компьютере. Если поле не отмечено, параметры соединения будут использованы только в рамках текущей сессии работы в консоли управления, а некоторые операции в виртуальной инфраструктуре не будут контролироваться vGate (подробнее см. стр.77).

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 ESXi-сервера (см. стр.148).
Кнопка-ссылка "Экспорт" позволяет выгрузить список защищаемых серверов в файл.

Развертывание компонентов защиты

Развертывание компонентов защиты на vCenter (vCSA)

vGate Standard позволяет осуществлять защиту только одного сервера vCenter. Если в компании эксплуатируются несколько серверов vCenter, объединенных с помощью режима VMware vCenter Linked Mode, необходимо установить компонент защиты vGate на каждый из них. Эта функция доступна только в vGate Enterprise и Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).
Если на компьютере, предназначенном для компонента защиты vCenter, эксплуатируется ПО Secret Net Studio, перед началом установки необходимо отключить межсетевой экран Secret Net Studio.

Внимание! На сервере vCenter (VCSA) для vGate по умолчанию используется порт 38085. При необходимости порт можно изменить. Для этого:

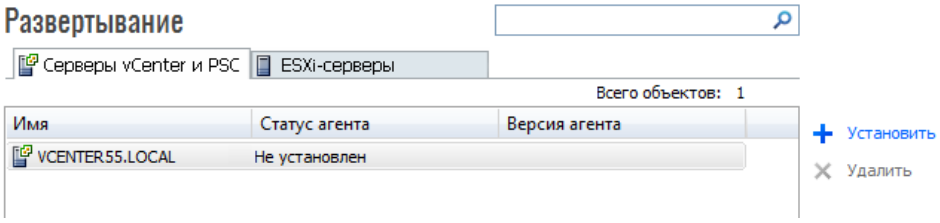
- закройте консоль управления vGate;
- измените значение порта в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Security Code\vGate DWORD VcpOnVCenterPort;
- перезапустите службу управления vGate (rhuid.exe).

Примечание. Для развертывания компонентов защиты на защищаемых серверах требуется указать параметры подключения к серверу виртуализации (см. стр.77).

Для развертывания компонентов защиты на сервере:

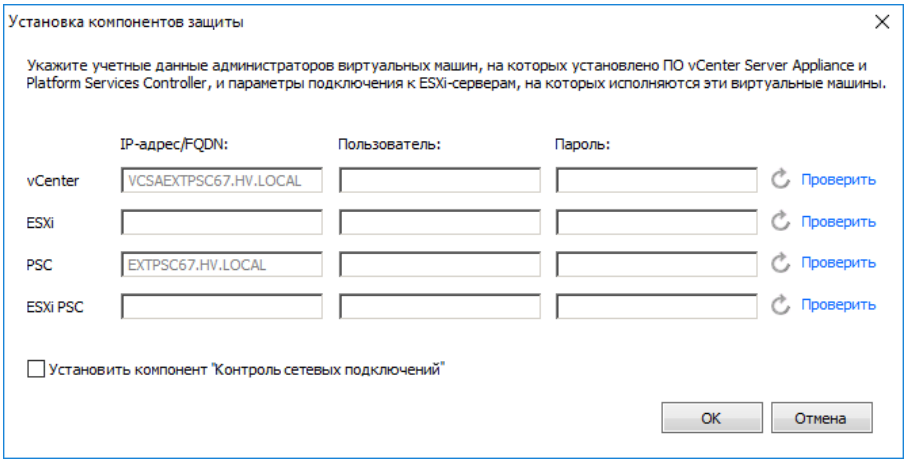
1. В консоли управления выберите функцию "Развертывание".

   На вкладке "Серверы vCenter и PSC" в области параметров появится список серверов vCenter (vCSA) и PSC.



2. Выберите из списка сервер vCenter (vCSA) и нажмите кнопку-ссылку "Установить".

   На экране появится диалог установки компонентов защиты vGate.



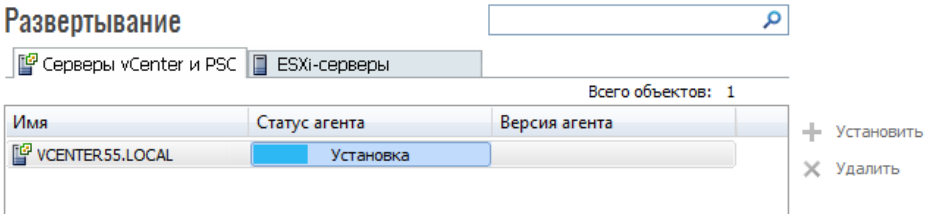
3. В зависимости от архитектуры виртуальной инфраструктуры и версии VMware vSphere будут запрошены учетные данные для подключения к различным серверам (vCenter, ESXi, PSC, ESXi PSC или ESXi passive). Укажите IP-адреса (FQDN), имена и пароли администраторов серверов.

   Примечание. Для проверки подключения к серверу с помощью указанных параметров нажмите кнопку-ссылку "Проверить" справа от нужной строки.

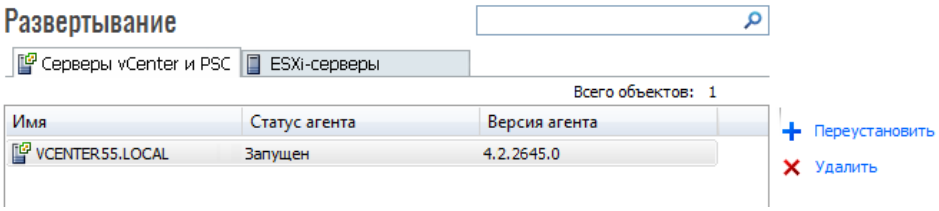
4. Отметьте поле "Установить компонент "Контроль сетевых подключений", чтобы после установки компонента защиты vGate ограничить входящие сетевые соединения на сервере vCenter. Подробнее о настройке фильтрации соединений с vCenter см. стр.**143**.

5. Нажмите кнопку "ОК" для проверки параметров подключения и установки компонентов vGate.

   На экране отобразится процесс установки.



6. При успешном завершении установки компонентов защиты параметр "Статус агента" выбранного сервера примет значение "Запущен".



Примечание. Кнопка-ссылка "Удалить" используется для запуска процедуры удаления развернутых на сервере модулей защиты. Их необходимо удалить перед удалением сервера авторизации (см. стр.59).

Развертывание компонентов защиты на ESXi-сервере

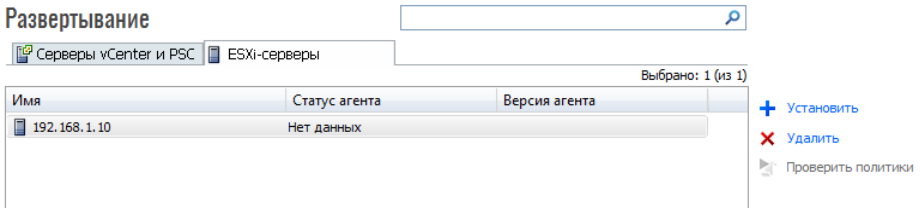
Внимание! Если в конфигурации виртуальной инфраструктуры присутствует vCenter и управление ESXi-серверами осуществляется с помощью vCenter Client или vSphere Web Client, то перед развертыванием модулей защиты ESXi-серверов необходимо установить компонент защиты на сервер vCenter (см. стр.98).

Примечание. Для развертывания компонентов защиты на защищаемых серверах требуется указать параметры подключения к серверу виртуализации (см. стр.77).

Для развертывания компонентов защиты на сервере:

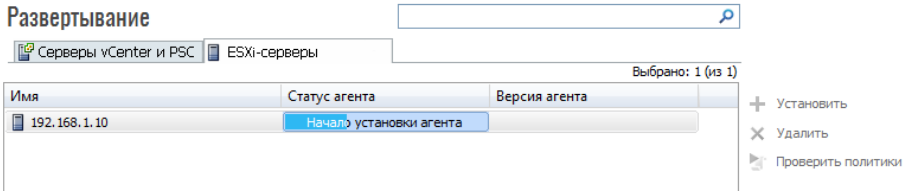
1. В консоли управления выберите функцию "Развертывание".
2. Выберите вкладку "ESXi-серверы".

   В области параметров появится список ESXi-серверов.

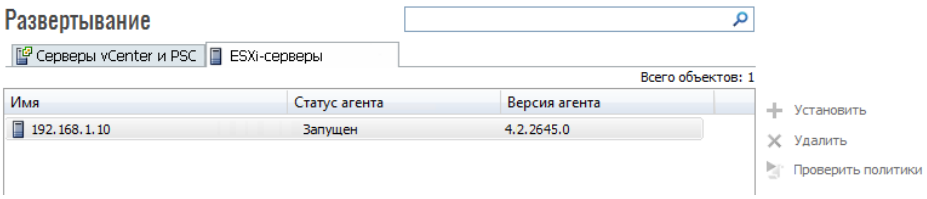


3. Выберите из списка ESXi-сервер и нажмите кнопку-ссылку "Установить".

   На экране отобразится процесс установки.



4. При успешном завершении установки компонентов защиты параметр "Статус агента" выбранного сервера примет значение "Запущен".



   Повторите эту процедуру для других серверов из списка.

Примечание. Кнопка-ссылка "Удалить" используется для запуска процедуры удаления развернутых на ESXi-серверах модулей защиты. Их необходимо удалить перед удалением сервера авторизации (см. стр.59).

Автоматическое развертывание компонентов защиты на ESXi-серверах с помощью VMware Auto Deploy

Данная функция доступна только в vGate Enterprise и Enterprise Plus.

VMware vSphere включает в себя функцию "Auto Deploy", предназначенную для автоматического развертывания ESXi. В состав vGate входит утилита VibModificator.exe, которая позволяет создать архив файлов для установки компонентов защиты vGate, чтобы затем добавить его в образ ESXi, используемый VMware Auto Deploy.

Утилита располагается в каталоге установки vGate на сервере авторизации и доступна из командной строки. Для вызова подробной информации об утилите откройте редактор командной строки и введите следующую команду:

```
VibModificator.exe –h
```

Для создания архива файлов по шаблону:

1. Откройте редактор командной строки от имени администратора и выполните следующую команду:

   ```
   C:\Program Files (x86)\vGate\VibModificator.exe -z -p <путь>
   ```

   где:

   - z — команда создания ZIP-архива по шаблону sc-vgate-autodeploy-xxxxx-esxi-template.vib;
   - p **<путь>** — путь к директории, в которую будет сохранен архив. Если директория не существует, она будет создана. По умолчанию сохранение производится в каталог установки vGate (C:\Program Files (x86)\vGate).

   В результате выполнения команды в указанной директории будет создан файл sc-vgate-autodeploy-xxxxx-esxi-offline-bundle.zip.

   Примечание. Результат запуска утилиты VibModificator.exe аналогичен результату выполнения команды "VibModificator.exe -z -p **<путь>**".

2. Скопируйте полученный архив на сервер vCenter для добавления в образ ESXi.

Для создания VIB-файла по шаблону:

1. Откройте редактор командной строки от имени администратора и выполните следующую команду:

   ```
   C:\Program Files (x86)\vGate\VibModificator.exe -s -p <путь>
   ```

   где:

   - s — команда создания набора файлов по шаблону sc-vgate-autodeploy-xx-xxx-esxi-template.vib;
   - p **<путь>** — путь к директории, в которую будет сохранен набор файлов. Если директория не существует, она будет создана. По умолчанию сохранение производится в каталог установки vGate (C:\Program Files (x86)\vGate).

   В результате выполнения команды в указанной директории будет создана папка с файлом sc- vgate-autodeploy-xxxxx-esxi.vib и набором файлов XML.

2. При необходимости проверьте VIB-файл, для этого выполните команду:

   ```
   C:\Program Files (x86)\vGate\VibModificator.exe -c -n sc-vgate-autodeploy-xxxxx-esxi.vib
   ```

где:

- c — команда проверки VIB-файла на наличие значений реестра;
- n **sc-vgate-autodeploy-xxxxx-esxi.vib** — имя шаблона VIB-архива. По умолчанию поиск VIB-архива производится в текущей папке.

В результате выполнения команды на экране появится список найденных параметров или пустая строка, если параметры не найдены. Для VIB-файла и для проверки используются ключи реестра. Например:

- ключи реестра AutodeployPort: deploy port is 9989, firewall port is 9989;
- ключи реестра RhuidHttpPort: haron port is 80, haron address is 192.168.5.30.

3. Создайте ZIP-архив из полученных XML-файлов и VIB-файла и скопируйте его на сервер vCenter для добавления в образ ESXi.

Для автоматического развертывания компонента защиты vGate на ESXi-сервере:

1. Добавьте созданный архив с файлом vgate-autodeploy-xxxxx-esxi.vib в образ ESXi-сервера, используемый VMware Auto Deploy.
2. Включите ESXi-сервер. В консоли управления vGate добавьте сервер в список защищаемых объектов.

   Через несколько минут на ESXi- сервер будет автоматически установлен компонент защиты vGate. Для ускорения процесса можно выполнить установку компонента защиты ESXi-сервера вручную (см. стр.**100**). В дальнейшем при перезагрузке ESXi- сервера компонент защиты vGate будет устанавливаться автоматически.
3. Создайте необходимые правила для доступа пользователей к ESXi-серверу (см. стр.**137**).

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.**104**).

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.**85**). Все доменные пользователи автоматически добавляются в группу "Аутентифицированный", и для них действуют соответствующие правила доступа к защищаемым серверам (см. стр.**137**).

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

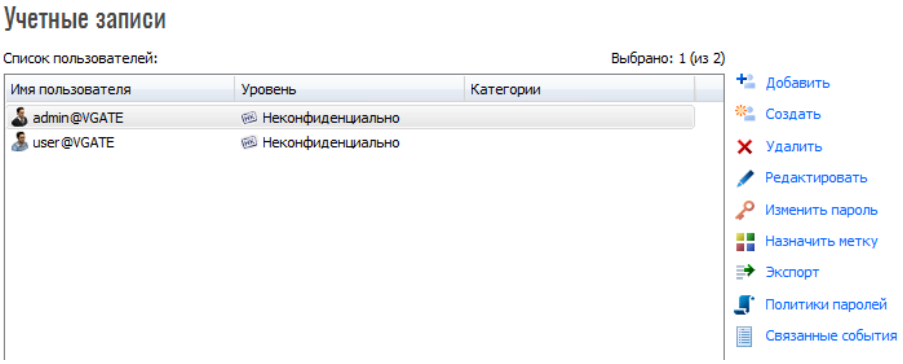
Внимание!
- vGate поддерживает работу только с одним уровнем вложенности групп Active Directory.
- Работа с вложенными группами реализуется только в случае, если контроллер домена Active Directory передает информацию о членстве пользователя во вложенных группах.

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.**104**)
Удалить	Удаление выбранной учетной записи
Редактировать	Изменение свойств выбранной учетной записи, в том числе и отключение учетной записи (см. стр.**106**)
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.**148**)
Экспорт	Экспорт выбранных учетных записей в файл
Политики паролей	Изменение уровня сложности паролей (см. стр.**107**). 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 ESXi-серверам и другим узлам сети администрирования.

Имена учетных записей компьютеров имеют следующий формат:

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

Например: arm$@VGATE.

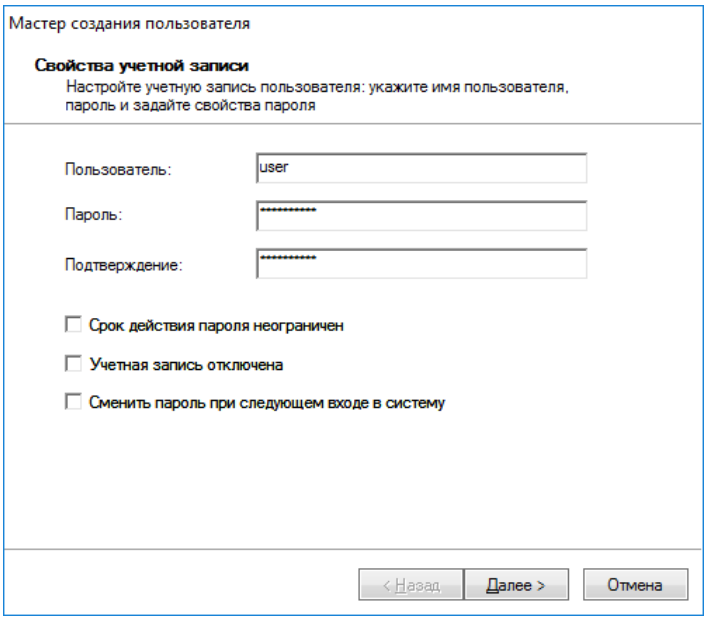
Внимание! Не рекомендуется удалять учетные записи компьютеров, так как для их восстановления потребуется повторная установка агента аутентификации.

Создание учетной записи

Для создания учетной записи:

1. Нажмите кнопку-ссылку "Создать".

   На экране появится окно мастера создания пользователя.

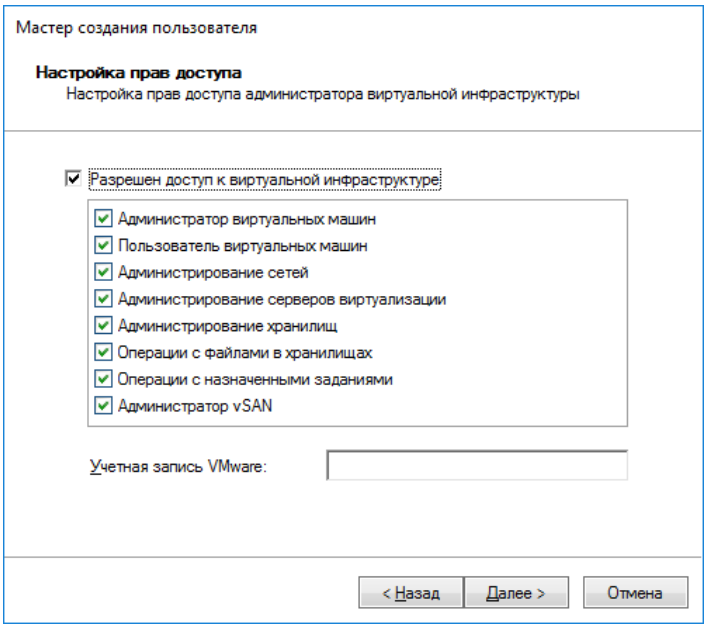


2. Укажите имя пользователя, дважды введите пароль. При необходимости настройте свойства пароля.

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.



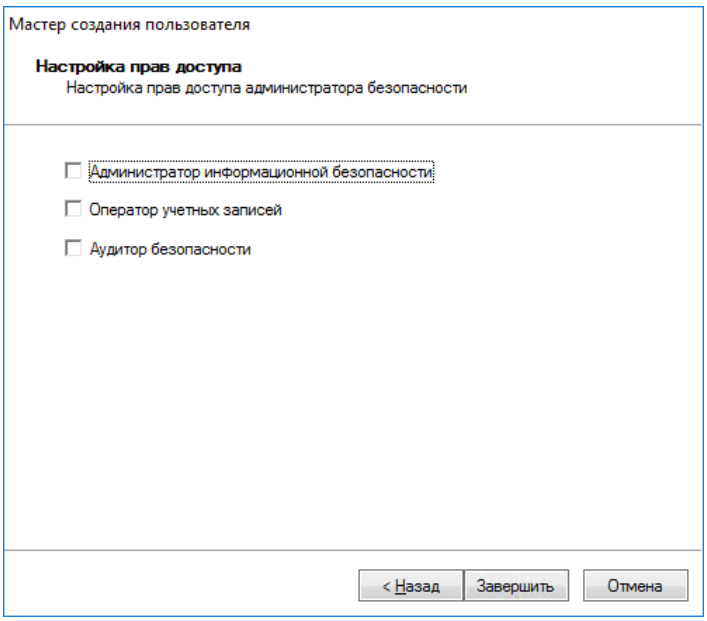
Примечание. Подробнее о привилегиях различных типов пользователей см. стр.**215**.

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.

Для контроля доступа пользователя к среде VMware vSphere укажите в поле "Учетная запись VMware " имя учетной записи администратора vSphere (см. стр.**106**).

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".

Учетная запись VMware

По умолчанию поле "Учетная запись VMware" в диалоге создания учетной записи пользователя vGate пустое. Это означает, что в среду VMware vSphere данный пользователь может входить под любой учетной записью.

Для контроля доступа пользователя к среде vSphere в данном поле следует указать одну или несколько учетных записей VMware. Каждую учетную запись необходимо указать во всех допустимых форматах: "domain\user", "user@domain", "full.domain.name\user" и "user@full.domain.name". В качестве разделителя между записями в разных форматах используется символ ";".

Например:

vsphere\admin;admin@vsphere;vsphere.local\admin;admin@vsphere.local

После этого данный пользователь vGate сможет войти в среду vSphere только под указанными учетными записями.

Параметр полезен для настройки ограничения полномочий АИБ при работе с виртуальной инфраструктурой. Для полноценного разделения административных функций полномочия АИБ должны быть ограничены только возможностью просмотра параметров. Таким образом, поле "Учетная запись VMware" дает возможность сопоставить для АИБ учетную запись в среде VMware с ограниченными полномочиями.

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.225.

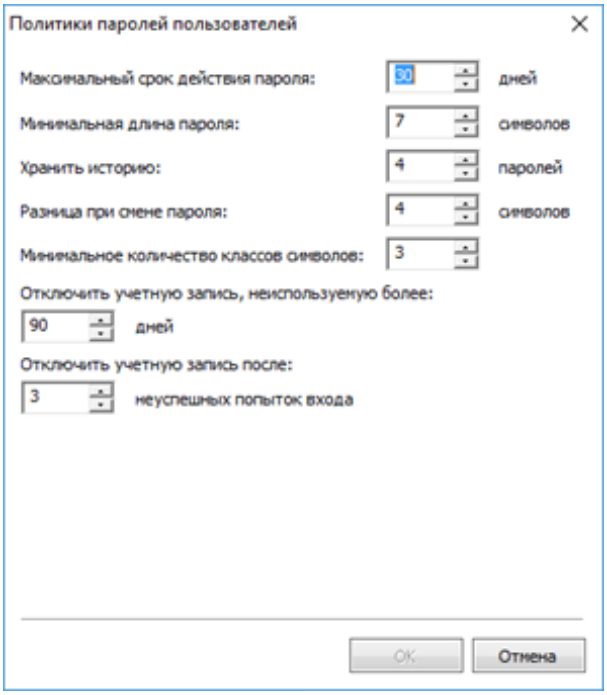
По умолчанию в системе заданы некоторые значения параметров политик паролей (подробнее описано ниже). АИБ может изменить значения этих параметров при необходимости.

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:

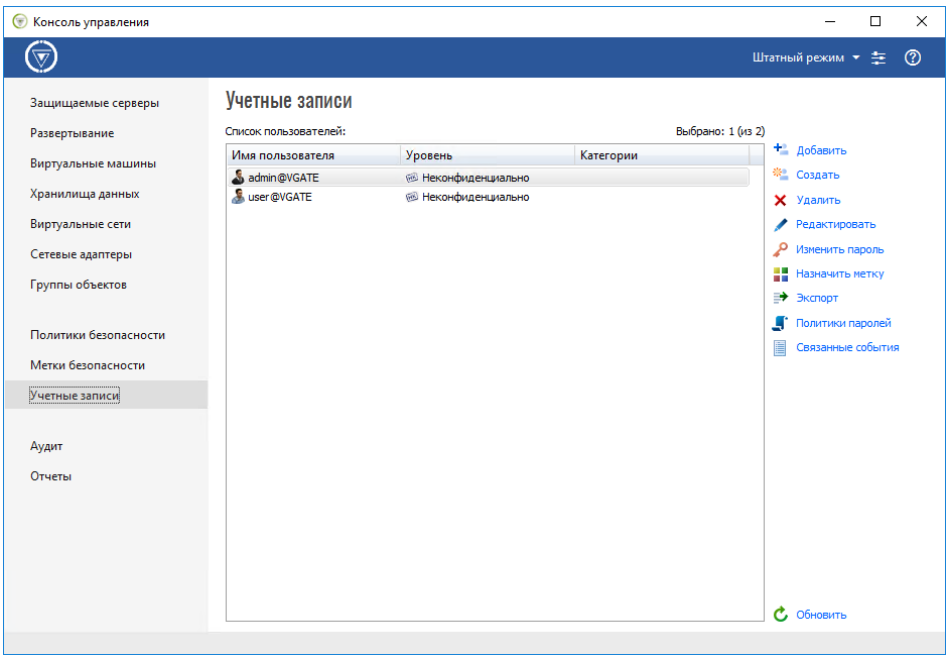
1. Выполните инициализацию персонального идентификатора в Secret Net Studio либо в ПО Рутокен или JaCarta (если Secret Net Studio не используется) согласно документации к этим продуктам.

   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.

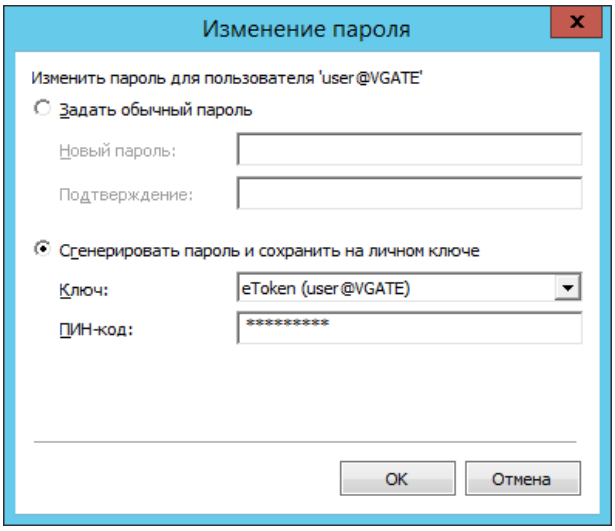
2. Подключите персональный идентификатор к компьютеру, на котором установлена консоль управления vGate.
3. В консоли управления выберите функцию "Учетные записи".

   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].

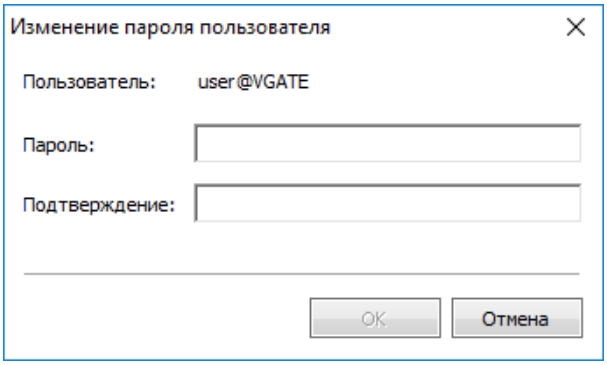
В vGate не поддерживается присвоение персонального идентификатора учетным записям из Active Directory. Если необходимо настроить работу с персональным ключом для таких пользователей, используйте сетевую версию Secret Net. В этом случае персональный идентификатор, присвоенный доменной учетной записи в 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".

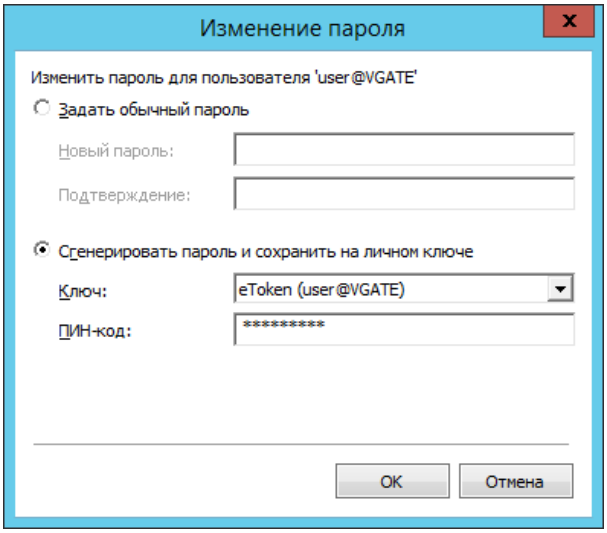
Примечание. Для учетных записей из Active Directory изменение пароля с помощью vGate не поддерживается. Для этого можно использовать средства администрирования Active Directory.

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.

Настройка правил доступа к vCenter и vSphere Web Client

Для предоставления АВИ доступа к защищаемым серверам после развертывания компонентов защиты vGate необходимо настроить правила разграничения доступа в консоли управления (подробнее о настройке ПРД см. стр.**137**).

При использовании vSphere Client и vSphere Web Client для администрирования виртуальной инфраструктуры серверам vCenter и vSphere Web Client следует добавить ПРД на основе следующих шаблонов:

- **Доступ пользователя к vCenter**

  Шаблон содержит набор ПРД для предоставления доступа АВИ к vCenter. В шаблоне указаны порты доступа к vCenter, заданные по умолчанию (TCP-порты 80, 443, 6501, 6502, 8084, 9084, 9087, 8000, 8001, 6500, 8098, 8099, 8109, 514, 1514). Данный набор правил следует настроить для сервера vCenter. В качестве пользователя, для которого действуют правила, следует указать учетную запись АВИ.

- **Подключение пользователя с помощью vSphere Web Client v6.x/v7.x**

  Шаблон ПРД для предоставления доступа пользователю к vCenter с помощью Web Client для vSphere 6.5 и выше. В шаблоне указан TCP-порт 443 для доступа по протоколу vSphere Web Client.

Группировка объектов

В консоли управления vGate 4.4 возможно объединение объектов виртуальной инфраструктуры в группы. Такими объектами могут быть виртуальные машины, ESXi-серверы, шаблоны виртуальных машин, 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.

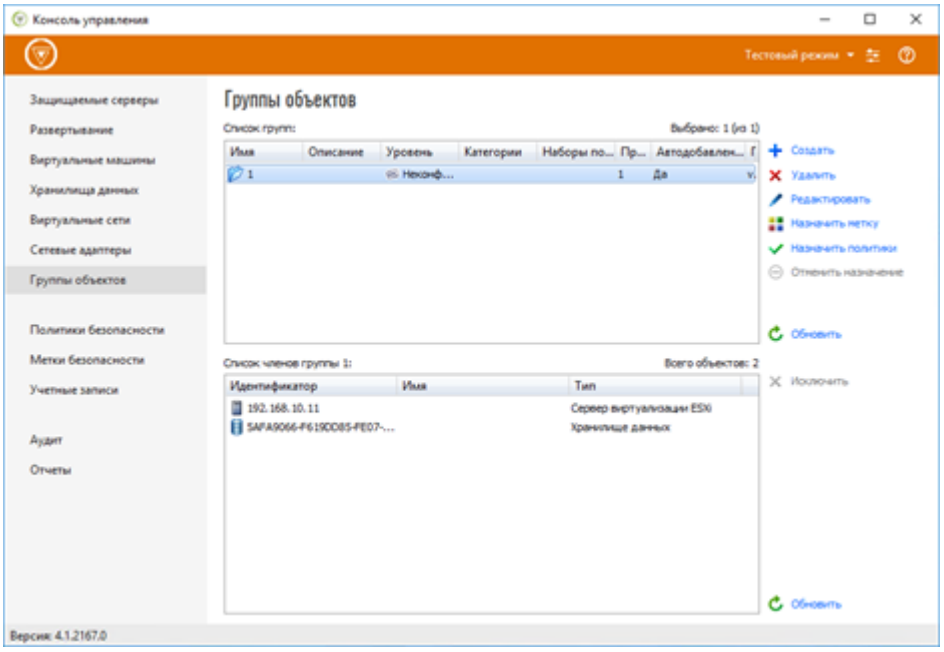
Внимание! Не рекомендуется использовать символы %, /, \ в названии виртуальных машин VMware. Возможно возникновение проблем при добавлении таких виртуальных машин в группы.

Внимание! При назначении политики "Контроль целостности шаблонов виртуальных машин" с включенным параметром "Целостность образов виртуальных дисков" группе, содержащей шаблоны виртуальных машин, операция подсчета контрольных сумм образов дисков может занять длительное время.

Для создания группы объектов:

1. В консоли управления выберите функцию "Группы объектов".

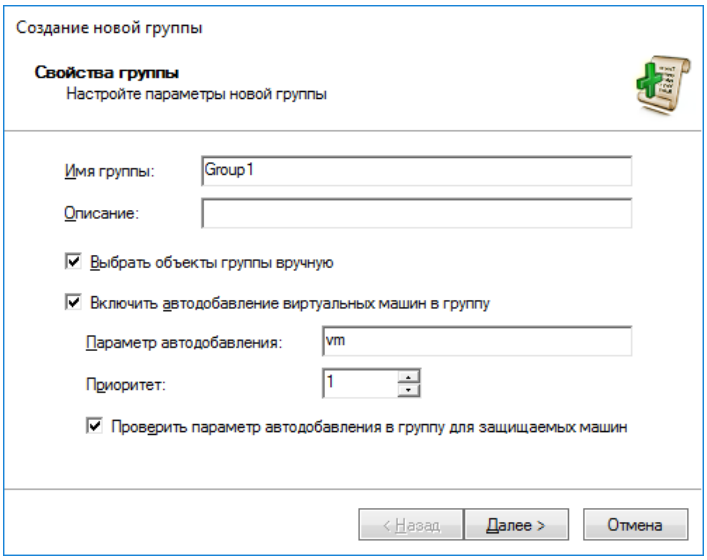
   В области параметров появится список групп.



2. Чтобы создать группу, нажмите кнопку-ссылку "Создать".

Внимание! Для создания групп в консоли управления должны быть сохранены параметры подключения к серверу виртуализации (см. стр.77).

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

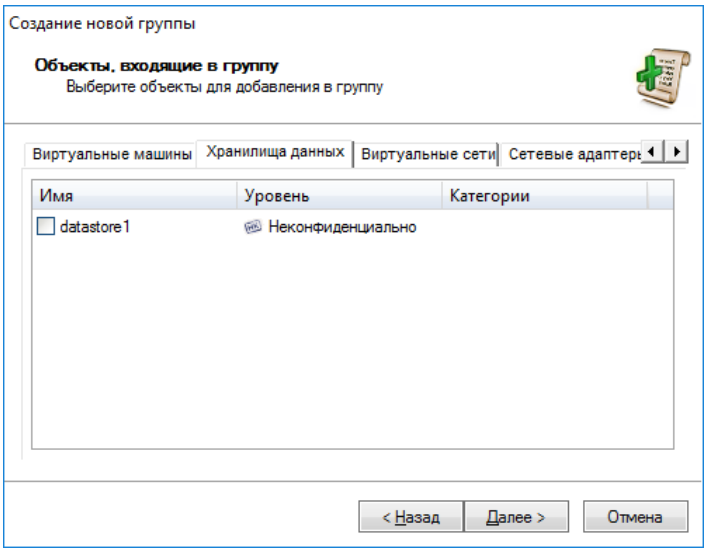
Примечание. По умолчанию автодобавление виртуальных машин в группы объектов выполняется каждые 10 минут. При необходимости настройки автоматического обновления могут быть изменены в консоли управления. Для этого перейдите в раздел "Конфигурация" — "Дополнительные настройки" — "Настройки сети, контроля 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).

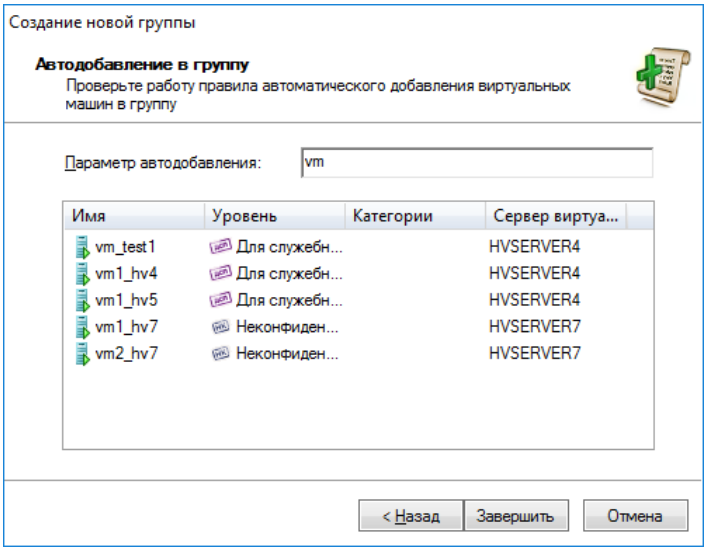
Если был отмечен пункт "Выбрать объекты группы вручную", на экране появится окно выбора объектов.



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.

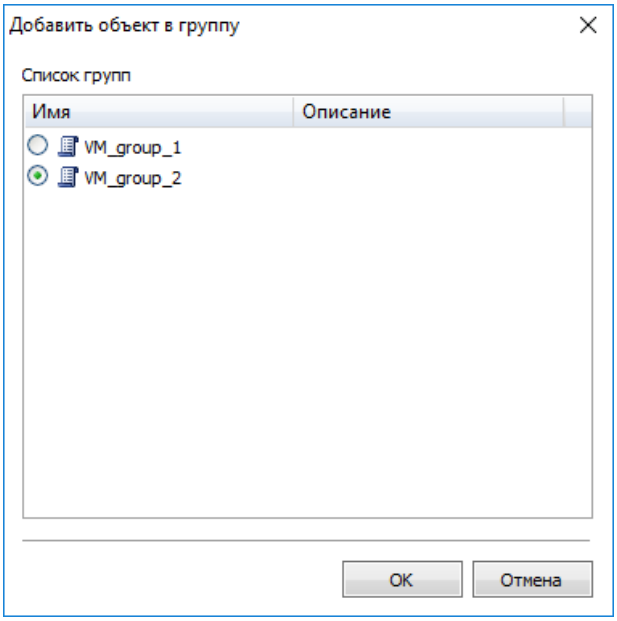
Для добавления объекта в группу:

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.

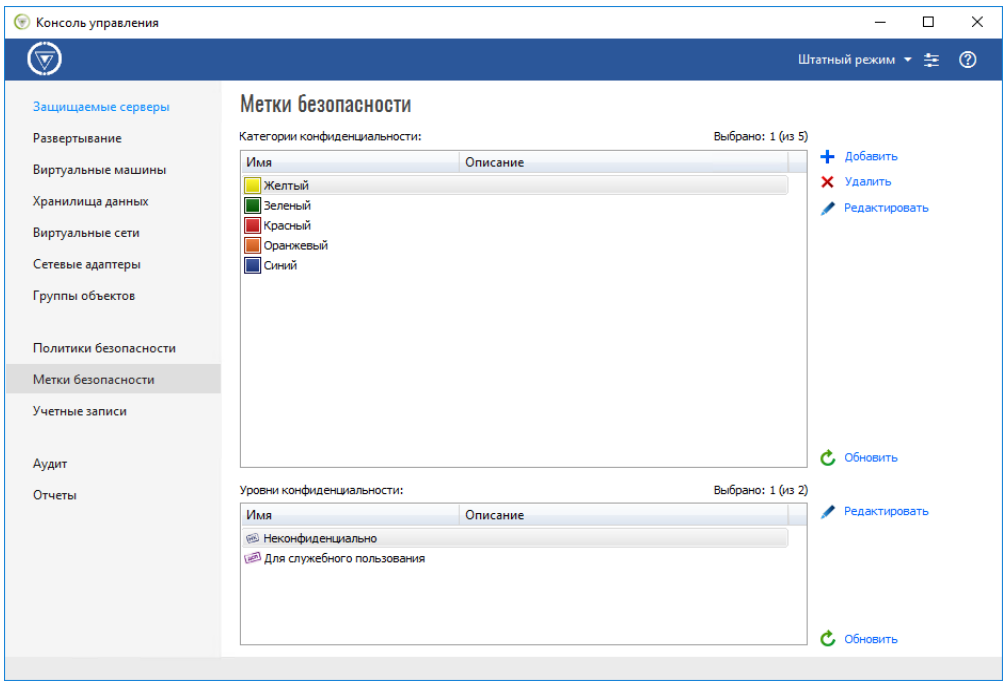
2. Выберите нужный объект и нажмите кнопку-ссылку "Исключить". Объект будет исключен из группы.

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.



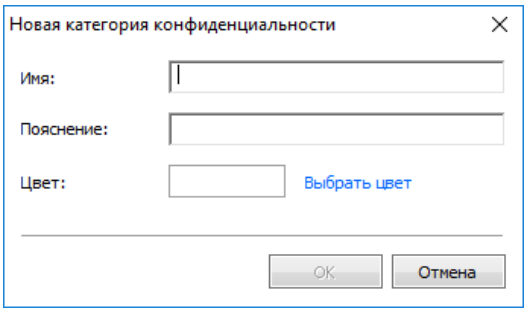
Редактирование списка категорий

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 "OK".

   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

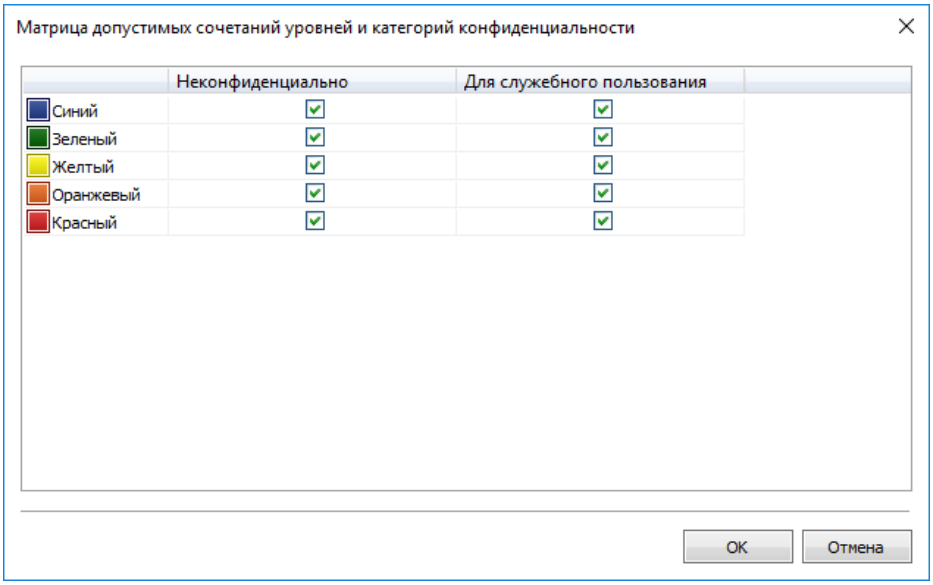
При назначении составных меток (меток, содержащих уровни и категории конфиденциальности одновременно) объектам осуществляется автоматическая проверка возможности задания метки с указанным АИБ сочетанием уровня и категорий конфиденциальности. Для этого используется матрица допустимых сочетаний уровней 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 ESXi-серверов 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	Специально разработанный для vGate набор политик, позволяющий задать более безопасный режим работы ESXi-серверов, ВМ и виртуальных сетевых коммутаторов
PCI DSS v3.2	Рекомендуемый набор политик для приведения виртуальной среды в соответствие требованиям PCI DSS. Requirements and Security Assessment Procedures v3.2
VMware 6.5 SCG	Набор политик для приведения виртуальной среды в соответствие требованиям VMware vSphere 6.5 Security Configuration Guide
VMware 6.7 SCG	Набор политик для приведения виртуальной среды в соответствие требованиям VMware vSphere 6.7 Security Configuration Guide
CIS for ESXi 6.5	Набор политик для приведения виртуальной среды в соответствие рекомендации CIS Security Configuration Benchmark for VMware vSphere (ESXi 6.5)
CIS for ESXi 6.7	Набор политик для приведения виртуальной среды в соответствие рекомендации CIS VMware ESXi 6.7 Benchmark version 1.0.1
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"
АС 1В	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду автоматизированных систем класса 1В в соответствие РД ФСТЭК России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации"
АС 1Б	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду автоматизированных систем класса 1Б в соответствие РД ФСТЭК России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации"
СТО БР ИСПДн-Д	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных класса ИСПДн-Д в соответствие стандарту СТО БР ИББС
СТО БР ИСПДн-Б	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных класса ИСПДн-Б в соответствие стандарту СТО БР ИББС
СТО БР ИСПДн-И	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных класса ИСПДн-И в соответствие стандарту СТО БР ИББС

Набор политик	Описание
СТО БР ИСПДн-С	Рекомендуемый набор политик безопасности для приведения перенесенных в виртуальную среду информационных систем персональных данных класса ИСПДн-С в соответствие стандарту СТО БР ИББС
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
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 ESXi-сервера

ESXi-серверам могут назначаться следующие политики безопасности.

Политика	Описание
Список разрешенных программ	Обеспечивает доверенную программную среду ESXi-сервера. На ESXi-сервере хранится список разрешенных по умолчанию программ. АИБ при необходимости может с помощью консоли управления добавить или удалить из этого списка нужные программы
Запрет подключения USB-носителей к ESXi-серверу	Политика исключает возможность подключения съемных USB-носителей к ESXi-серверу. После включения данной политики необходима перезагрузка ESXi-сервера
Установка и поддержка целостности файловой системы	Политика ограничивает доступ к конфигурационным файлам служб
Запрет операций с буфером обмена	Политика устанавливает запрет на выполнение операций с буфером обмена для каждой виртуальной машины. После включения данной политики необходима перезагрузка виртуальных машин
Разделение сетей консоли управления и виртуальных машин	Политика проверяет, что не используется одна сеть для Service Console (или Management vmkernel interface для ESXi-сервера) и виртуальных машин
Использование протокола CHAP для iSCSI	Политика задает необходимость использования CHAP для проверки подлинности при подключении iSCSI-устройств
Настройки логирования виртуальных машин на ESXi-сервере	Политика настраивает следующие параметры логирования для каждой виртуальной машины: log.rotateSize=100000, log.keepOld=10
Предотвращение сжатия виртуальных дисков	Политика устанавливает запрет на выполнение операции сжатия виртуального диска для каждой виртуальной машины. После включения данной политики необходима перезагрузка виртуальных машин
Предотвращение шпионажа других пользователей на удаленных консолях администратора	Политика защищает открытую удаленную консоль администратора от других подключений. Будет разрешено соединение удаленной консоли только с одной виртуальной машиной. Другие запросы будут отклоняться до окончания первой сессии. После включения данной политики необходима перезагрузка виртуальных машин
Запрет отсылки информации о производительности ESXi-сервера гостевым системам	Политика отключает отсылку информации о загрузке ESXi-сервера на гостевую ОС, так как нарушитель потенциально может использовать эти данные для получения информации об узле для осуществления дальнейших атак на хост. После включения данной политики необходима перезагрузка виртуальных машин
Ограничение размера информационных сообщений от виртуальной машины в VMX-файле	Политика устанавливает максимальный размер для VMX-файла. Неконтролируемый размер VMX-файла может привести к отказу в обслуживании при заполнении хранилища данных. По умолчанию устанавливается ограничение в 1МБ, чего должно быть достаточно в большинстве случаев. После включения данной политики необходима перезагрузка виртуальных машин
Избегать использования несохраняющихся (nonpersistent) дисков	Политика проверяет и информирует об использовании independent-nonpersistent дисков у виртуальных машин. После включения данной политики необходима перезагрузка виртуальных машин

Политика	Описание
Запрет использования Managed Object Browser	Политика блокирует возможность использования Managed Object Browser
Контроль за доступом через VMSafe CPU/Mem API	Если не используются продукты, работающие с VMSafe CPU/Mem API, то необходимо контролировать его применение. Политика проверяет, что у всех виртуальных машин сервера этот API отключен и не настроен. Если же использование данного API необходимо, отметьте параметр "Разрешить VMsafe API" и укажите IP-адрес и порт для доступа к VMsafe CPU/Memory API. В этом случае политика будет проверять и/или применять заданные параметры vmsafe.enable, vmsafe.agentAddress, vmsafe.agentPort
Контроль за доступом через dvfilter Network API	Если ВМ не должна быть защищена с помощью dvfilter Network API, то необходимо убедиться в том, что в VMX-файле отсутствуют записи вида "ethernet0.filter1.name = dv-filter1", где "ethernet0" — сетевой адаптер виртуальной машины, "filter1" – номер фильтра, "dv-filter1" — имя модуля ядра, реализующего защиту данной ВМ. Соответственно, если ВМ должна быть защищена, то необходимо убедиться в том, что имя данного модуля ядра указано корректно. После включения данной политики необходима перезагрузка виртуальных машин
Настройка постоянного журналирования на ESXi-сервере	Политика позволяет задать путь к журнальному файлу в хранилище данных, что исключает потерю журнальных данных при перезагрузке сервера
Запрет доступа к VMSafe Network API	Политика запрещает доступ к VMSafe Network API
Проверка настроек SNMP-агента	Политика позволяет проверить и задать в случае необходимости настройки для SNMP-агента. Используйте ";" в качестве разделителя для указания нескольких обществ и приемников SNMP-данных
Включить Lockdown Mode	Включение Lockdown Mode отключает возможность прямого доступа к ESXi-серверу, что обязывает использовать vCenter для управления сервером. Это делается для того, чтобы избежать возможности обхода механизма ролей и контроля доступа, реализованного в vCenter, путем локального входа на хост. В случае, когда все взаимодействия происходят через сервер vCenter, значительно снижается риск того, что кто-то необоснованно получит повышенные привилегии или выполняемые операции произойдут без соответствующего аудита. Режим блокировки не распространяется на пользователей, которые выполняют вход с помощью уполномоченных ключей. В таком случае пользователю root не блокируется доступ к хосту по протоколу SSH, даже если он находится в режиме Lockdown Mode. Обратите внимание, что пользователям, перечисленным в списке DCUI.Access для каждого хоста, разрешается переопределить режим Lockdown Mode и выполнять локальный вход. По умолчанию в этом списке присутствует только пользователь root
Отключение Direct Console User Interface	Политика блокирует возможность использования Direct Console User Interface
Аудит модулей ядра гипервизора без цифровой подписи	Политика проверяет загруженные модули ядра и информирует об использовании неподписанных модулей. Список разрешенных к загрузке неподписанных модулей можно расширить
Отключить протокол IPv6	Политика позволяет отключить протокол IPv6, если он не используется. После применения политики необходим перезапуск сервера

Политика	Описание
Запрет контроля устройств ESXi-сервера со стороны виртуальных машин	Политика запрещает гостевой операционной системе виртуальной машины контролировать устройства ESXi-сервера
Синхронизация времени	Политика позволяет настроить синхронизацию времени
Отсылка событий сервера виртуализации на syslog-сервер	Политика позволяет настроить ведение журнала событий ESXi-сервера на удаленном сервере syslog
Очистка памяти виртуальных машин	Политика обеспечивает очистку памяти после завершения работы ВМ. После включения данной политики требуется перезагрузка виртуальной машины
Очистка памяти виртуальных машин (двукратная запись)	Политика обеспечивает двукратную очистку памяти после завершения работы ВМ. После включения данной политики требуется перезагрузка виртуальной машины
Настройки безопасности для виртуальных коммутаторов	Политика задает более строгие настройки работы виртуального коммутатора (запрещены смешанный режим, смена MAC-адреса и несанкционированные передачи)
Группы портов не настроены на значения VLAN 4095, кроме как для Virtual Guest Tagging	Когда группе портов назначен номер VLAN 4095, то считается, что активируется режим Virtual Guest Tagging (VGT). В этом режиме виртуальный коммутатор передает весь трафик внутрь гостевой ОС виртуальной машины без каких-либо модификаций тегов VLAN. VLAN 4095 следует использовать только в случае, если гостевая ОС специально настроена для самостоятельного управления тегами VLAN. Политика назначается на ESXi-сервер и блокирует возможность указания значения VLAN 4095
Группы портов не настроены на значения native VLAN	ESXi-серверы не используют концепцию native VLAN. Сетевые пакеты с VLAN, указанным в группе портов, будут помечены специальным тегом. Пакеты с VLAN, не указанным в группе портов, не будут помечены и, следовательно, будут считаться относящимися к native VLAN физического коммутатора. Например, пакеты с VLAN 1, исходящие из физического коммутатора Cisco, не будут помечены, поскольку они трактуются как пакеты с native VLAN. В то же время пакеты с VLAN 1, исходящие с ESXi-сервера, будут отмечены тегом "1". Таким образом, трафик с ESXi-сервера, предназначенный для native VLAN, будет маршрутизироваться некорректно (так как пакеты помечены тегом), а трафик, исходящий из физического коммутатора с native VLAN, не будет виден (так как пакеты без тегов). Политика назначается на ESXi-сервер и блокирует возможность использования идентификатора native VLAN, указанного в настройках политики
Запрет автоматической установки VMware Tools	Автоматическая установка VMware Tools может автоматически запускать перезагрузку компьютера. Политика запрещает автоматическую установку VMware Tools и предотвращает автоматические перезагрузки компьютера
Запрет VM Monitor Control	Виртуальные машины, работающие на ESXi-сервере, "знают", что работают в виртуальном окружении, и эта информация доступна VMware Tools, установленным в гостевой ОС. Из-за этого злоумышленник может получить информацию о платформе, на которой работают ВМ, которую нельзя было бы получить в случае обычного аппаратного сервера. Политика полностью отключает все обработчики для виртуальных машин, и при ее использовании гостевая ОС совершенно не "осознает", что работает в виртуальном окружении

Политика	Описание
Запрет некоторых скрытых возможностей	Некоторые параметры VMX не применяются к vSphere, потому что виртуальные машины VMware работают на vSphere и настольных платформах виртуализации, таких как Workstation или Fusion. Явное отключение данных функций сокращает число потенциальных уязвимостей за счет того, что уменьшается количество способов воздействия гостевой системы на хост-систему
Запрет ESXi Shell, кроме случаев диагностики и устранения неполадок	ESXi Shell — это интерактивный интерпретатор командной строки, доступный для запуска в DCUI или удаленно по SSH. Для доступа в этот режим требуется пароль суперпользователя root на данном сервере. ESXi Shell можно включать и выключать для отдельных ESXi-серверов. Действия, инициированные в ESXi Shell, совершаются в обход vCenter RBAC и не фиксируются средствами аудита. ESXi Shell следует включать только для устранения неполадок/решения проблем, если оно невозможно с помощью vSphere Client или vCLI/PowerCLI
Запрет SSH	Если разрешено использование ESXi Shell, то его можно запустить непосредственно на ESXi-сервере через DCUI или удаленно по SSH. Удаленный доступ к ESXi-серверу следует предоставлять только vSphere Client, утилитам удаленного доступа (vCLI/PowerCLI) и по публичным API. В обычных условиях удаленный доступ к серверу по SSH должен быть запрещен
Запрет логирования ВМ	Политика запрещает логирование для виртуальных машин. Запрет логирования ВМ усложняет процесс поддержки и устранения неполадок. Для ограничения размера и количества лог-файлов можно использовать описанные ниже настройки. Обычно новый лог-файл создается только после перезагрузки хост-системы, поэтому файл может достигать довольно больших размеров. Чтобы новые лог-файлы создавались чаще, можно ограничить максимальный размер файла. В целях ограничения общего объема сохраняемой в журналах информации VMware рекомендует хранить 10 лог-файлов размером 1000 КБ каждый. Для хранилища данных рекомендуется устанавливать размер блока 2 или 4 МБ, так как ограничение размера файлов до гораздо меньшего объема приведет к избыточности ресурсов хранилища. Каждый раз, когда в существующий файл добавляется новая запись, проверяется размер файла; если он превышает установленный порог, то следующая запись добавляется в новый файл. Если достигнуто максимально допустимое количество файлов, то перед добавлением нового файла самый старый файл удаляется. Для обхода этих ограничений злоумышленник может совершить попытку сетевой DoS-атаки с внесением в файл огромной записи. Но размер каждой записи ограничен 4 КБ, так что каким бы крупным ни был файл, его размер не будет превышать установленный лимит более чем на 4 КБ. Не следует отключать логирование до тех пор, пока описанный вариант с ротацией лог-файлов не докажет свою несостоятельность. Отсутствие контроля за логированием может привести к отказу в обслуживании (DoS) из-за переполнения хранилища данных

Политика	Описание
Включить фильтр BPDU на ESXi-сервере для предотвращения отключения от портов физического коммутатора при включенном Portfast или BPDU Guard	На аппаратном коммутаторе, к которому непосредственно подключен ESXi-сервер, для сокращения задержек соединения по протоколу STP часто включены BPDU Guard и Portfast. Если пакет BPDU отправляется с виртуальной машины ESXi-сервера на настроенный таким образом аппаратный коммутатор, то может возникнуть последовательное отключение всех интерфейсов исходящих соединений от ESXi-сервера. Для предотвращения этого на ESXi-сервере можно включить BPDU Filter, который будет отсеивать все BPDU-пакеты, отправляемые на аппаратный коммутатор. Следует помнить, что некоторые решения SSL VPN, использующие возможности Windows по управлению сетевыми мостами, могут обоснованно генерировать BPDU-пакеты. Перед тем как активировать BPDU Filter, администратор должен убедиться, что виртуальные машины на ESXi-сервере не генерируют допустимые BPDU-пакеты. Если это так и BPDU Filter включен, то включение опции Reject Forged Transmits в группе портов виртуального коммутатора добавляет защиту от возникновения топологических петель
Задать ограничение допустимого времени работы служб ESXi Shell и SSH	При запуске служб ESXi Shell или SSH на ESXi-сервере время их работы не ограничено. Чтобы избежать бесконечной работы этих служб, установите значение параметра ESXiShellTimeOut. Параметр ESXiShellTimeOut определяет период времени, по истечении которого службы ESXi Shell и SSH будут автоматически остановлены
Задать ограничение допустимого времени простоя сессий ESXi Shell и SSH	Если пользователь забывает завершить SSH-сессию, то неиспользуемое соединение остается активным на неограниченный срок, повышая риск того, что злоумышленник сможет получить привилегированный доступ к ESXi-серверу. Параметр ESXiShellInteractiveTimeOut позволяет автоматически завершать неиспользуемые сессии работы с командной строкой
Установить доверенным пользователям DCUI.Access для обхода запрета на вход	Запрет на вход отменяет возможность прямого доступа к ESXi-серверу, позволяя администратору управлять им только через vCenter Server. Однако в случае потери связи между ESXi-сервером и vCenter Server администратор утратит доступ к серверу и не сможет им управлять. Для предотвращения потери доступа к ESXi-серверу, который работает в режиме запрета на вход, установите DCUI.Access для списка доверенных пользователей, чтобы они могли обходить запрет на вход и получать доступ к DCUI
Настроить централизованное хранилище для сбора дампов памяти ESXi-сервера с помощью ESXi Dump Collector	В случае сбоя на ESXi-сервере для определения причины сбоя и пути решения проблемы необходимо проанализировать полученный при сбое дамп памяти. Настройка централизованного сбора дампов памяти гарантирует успешное сохранение и доступность файлов памяти в любой момент при неполадках на ESXi-сервере
Удалить ключи SSH из файла authorized_keys	Удаленный доступ к ESXi-серверу по протоколу SSH возможен без обязательной аутентификации пользователя. Для обеспечения доступа без ввода пароля скопируйте публичный ключ удаленного пользователя в файл /etc/ssh/keys-root/authorized_keys на ESXi-сервере. Присутствие публичного ключа пользователя в файле authorized_keys означает, что пользователь является доверенным, а значит, может получать доступ к серверу без ввода пароля. Режим запрета на вход не распространяется на суперпользователя root, если он подключается к серверу, используя файл, в котором хранятся авторизованные ключи. В этом случае суперпользователь root получает SSH-доступ к ESXi-серверу, даже если сервер работает в режиме запрета на вход

Политика	Описание
Проверка описаний и уровней поддерживаемости VIB-пакетов	Политика проверяет описание образа (Image Profile) дистрибутива ESXi-сервера, чтобы разрешать использование только подписанных VIB-пакетов. Отсутствие у VIB-пакета цифровой подписи свидетельствует о том, что на ESXi-сервере установлен непротестированный код. В описании образа ESXi-сервера может быть указан один из четырех уровней поддерживаемости (Acceptance Levels): 1) VMwareCertified — VIB-пакет был создан, протестирован и подписан VMware; 2) VMwareAccepted — VIB был создан партнером VMware, но протестирован и подписан VMware ; 3) PartnerSupported — VIB был создан, протестирован и подписан партнером VMware и 4) CommunitySupported — VIB не был протестирован VMware или ее партнером. VIB-пакеты в статусе CommunitySupported не имеют цифровой подписи и не поддерживаются. Чтобы защищать целостность и безопасность ESXi-серверов, не разрешайте устанавливать на них неподписанные VIB-пакеты (с уровнем поддерживаемости CommunitySupported)
Отключить передачу сообщений VIX API от виртуальной машины	VIX API — это библиотека для написания скриптов и программ для управления виртуальными машинами. Если в окружении не планируется специальная разработка с использованием этой библиотеки, то рекомендуется отключить некоторые функции, чтобы сократить возможности для использования уязвимостей. Отправка сообщений от ВМ на ESXi-сервер является одной из этих функций. Обратите внимание, что отключение этой функции не блокирует выполнение операций VIX API внутри гостевой ОС, так что определенные решения от компании VMware и продукты сторонних разработчиков, которые полагаются на эти функции, должны продолжать работать. Это устаревший интерфейс. Включение этого параметра предназначено только для Профиля 1, чтобы гарантировать, что любой устаревший интерфейс выключен для целей аудита
Отключение ненужных устройств	Политика гарантирует, что к виртуальной машине не подключены ненужные устройства, которые могут нести в себе риск потенциальной атаки. Например, последовательный и параллельный порты редко используются в дата-центрах, а CD/DVD-приводы обычно используются только в момент установки ПО. Соответствующие редко используемым устройствам параметры не должны присутствовать в конфигурационном файле либо должны иметь значение FALSE. Стоит отметить, что для функционирования разрешенных устройств в их свойствах должны быть определены дополнительные параметры
Доступ к консоли виртуальной машины по протоколу VNC	Консоль виртуальной машины позволяет подключиться к виртуальной машине аналогично локальному подключению к физическому серверу. Консоль ВМ также доступна по протоколу VNC. Для использования протокола VNC необходимо включить правила брандмауэра на каждом ESXi-сервере, где запускается виртуальная машина
Создание политики сложности паролей	ESXi-сервер использует подключаемый модуль pam_ passwdqc.so для настройки политики сложности паролей. Очень важно использовать пароли, которые нельзя просто подобрать с помощью различных генераторов паролей. Обратите внимание, что ESXi-сервер не накладывает никаких ограничений на пароль учетной записи root

Политика	Описание
Настройка брандмауэра ESXi-сервера для ограничения доступа к службам, работающим на сервере	Неограниченный доступ к службам, работающим на ESXi-сервере, может повлечь атаки на сервер извне и несанкционированный доступ к нему. Для снижения подобных рисков рекомендуется настроить брандмауэр ESXi-сервера, чтобы разрешить доступ только из доверенных сетей. Правила задаются в формате: Ruleset Name: 1.1.1.1, 2.2.2.2/24, 3.3.3.3
Отключение всех режимов, кроме VGA	Политика проверяет, что для видеокарт всех виртуальных машин ESXi-сервера включен режим VGA Only
Ограничение допустимого времени простоя сессии DCUI	DCUI (Direct Console User Interface) используется для локального доступа к ESXi-серверу и выполнения операций управления виртуальной инфраструктурой. Для предотвращения привилегированного доступа злоумышленника к ESXi-серверу все неактивные сессии должны завершаться по истечении определенного времени бездействия. Параметр UserVars.DcuiTimeOut позволяет автоматически завершать сессии по истечении заданного периода бездействия
Установка времени автоматического разблокирования учетной записи	Несколько неудачных попыток входа в систему с помощью одной учетной записи могут свидетельствовать о попытке перебора паролей или о попытке вызвать отказ в обслуживании. После превышения допустимого количества неудачных попыток входа в систему происходит блокирование учетной записи на некоторое время (120 секунд). Политика увеличивает время разблокирования учетных записей до 900 секунд
Ограничение количества неуспешных попыток входа в систему	Несколько неудачных попыток входа в систему с помощью одной учетной записи могут свидетельствовать о попытке перебора паролей или о попытке вызвать отказ в обслуживании. Чтобы это предотвратить, необходимо установить ограничение на количество неуспешных попыток ввода пароля. По умолчанию количество попыток ввода пароля равно 10. Данная политика делает максимальное количество неправильных попыток ввода пароля равным 3
Настройка безопасности Transparent Page Sharing	Политика включает дополнительные параметры безопасности Mem.ShareForceSalting при использовании технологии Transparent Page Sharing (TPS). По умолчанию TPS позволяет использование идентичных страниц памяти несколькими виртуальными машинами. Данная политика включает дополнительную проверку параметра sched.mem.pshare.salt в vmx-файле для предотвращения несанкционированного доступа к страницам памяти. По умолчанию параметр sched.mem.pshare.salt содержит уникальное для каждой ВМ значение vc.uuid. Таким образом будет запрещен доступ к идентичным страницам памяти для разных ВМ
Установка значения sched.mem.pshare.salt	При включенном параметре Mem.ShareForceSalting технологии Transparent Page Sharing в vmx-файле проверяется дополнительный параметр sched.mem.pshare.salt. Политика задает значение параметра sched.mem.pshare.salt, что позволяет разным виртуальным машинам использовать идентичные страницы памяти
Контроль целостности файлов конфигурации ESXi-сервера	Политика предназначена для запрета несанкционированных операций с файлами конфигурации ESXi -сервера путем контроля целостности данных файлов. Действие политики распространяется на выбранные файлы конфигурации (наборы файлов)

Политики безопасности ВМ

Виртуальным машинам могут назначаться следующие политики безопасности.

Политика	Описание
Доверенная загрузка виртуальных машин	Контролирует целостность базовой системы ввода-вывода ВМ и конфигурации ВМ. Блокирует запуск ВМ при нарушении целостности
Список запрещенных устройств	Ограничивает список устройств, доступных для подключения к ВМ, и контролирует модификацию уже добавленных устройств, тем самым обеспечивая контроль монтирования устройств к ВМ
Запрет клонирования виртуальных машин	Блокирует возможность клонирования ВМ
Запрет операций со снимками виртуальных машин	Блокирует возможность создания и удаления снимков (snapshots) ВМ, а также возврата к снимкам ВМ (revert to snapshot)
Запрет доступа к консоли виртуальной машины	Политика блокирует доступ к консоли виртуальной машины
Затирание остаточных данных на СХД при удалении ВМ	Политика обеспечивает автоматическое затирание файлов жестких дисков при удалении ВМ посредством однократной записи нулевых значений. Данная политика не работает для дисков ВМ, имеющих снимки (snapshots). Перед удалением ВМ необходимо удалить все ее снимки
Затирание остаточных данных на СХД при удалении ВМ (двукратная запись)	Политика обеспечивает автоматическое затирание файлов жестких дисков при удалении ВМ посредством двукратной записи нулевых значений. Данная политика не работает для дисков ВМ, имеющих снимки (snapshots). Перед удалением ВМ необходимо удалить все ее снимки

Политики безопасности сетевого адаптера

Физическому сетевому адаптеру pNIC может назначаться следующая политика безопасности.

Политика	Описание
Запрет смешивания разных типов сетевого трафика	Политика блокирует возможность подключения к виртуальному коммутатору группы сетевых портов с типом VMKernel

Политики безопасности распределенного виртуального коммутатора

Примечание. Назначение политик безопасности распределенному виртуальному коммутатору (distributed vSwitch) производится с помощью утилиты clacl.exe (см. стр.234).

Распределенному виртуальному коммутатору (distributed vSwitch) могут назначаться следующие политики безопасности.

Политика	Описание
Проверка соответствия параметра MAC Address Change значению Reject	Если операционная система виртуальной машины меняет MAC-адрес, то она может в любое время отправлять фреймы с подмененным начальным MAC-адресом. Это позволяет ей осуществлять вредоносные атаки на устройства в сети путем подмены сетевого адаптера, которому доверяет принимающая сеть. Данная политика предотвращает смену эффективного MAC-адреса виртуальной машиной, и это сказывается на программах, которым требуется такая функциональность, например, Microsoft Clustering, которая требует от систем эффективно разделять MAC-адрес. Также она повлияет на работу сетевого моста второго уровня и на программ, для лицензирования которых требуется привязка к определенному MAC-адресу. Чтобы обеспечить работу таких программ, нужно сделать исключение для группы портов, к которой они подключаются
Проверка соответствия параметра Forged Transmits значению Reject	Если операционная система виртуальной машины меняет MAC-адрес, то она может в любое время отправлять фреймы с подмененным начальным MAC-адресом. Это позволяет ей осуществлять вредоносные атаки на устройства в сети путем подмены сетевого адаптера, которому доверяет принимающая сеть. По умолчанию подложная передача данных (forged transmissions) разрешена. Это значит, что dvPortgroup не сравнивает начальный и эффективный MAC-адреса. Для предотвращения подмены MAC-адресов на всех виртуальных коммутаторах forged transmissions должны быть запрещены
Проверка соответствия параметра Promiscuous Mode значению Reject	Когда для группы портов активирован "неразборчивый" режим (Promiscuous Mode), все подключенные к ней виртуальные машины (и только те ВМ, которые подключены к этой группе портов) потенциально могут читать все пакеты в этой сети. По умолчанию "неразборчивый" режим отключен на ESXi-сервере и эта настройка является рекомендуемой. Однако существуют обоснованные причины его включить, например, для отладки, мониторинга или устранения неисправностей. Устройствам безопасности может быть необходима возможность читать все пакеты на виртуальном коммутаторе. Поэтому нужно сделать исключение для группы портов, к которой подключены такие программы, чтобы обеспечить возможность постоянного мониторинга трафика для этой группы портов. В отличие от стандартных виртуальных коммутаторов (vSwitches), коммутаторы dvSwitches разрешают "неразборчивый" режим только на уровне группы портов (dvPortgroup level)
Отключение опции autoexpand для группы портов VDS	Если используется политика no-unused-dvports, то на VDS должен быть только один набор портов, который действительно необходим. Функция Autoexpand для VDS dvPortgroups позволяет обойти это ограничение. Она позволяет добавить 10 портов vSphere Distributed Switch в группу портов, в которой закончились доступные порты. Есть риск того, что виртуальная машина, которая не должна относиться к этой группе портов, сможет злонамеренно или случайно нарушить конфиденциальность, целостность или подлинность данных других виртуальных машин на этой группе портов. Чтобы снизить риск неправомерного доступа к группе портов, опция VDS autoexpand должна быть отключена. Она отключена по умолчанию, но следует проводить регулярный мониторинг для подтверждения того, что это состояние не было изменено

Политики безопасности шаблона виртуальной машины

Шаблону виртуальной машины может назначаться следующая политика безопасности.

Политика	Описание
Контроль целостности шаблонов виртуальных машин	Политика предназначена для запрета несанкционированных операций с шаблонами виртуальных машин путем контроля целостности конфигураций и дисков шаблонов ВМ

Порядок настройки политик безопасности

Назначение политики объекту осуществляется следующим образом:

- на базе шаблонов формируются наборы политик (см. стр.**129**);
- набор политик назначается объекту (ESXi-серверу, ВМ, шаблону ВМ, сетевому адаптеру, виртуальной сети или хранилищу) или группе объектов.

Примечание. При назначении политики на ESXi-сервер проверки, осуществляемые этой политикой, начинают выполняться не сразу, а по истечении некоторого периода времени. Этот период задается на сервере авторизации в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate с помощью параметра VagentdCheckTimeout (в сек.). По умолчанию интервал равен 10 минутам. Также можно запустить проверку изменений политик вручную, нажав кнопку-ссылку "Проверить политики" на странице "Развертывание".

Информацию о статусе применения всех политик на защищаемых объектах, а также о возникновении ошибок можно получить с помощью отчета "Соответствие стандартам безопасности (подробно)" (см. стр.**175**). Подробную информацию об ошибке можно получить из соответствующего сообщения журнала событий (см. стр.**169**).

Если настройки в реестре были изменены, перед установкой/переустановкой компонента защиты ESXi-сервера нужно подождать минуту или перезагрузить службу управления vGate (rhuid.exe).

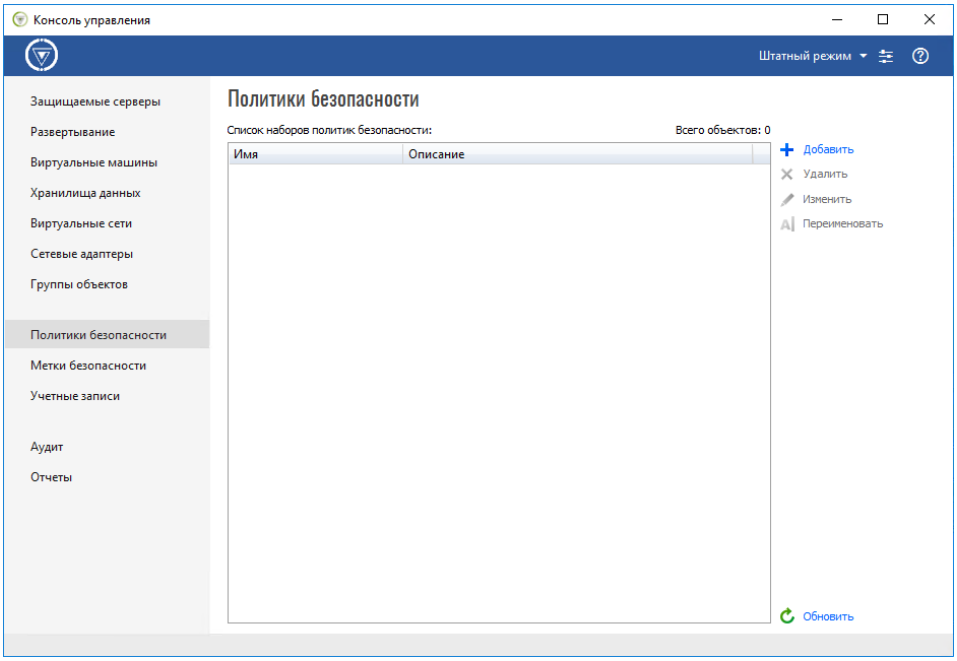
Формирование наборов политик

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.

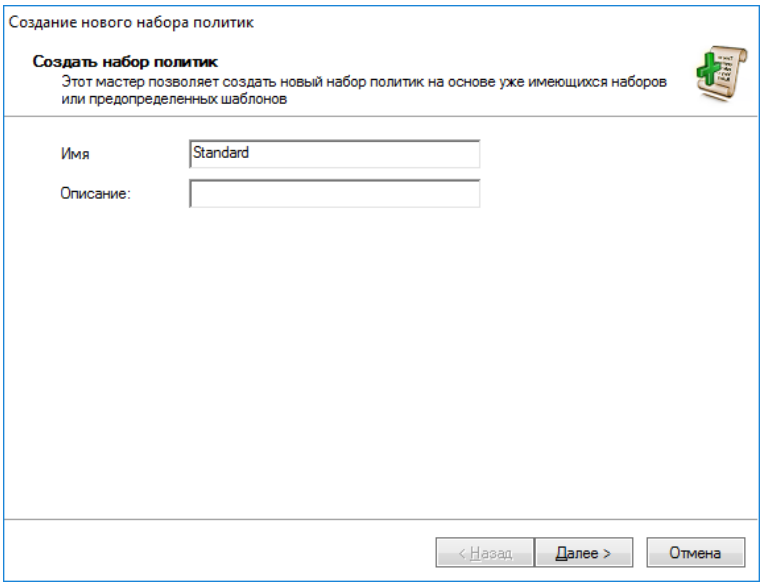
Кнопка	Описание
Добавить	Добавление нового набора политик (см. стр.**130**) или формирование на базе существующего (см. стр.**132**)
Удалить	Удаление выбранного набора политик
Изменить	Изменение настроек выбранного набора политик
Переименовать	Редактирование названия и описания выбранного набора

Добавление нового набора политик

Для добавления набора политик:

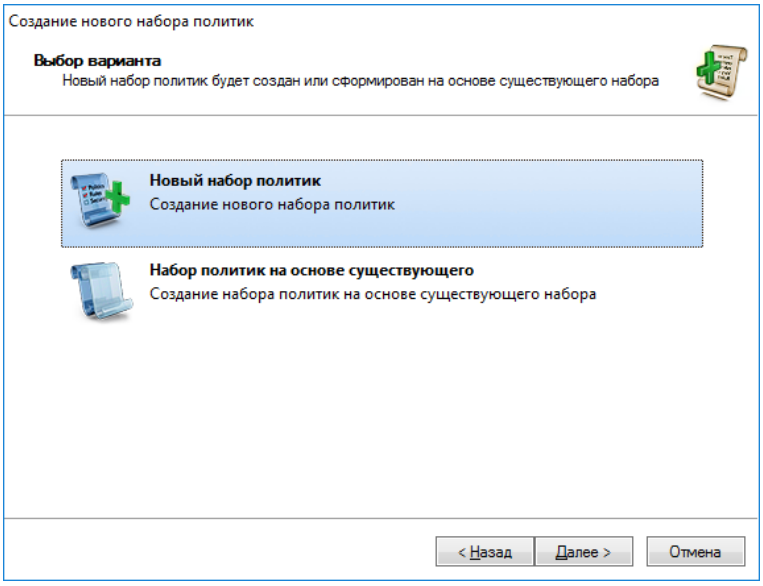
1. Нажмите кнопку-ссылку "Добавить".

   На экране появится следующий диалог.

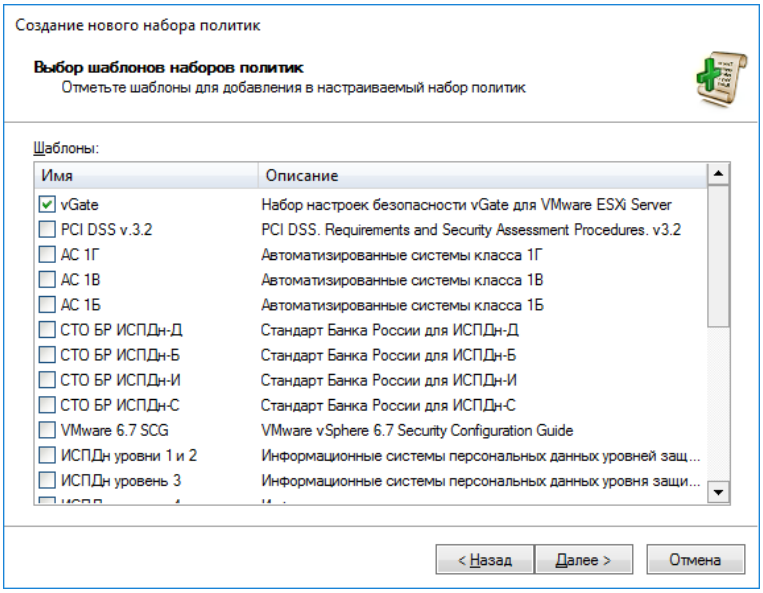


2. Укажите имя набора политик и описание (при необходимости). Нажмите кнопку "Далее".

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

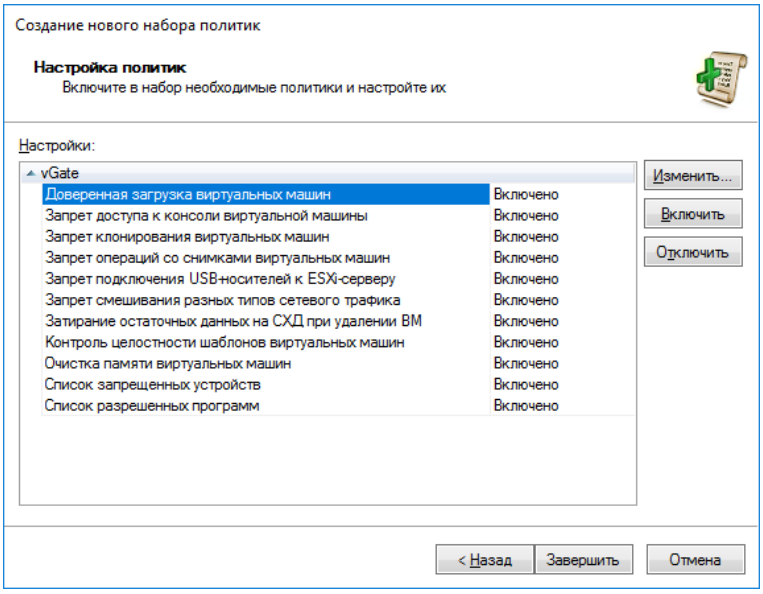


3. Выберите вариант "Новый набор политик" и нажмите кнопку "Далее".
   На экране появится диалог выбора шаблонов.



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.



Ненастроенные политики собраны в начале списка, а все остальные отсортированы по алфавиту.

Совет. Если набор формируется на основе нескольких шаблонов, то просмотреть, какие политики входят в тот или иной стандарт, можно в конце списка, дважды нажав нужный шаблон.

5. Настройте параметры политик (см. стр.**135**) и нажмите кнопку "Завершить".

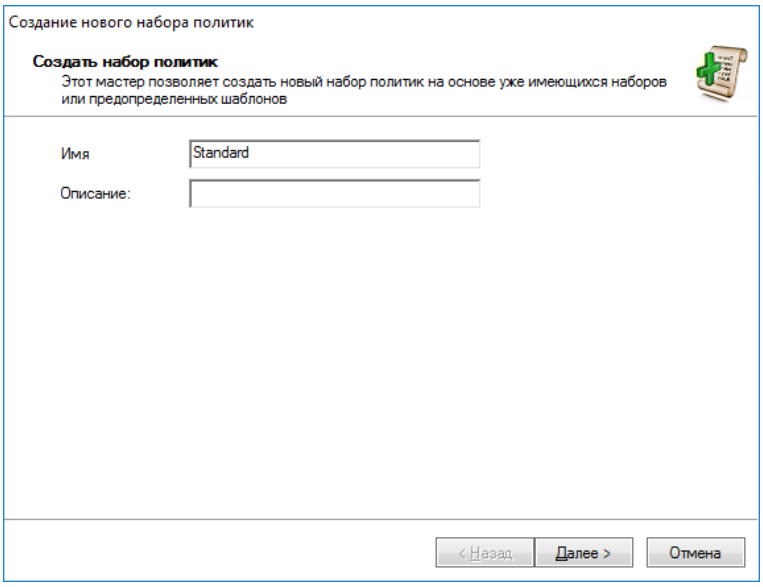
Примечание. До тех пор пока для всех политик со статусом "Не настроено" не будут настроены дополнительные параметры (см. стр.**230**), сохранить набор политик будет невозможно (на месте кнопки "Завершить" будет расположена недоступная кнопка "Далее").

Добавление набора политик на основе существующего

Для добавления набора политик:

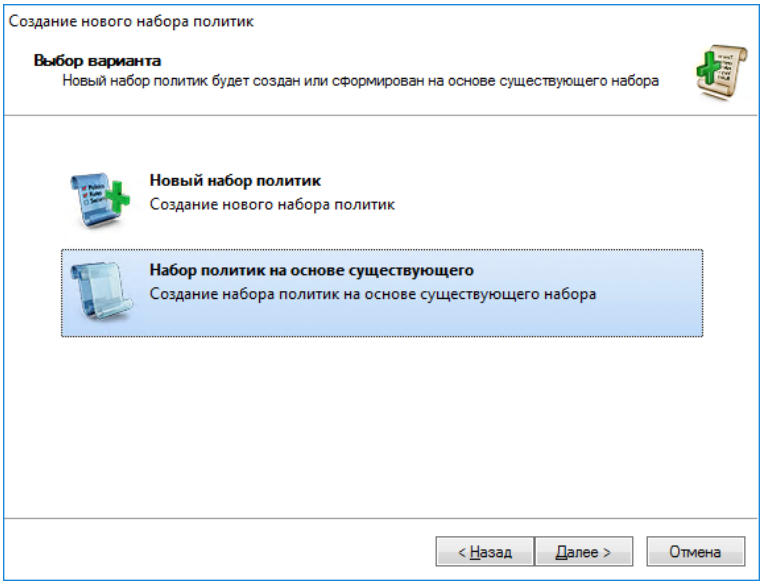
1. Нажмите кнопку-ссылку "Добавить".

   На экране появится следующий диалог.



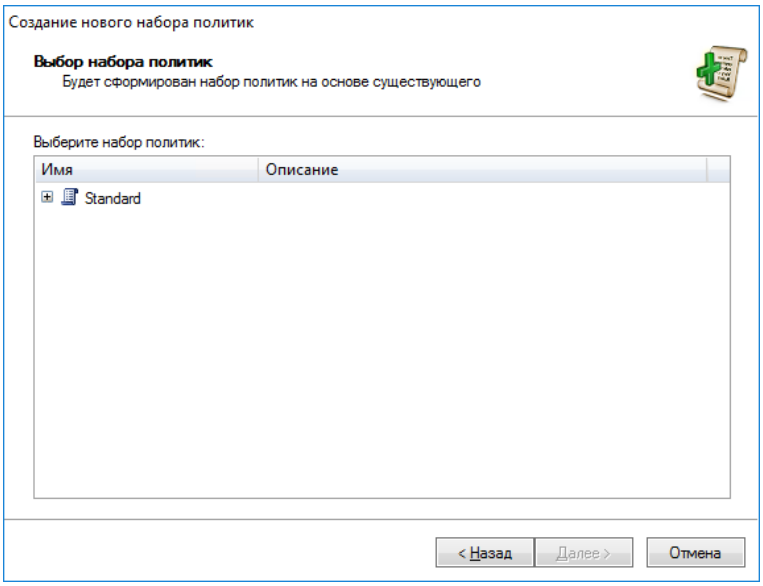
2. Укажите имя набора политик и описание (при необходимости). Нажмите кнопку "Далее".

   На экране появится диалог выбора варианта создания набора политик.



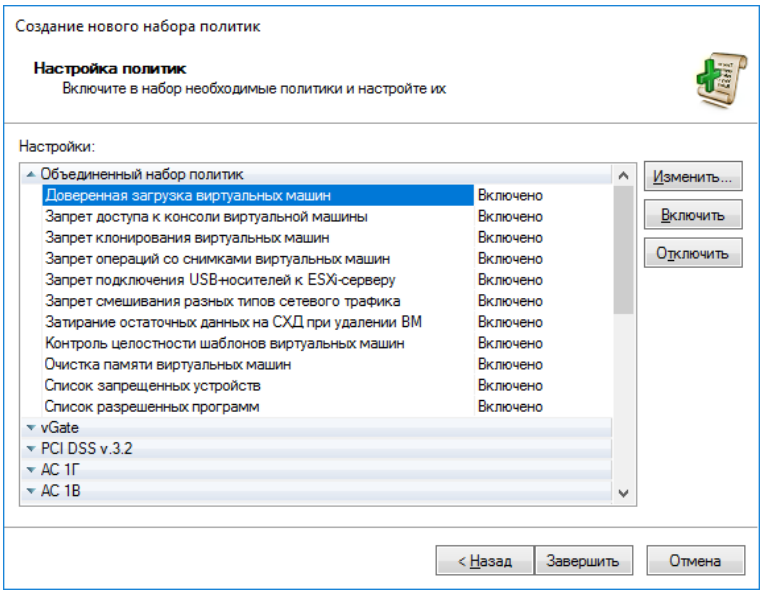
3. Выберите вариант "Набор политик на основе существующего" и нажмите кнопку "Далее".

   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 шаблонах стандартов безопасности.

Совет. Просмотреть, какие политики входят в тот или иной стандарт, можно в конце списка, дважды нажав нужный шаблон.

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

Примечание. До тех пор пока для всех политик со статусом "Не настроено" не будут настроены дополнительные параметры (см. стр.230), сохранить набор политик будет невозможно (на месте кнопки "Завершить" будет расположена недоступная кнопка "Далее").

Редактирование настраиваемых политик

Для некоторых политик безопасности, таких как "Список разрешенных программ", "Список запрещенных устройств", "Доверенная загрузка виртуальных машин" и т. д., можно настроить дополнительные параметры. Полный список настраиваемых политик и описание их параметров приведены в "Приложении" (см. стр.**230**).

Примечание. После включения некоторых политик может потребоваться перезагрузка ВМ или ESXi-сервера. Под перезагрузкой ВМ в данном случае понимается остановка ВМ (stop) с последующим запуском (start).

Для настройки параметров политики:

1. В диалоге "Создание нового набора политик" выберите нужную политику и нажмите кнопку "Изменить".

   На экране появится диалог настройки параметров политики.

   Внешний вид диалога зависит от перечня параметров, доступных для редактирования.

2. Отредактируйте параметры политики.

   Отметьте нужные пункты в диалоге настройки, укажите в полях диалога или выберите в раскрывающемся списке необходимые значения параметров.

   Совет. Если настройка параметра предусматривает возможность формирования списка из нескольких значений, используйте кнопки "Добавить" и "Удалить" для добавления и удаления элементов списка.

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

Редактирование набора политик

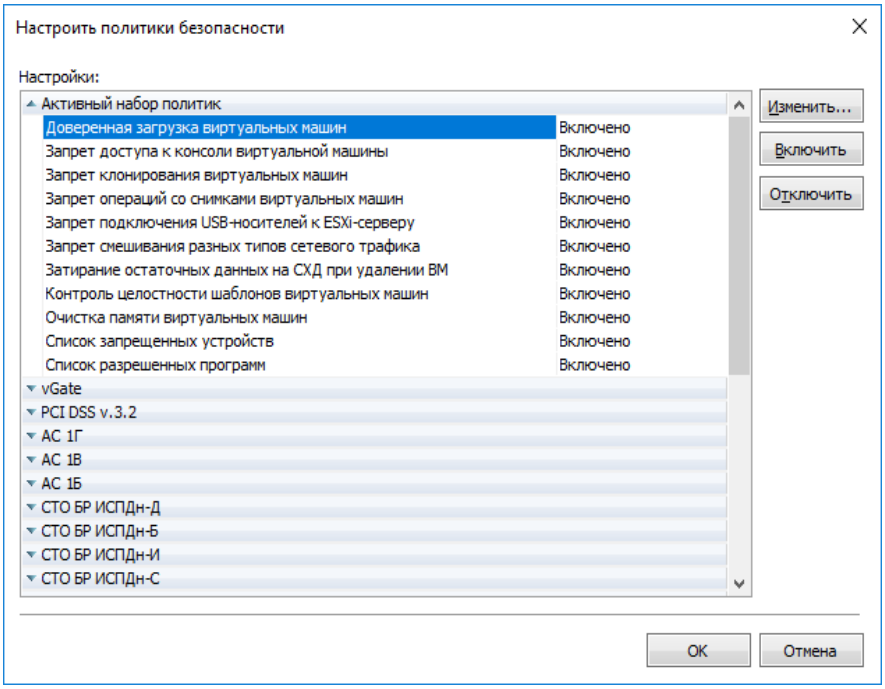
В наборе политик можно включить или отключить выбранную политику или сразу группу политик (выделив активный набор политик), а также изменить параметры политик.

Для большинства политик отключение с помощью консоли управления НЕ позволяет вернуть настройки ESXi-сервера 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 нужного шаблона и нажмите кнопку "Включить".

   Все политики безопасности, входящие в указанный шаблон, получат статус "Включено" (в том числе и в других шаблонах).

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

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

   В списке наборов политик будет обновлена информация о стандартах безопасности, которым соответствует отредактированный набор (о входящих в набор шаблонах).

Примечание. Если при редактировании набора были отключены политики, необходимые для защиты хотя бы по одному стандарту безопасности, в списке наборов политик для данного набора будет указан статус "Нет соответствий стандартам безопасности".

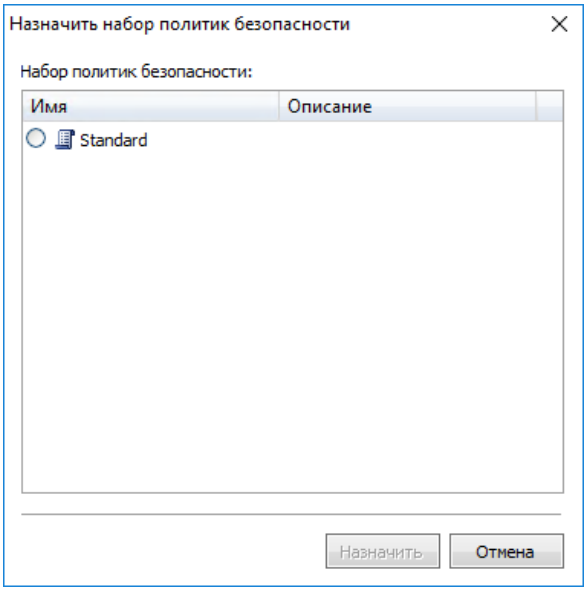
Назначение набора политик объекту или группе

Для назначения набора политик:

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

   Примечание. Для выбора шаблона виртуальной машины перейдите в раздел "Виртуальные машины" и нажмите кнопку-ссылку "Список" для отображения шаблонов.

   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:

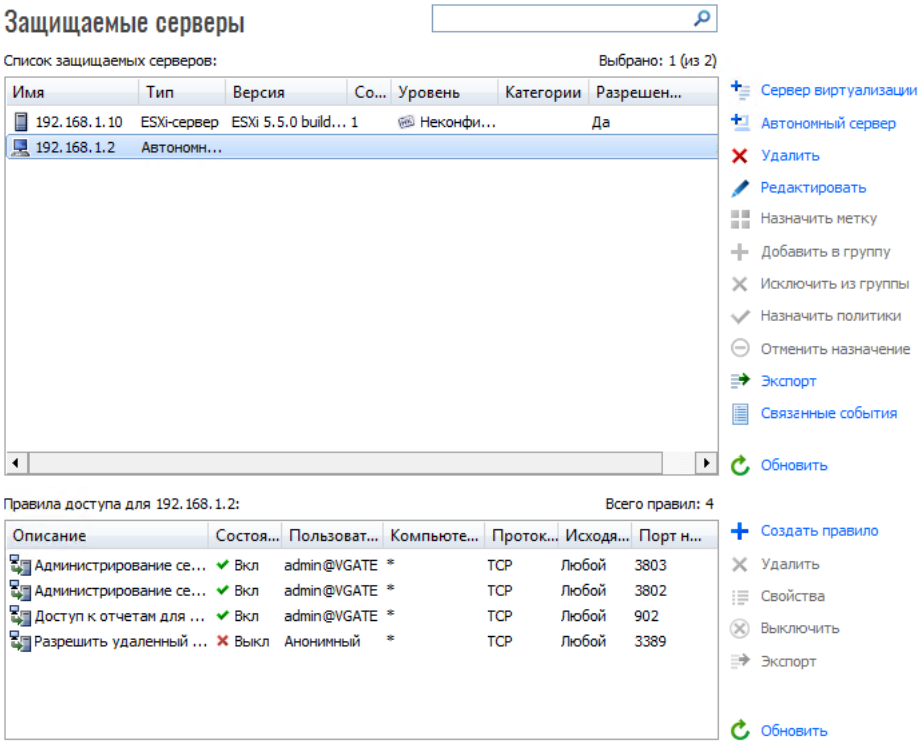
- зарегистрировать пользователей vGate (см. стр.**102**);
- при необходимости установить агенты аутентификации (см. стр.**13**) на компьютеры сервисных служб, которым требуются входящие соединения в защищаемый периметр для организации санкционированного доступа служб и сервисов компьютеров к защищаемым ESXi-серверам и другим узлам защищаемой сети.

Внимание! После предоставления пользователям доступа к защищаемым серверам необходимо перевести vGate из тестового в штатный режим работы (см. стр.**93**).

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.

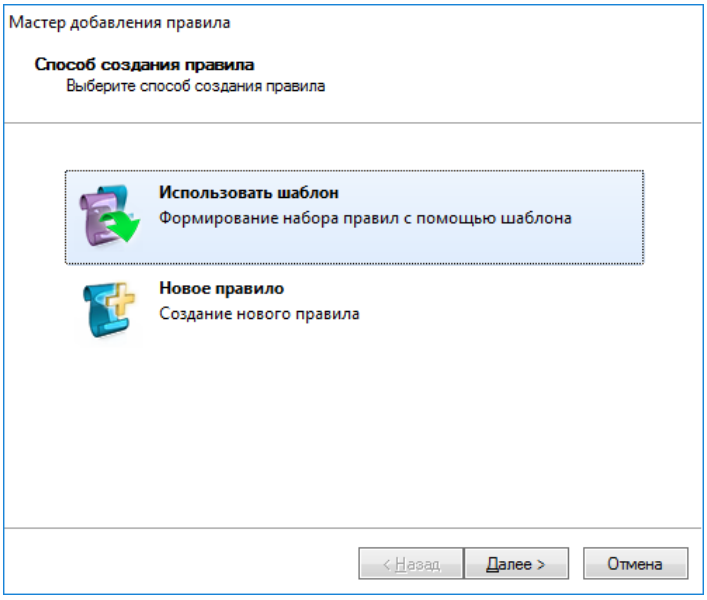


2. Выберите нужный сервер в таблице "Список защищаемых серверов".

   В нижней таблице отобразится список действующих правил.

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

   На экране появится диалог мастера добавления правила.

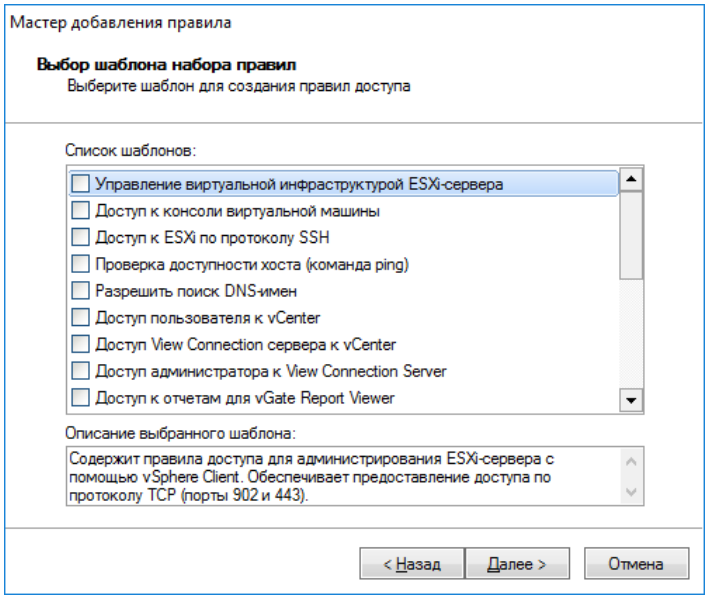


4. Выберите способ создания правила и нажмите "Далее >".

Способ	Описание
Использовать шаблон	Выбор готового набора правил из списка шаблонов, настроенных для разграничения доступа к различным объектам виртуальной инфраструктуры (см. стр.**139**)
Новое правило	Создание и ручная настройка нового правила (см. стр.**141**)

Создание правил на основе шаблона

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

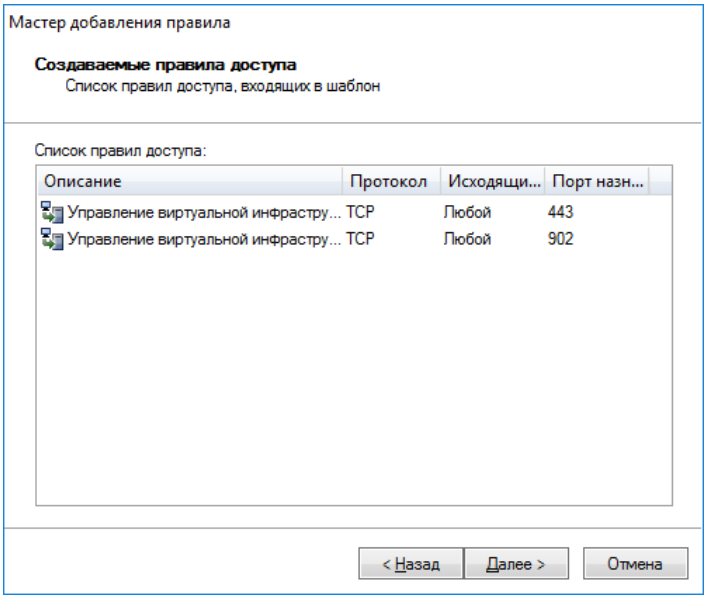


Примечание. Описание правил, входящих в каждый шаблон, приведено в приложении на стр.**223**.

Для создания правил по шаблону:

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

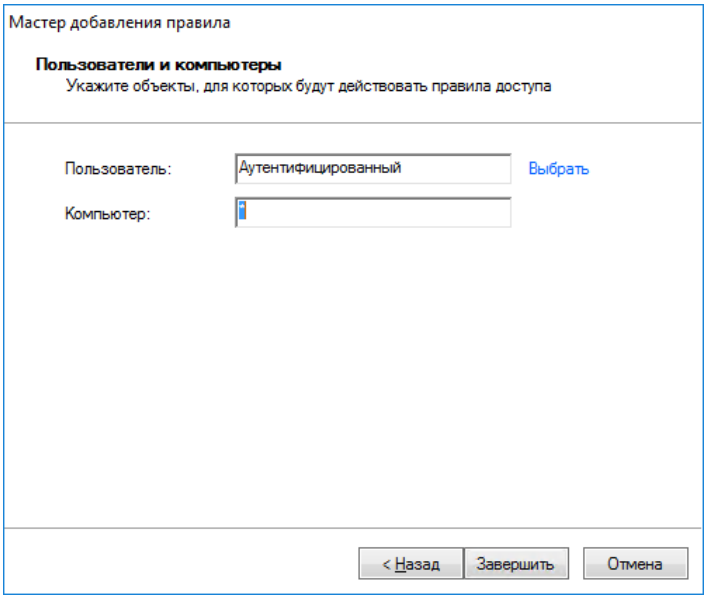
   На экране появится диалог со списком правил, входящих в выбранные шаблоны.



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.

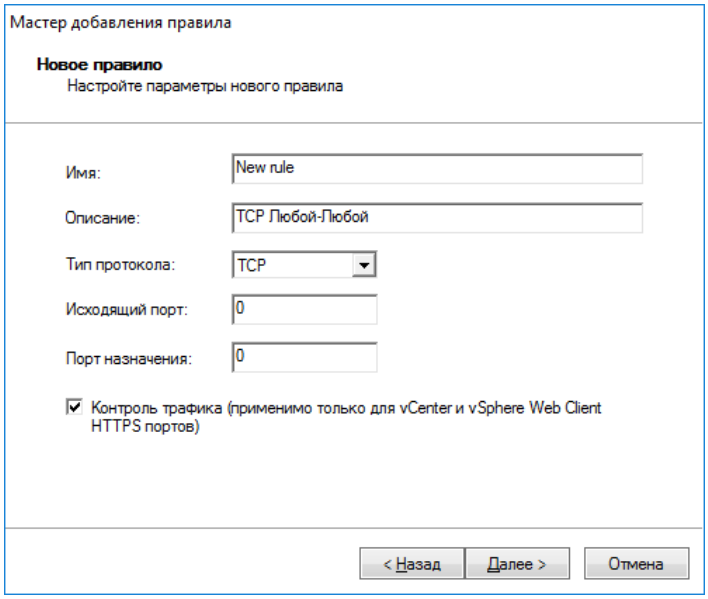
Параметр	Описание
Пользователь	Учетная запись пользователя или компьютера. Для выбора учетной записи нажмите кнопку-ссылку "Выбрать". В появившемся диалоге выберите зарегистрированную учетную запись. Если нужная учетная запись не зарегистрирована в консоли управления, то можно создать новую учетную запись, нажав кнопку "Создать" (см. стр.**104**), 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.

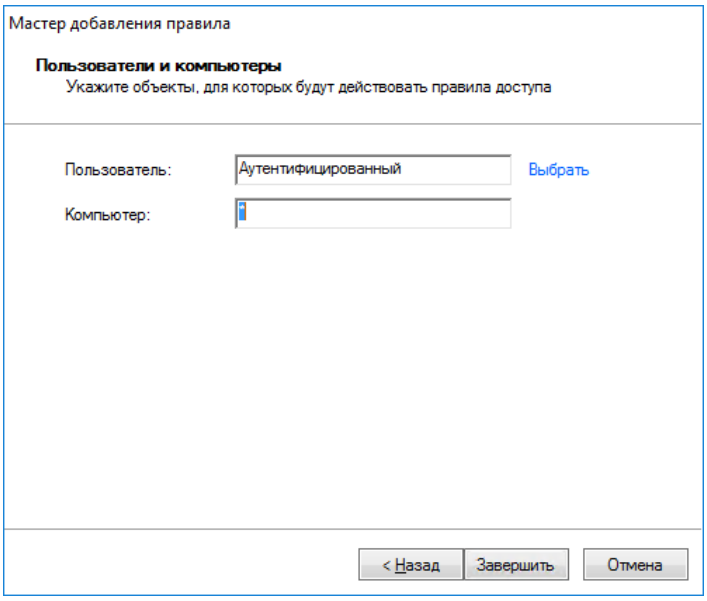


Для создания нового правила:

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
Контроль трафика	Удалите отметку из этого поля, если не требуется фильтрация HTTPS-трафика для защищаемого сервера vCenter. Если поле отмечено, то служба проксирования трафика vGate (vcp.exe) будет выполнять подробный анализ трафика для сервера vCenter при проходе трафика через сервер авторизации

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.**104**), 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.**234**).

3. Нажмите кнопку "Завершить".

Правило доступа будет добавлено в список.

Настройка правил фильтрации сетевых подключений к vCenter

Компонент защиты, устанавливаемый на vCenter, осуществляет фильтрацию входящего трафика.

По умолчанию после установки компонента всегда разрешены все исходящие и только следующие входящие соединения:

- доступ с сервера авторизации по протоколам TCP и ICMP по всем портам;
- доступ с любого компьютера по протоколу UDP по всем портам.

Эти основные правила фильтрации сетевых подключений отмечены в списке правил серым цветом и не могут быть удалены администратором. Помимо них в списке могут присутствовать правила для следующих соединений:

- доступ с любого IP-адреса на SOAP-порт VMware vSphere Update Manager (по умолчанию 8084), если служба установлена на vCenter;
- доступ с любого IP-адреса на порт 3389 по протоколу RDP, если на vCenter включена возможность удаленного подключения рабочего стола;
- доступ с любого компьютера по протоколу ICMP (команда ping).

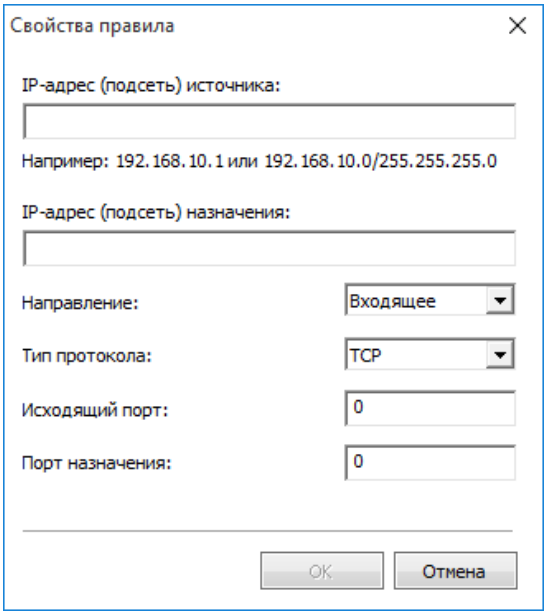
Внимание! При необходимости разрешить доступ к vCenter с какого-либо иного направления следует добавить правила фильтрации сетевых соединений в консоли управления vGate.

Для создания правила фильтрации сетевых подключений:

1. В разделе "Развертывание" выберите сервер vCenter, для которого требуется создать правило фильтрации сетевых подключений.

   В нижней таблице отобразится список действующих правил.

2. Для создания правила нажмите кнопку-ссылку "Создать правило".
   На экране появится диалог создания правила.



3. Укажите значения параметров правила и нажмите кнопку "OK".

Параметр	Описание
IP-адрес (подсеть) источника	IP-адрес сервера, которому будет предоставлен доступ к vCenter, или адрес подсети, если необходимо разрешить входящие соединения со всех серверов этой подсети. Поле активно, если выбрано входящее направление трафика
IP-адрес (подсеть) назначения	IP-адрес сервера, к которому будет разрешено подключаться серверу vCenter, или адрес подсети, если необходимо разрешить исходящие соединения для всех серверов этой подсети. Поле активно, если выбрано исходящее направление трафика
Направление	Направление сетевого трафика, для которого действует правило (входящее или исходящее)
Тип протокола	Тип протокола соединения: TCP, UDP, ICMP или IP-level (номер IP-протокола на сетевом уровне)
Исходящий порт	Исходящий порт на сервере, с которого выполняется подключение к vCenter. Для соединения по любому порту выберите значение "0"
Порт назначения	Порт назначения на сервере vCenter. Для соединения по любому порту выберите значение "0"

Правило доступа будет добавлено в список.

Для удаления правила выберите его в списке и нажмите кнопку-ссылку "Удалить". Для редактирования параметров правила — нажмите кнопку-ссылку "Свойства".
Для создания правил фильтрации сетевых подключений к vCenter также можно воспользоваться утилитой командной строки drvmgr.exe (см. стр. 238).

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. 84);

- назначаются метки безопасности учетным записям пользователей и ресурсам (объектам виртуальной инфраструктуры) или группам объектов (см. стр.**112**).

Примечание. О настройке перечня типов объектов, для которых будет действовать механизм полномочного управления доступом (для которых будет проверяться соответствие меток безопасности), см. стр.**87**.

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. **84**). Кроме того, можно изменить список допустимых категорий конфиденциальности под свои задачи (подробнее о настройке списка категорий см. стр.**116**).

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.**117**).

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: ESXi-серверы введены в эксплуатацию, подключены физические сетевые адаптеры, настроены хранилища, но ВМ еще не созданы;
- виртуальная инфраструктура используется: на ESXi-серверах запущены ВМ.

На стр.**151** 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 ESXi-серверов в соответствии с уровнем конфиденциальности информации, которая будет обрабатываться на нем. Если на ESXi-сервере планируется обрабатывать информацию разных уровней конфиденциальности, то:
   - отметьте поле "Разрешено исполнять ВМ с меньшим уровнем";
   - задайте уровень конфиденциальности ESXi-сервера, равный максимальному уровню конфиденциальности обрабатываемой на нем информации.
3. Задайте уровень конфиденциальности каждому физическому сетевому адаптеру ESXi-сервера. Уровень конфиденциальности каждого из физических сетевых адаптеров ESXi-сервера должен быть не выше уровня конфиденциальности этого сервера. Если через один физический сетевой адаптер будет проходить трафик с VLAN разных уровней конфиденциальности, то отметьте поле "Разрешен трафик для VLAN с меньшим уровнем".

   Примечание. Сценарий работы функции при смешивании трафика с VLAN разных уровней конфиденциальности на физическом адаптере считается менее безопасным.
4. Если планируется использовать виртуальные сети (VLAN), добавьте их в консоли управления (см. стр. **148**) и назначьте уровень конфиденциальности каждой из них. Уровень конфиденциальности VLAN должен быть:
   - не больше уровня конфиденциальности физического сетевого адаптера, к которому она подключена (если поле "Разрешен трафик для VLAN с меньшим уровнем" отмечено);
   - равен уровню конфиденциальности физического сетевого адаптера, к которому она подключена (если поле "Разрешен трафик для VLAN с меньшим уровнем" не отмечено).

   Если уровень конфиденциальности физического сетевого адаптера отличен от значения "неконфиденциально" и VLAN не планируется использовать, то:
   - в список виртуальных сетей (в консоли управления) добавьте VLAN с ID=0;
   - задайте для добавленной VLAN уровень конфиденциальности, равный уровню конфиденциальности физического сетевого адаптера.
5. 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 **6**.
6. Задайте уровни конфиденциальности для всех существующих ВМ. Уровень конфиденциальности ВМ должен быть:
   - не выше уровня конфиденциальности ESXi-сервера, на котором она выполняется (если в настройках уровня конфиденциальности сервера отмечено поле "Разрешено исполнять ВМ с меньшим уровнем"), или равен уровню ESXi-сервера (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).

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

Совет. При выполнении операций с виртуальными машинами можно выбрать один из двух способов отображения ВМ: в виде простого списка или в виде дерева, соответствующего иерархии виртуальной инфраструктуры vSphere. Для переключения между режимами используйте кнопки-ссылки "Список" и "Иерархия".

Примечание. При создании новой ВМ с несколькими сетевыми картами проверяется соответствие уровней конфиденциальности ВМ, сетевых карт, VLAN 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 (ESXi-серверы, хранилища виртуальных машин, физические сетевые адаптеры, виртуальные сети), 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 ESXi-серверов в соответствии с категорией конфиденциальности информации, которая будет обрабатываться на нем. Если на ESXi-сервере будет обрабатываться информация разных категорий, то задайте список из этих категорий.
3. Задайте категорию конфиденциальности каждому физическому сетевому адаптеру ESXi-сервера. При этом список категорий каждого из физических сетевых адаптеров должен иметь хотя бы одну общую категорию со списком категорий ESXi-сервера.
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. При этом список категорий каждой из сетей должен иметь хотя бы одну общую категорию со списком категорий физического сетевого адаптера.
5. Задайте категории конфиденциальности каждому из хранилищ ВМ, равные категориям конфиденциальности хранящейся на них информации. При этом список категорий конфиденциальности хранилища должен содержать хотя бы одну категорию из списка категорий конфиденциальности каждого из ESXi-серверов.

   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 **6**.

6. Задайте категории конфиденциальности для всех существующих ВМ. Список категорий ВМ должен иметь хотя бы одну общую категорию:
   - со списком категорий ESXi-сервера, на котором она выполняется;
   - со списком категорий хранилища, на котором хранятся файлы ВМ.

Совет. При выполнении операций с виртуальными машинами можно выбрать один из двух способов отображения ВМ: в виде простого списка или в виде дерева, соответствующего иерархии виртуальной инфраструктуры vSphere. Для переключения между режимами используйте кнопки-ссылки "Список" и "Иерархия".

Примечание. При создании новой ВМ с несколькими сетевыми картами проверяется соответствие категорий конфиденциальности ВМ, сетевых карт, VLAN 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 (ESXi-серверы, хранилища виртуальных машин, физические сетевые адаптеры, виртуальные сети), а также новым учетным записям пользователей.

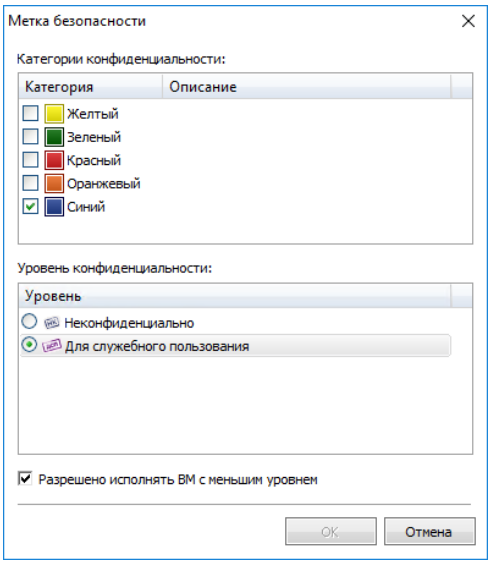
Назначение меток безопасности

Внимание! Перед назначением меток безопасности виртуальным сетям (VLAN) следует добавить их в список виртуальных сетей в консоли управления (см. стр.149).

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 ESXi-серверов
Разрешено хранить ВМ с меньшим уровнем	Дополнительный параметр для хранилищ
Разрешено подключаться к сетям с меньшим уровнем	Дополнительный параметр для ВМ
Разрешен трафик для VLAN 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.

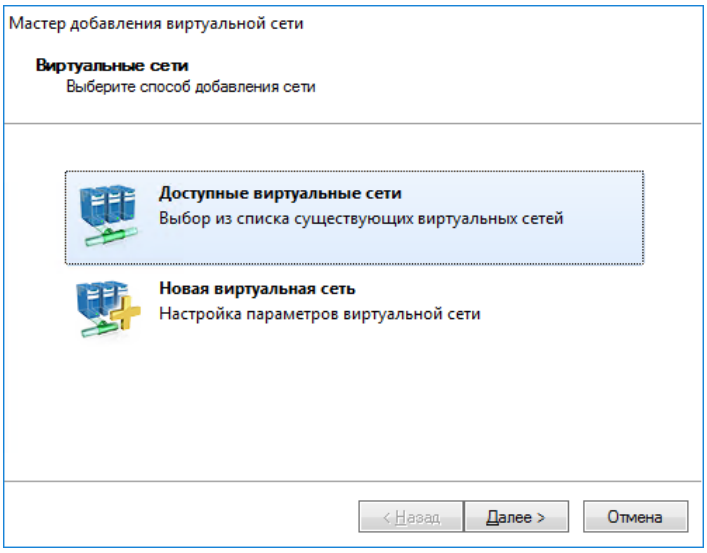
Особенности назначения меток виртуальным сетям

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".

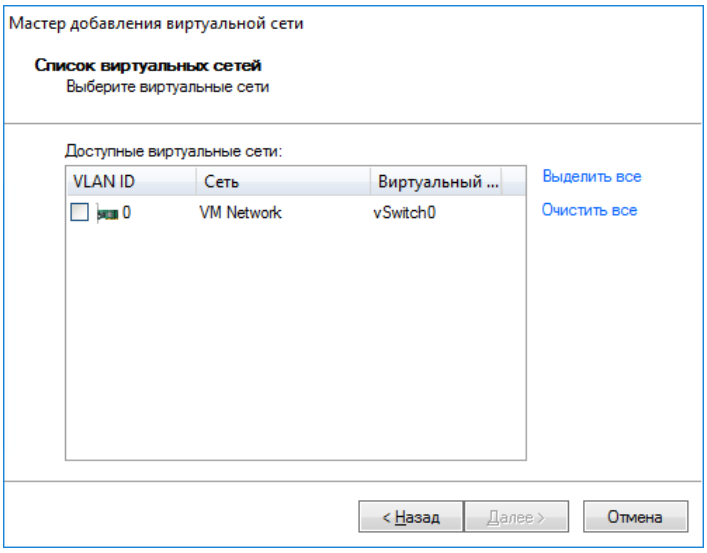
   На экране появится следующий диалог.



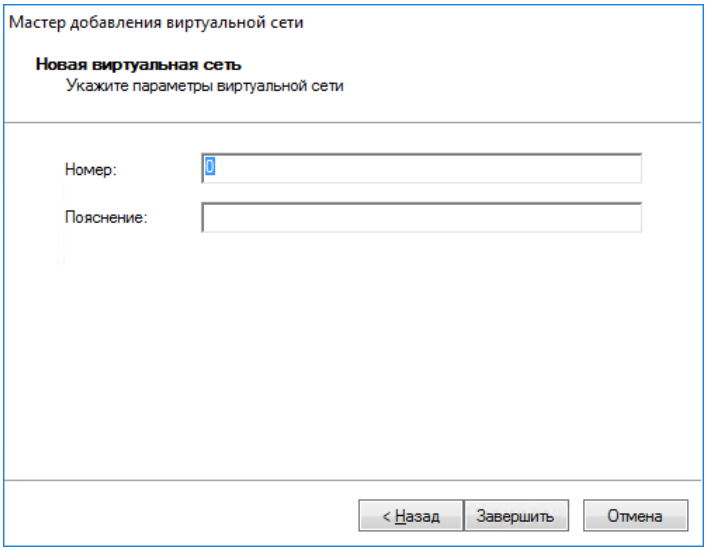
2. Выберите способ добавления виртуальной сети и нажмите "Далее >".

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

ESXi-сервер имеет физический сетевой адаптер — pNIC с уровнем конфиденциальности "для служебного пользования", который одновременно подключен к VLAN 1 и VLAN 2. VLAN 1 имеет уровень конфиденциальности "неконфиденциально", VLAN 2— "для служебного пользования". Поэтому для pNIC задан дополнительный параметр "Разрешен трафик для VLAN с меньшим уровнем".

На ESXi-сервере запущены три виртуальные машины:

- на ВМ 1 находится неконфиденциальная информация;
- ВМ 2 является сторонним межсетевым экраном, который разграничивает доступ между сетями разного уровня конфиденциальности;
- на ВМ 3 находится конфиденциальная информация.

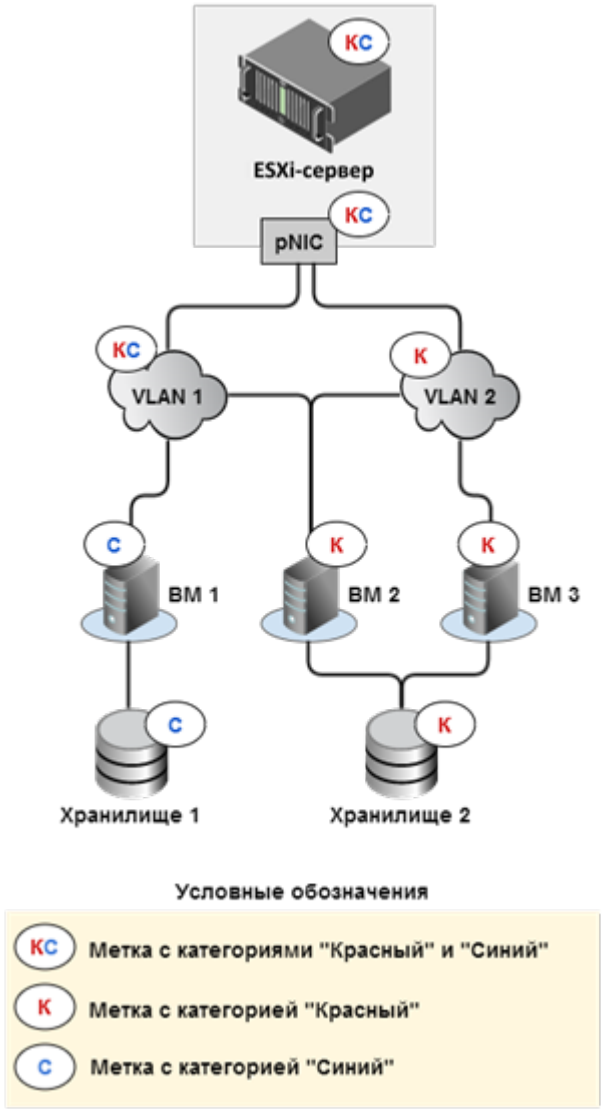
ВМ 1 и ВМ 3 назначен уровень конфиденциальности в соответствии с уровнем информации, которая на них находится ("неконфиденциально" и "для

служебного пользования" соответственно). ВМ 2 назначен уровень конфиденциальности, соответствующий максимальному уровню конфиденциальности находящейся на ней информации, т. е. "для служебного пользования". Кроме того, для ВМ 2 задан дополнительный параметр "Разрешено подключаться к сетям с меньшим уровнем".

Для хранения файлов ВМ используется хранилище с уровнем конфиденциальности "для служебного пользования". Поскольку в хранилище находятся файлы ВМ разного уровня конфиденциальности, то хранилищу назначен дополнительный параметр "Разрешено хранить ВМ с меньшим уровнем".

Пример 2. Использование категорий конфиденциальности

На рисунке приведен пример назначения категорий конфиденциальности объектам виртуальной инфраструктуры.



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

ESXi-сервер имеет физический сетевой адаптер — pNIC, который имеет одновременное подключение к виртуальным сетям VLAN 1 и VLAN 2. При этом в виртуальной сети VLAN 1 обрабатываются данные категорий "Синий" и "Красный", в VLAN 2 обрабатываются данные только категории "Красный". Поэтому для pNIC и VLAN 1 назначен список из категорий "Синий" и "Красный", а для VLAN 2 задана категория конфиденциальности "Красный".

На ESXi-сервере запущены три виртуальные машины:

- на ВМ 1 находится информация категории "Синий";
- ВМ 2 является сторонним межсетевым экраном, который разграничивает доступ между сетями разных категорий конфиденциальности и содержит информацию категории "Красный";
- на ВМ 3 находится информация категории "Красный".

Для хранения файлов разных категорий конфиденциальности используются два хранилища: Хранилище 1 с категорией конфиденциальности "Синий" и Хранилище 2 с категорией конфиденциальности "Красный".

Настройка исключений полномочного управления доступом

В vGate предусмотрена возможность настройки исключений полномочного управления доступом для определенных типов объектов виртуальной инфраструктуры. Объекты, для которых не требуется разграничение доступа на основании меток безопасности, следует добавить в список исключений с помощью утилиты clacl.exe.

Для создания списка исключений:

- Откройте редактор командной строки и выполните следующую команду:

  ```
  clacl.exe smarkers set-trumps –t <типы объекта> -k admin -s pAsswor1d
  ```

  где

  - **<тип объекта>** — тип объекта виртуальной инфраструктуры, для которого устанавливается исключение:
    - **A** — сетевой адаптер;
    - **D** — DVSwitch;
    - **E** — ESXi-сервер;
    - **N** — виртуальная сеть;
    - **S** — дисковое хранилище;
    - **U** — пользователь;
    - **V** — виртуальная машина;
  - **admin** — имя АИБ;
  - **pAsswor1d** — пароль АИБ.

Пример:

```
clacl.exe smarkers set-trumps –t ADN -k admin@VGATE -s 1
```

Для просмотра текущего списка исключений:

- Откройте редактор командной строки и выполните следующую команду:

  clacl.exe smarkers get-trumps -k **admin** -s **pAsswor1d**

  где

  - **admin** — имя АИБ;
  - **pAsswor1d** — пароль АИБ.

Пример:

```
clacl.exe smarkers get-trumps -k admin@VGATE -s 1
Network Adapter, VLAN, DVSwitch
Done.
```

Для очистки списка исключений:

- Откройте редактор командной строки и выполните следующую команду:

  ```
  clacl.exe smarkers set-trumps -t "" -k admin -s pAsswor1d
  ```

  где

  - **admin** — имя АИБ;

- **pAsswor1d** — пароль АИБ.

Пример:

```
clacl.exe smarkers set-trumps -t "" -k admin@VGATE -s 1
```

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 следующими способами:

- свойством учетной записи "Пользователь виртуальных машин" (см. стр.**102**);
- политикой безопасности "Запрет доступа к консоли виртуальной машины";
- 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.**104**).

АИБ может запретить использование консоли на отдельных ВМ для всех пользователей. Для этого предназначена политика безопасности "Запрет доступа к консоли виртуальной машины" (см. стр.**126**) из шаблона "vGate". Если данная политика назначена на ВМ, то доступ пользователя к консоли данной ВМ будет невозможен даже при наличии права "Пользователь виртуальных машин".

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.

Примеры настройки доступа к консоли ВМ

1. Пользователь обладает правом доступа "Пользователь виртуальных машин" и на ВМ не назначена политика "Запрет доступа к консоли виртуальной машины".

   При попытке пользователя получить доступ к консоли ВМ консоль будет открыта.

2. Пользователь обладает правом доступа "Пользователь виртуальных машин" и на ВМ назначена политика "Запрет доступа к консоли виртуальной машины".

   При попытке пользователя получить доступ к консоли ВМ консоль открыта не будет. В журнале аудита появится сообщение об отказе в выполнении операции из-за нарушения политик безопасности.

3. Пользователь не обладает правом доступа "Пользователь виртуальных машин" и на ВМ назначена политика "Запрет доступа к консоли виртуальной машины".

   При попытке пользователя получить доступ к консоли ВМ консоль открыта не будет. В журнале аудита появится сообщение об отказе в выполнении операции из-за недостатка привилегий.

4. Пользователь не обладает правом доступа "Пользователь виртуальных машин" и на ВМ не назначена политика "Запрет доступа к консоли виртуальной машины".

   При попытке пользователя получить доступ к консоли ВМ консоль открыта не будет. В журнале аудита появится сообщение об отказе в выполнении операции из-за недостатка привилегий.

Контроль целостности

Объекты и методы контроля

В vGate средства контроля целостности (КЦ) используются для защиты следующих объектов на сервере авторизации, ESXi-серверах 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

Компонент	Объект контроля	Параметры и методы контроля
ESXi-сервер	Файлы ВМ	Контролируются: • *.vmx — основной конфигурационный файл ВМ; • *.nvram — файл конфигурации BIOS (bin-файл); • *.vmsd — файл конфигурации снимков ВМ (snapshot). Перечень контролируемых файлов и параметров файла VMX задается в настройках политики "Доверенная загрузка виртуальных машин" (см. стр.**158**). Контроль целостности производится в момент старта ВМ, а также службой компонента защиты vGate на ESXi-сервере (vagentd) через заданный интервал времени. Контрольные суммы файлов хранятся централизованно, в базе данных, для каждой виртуальной машины. Интервал проверки задается на ESXi-сервере в конфигурационном файле /etc/config/vgate/vgate.cfg, секция vagentd, параметр interval (в сек.). По умолчанию интервал равен 600 сек.
	Файлы шаблонов ВМ	Контролируются: • *.vmtx — файл шаблона ВМ; • *.nvram — файл конфигурации BIOS (bin-файл); • *.vmdk — файл образа виртуального диска шаблона; • *flat.vmdk — файл данных виртуальной машины. Перечень контролируемых файлов и параметров файла задается в настройках политики "Контроль целостности шаблонов виртуальных машин" (см. стр.**158**). Контроль целостности производится службой компонента защиты vGate на ESXi-сервере (vagentd) через заданный интервал времени. Контрольные суммы файлов хранятся централизованно, в базе данных, для каждого шаблона виртуальной машины. Интервал проверки задается на сервере авторизации в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Security Code\vGate с помощью параметра VagentdTemplateCheckTimeout (в сек.). По умолчанию интервал равен 1800 сек. Если настройки в реестре были изменены, перед установкой/переустановкой компонента защиты ESXi-сервера нужно подождать минуту или перезагрузить службу управления vGate (rhuid.exe)

Компонент	Объект контроля	Параметры и методы контроля
	Файлы конфигурации	Контролируются файлы конфигурации ESXi-сервера. Возможен контроль следующих файлов: • загрузочные сектора; • файлы конфигурации загрузчика; • образ начальной загрузки • файлы сетевой конфигурации; • файлы контроля ОС; • файлы каталогов /bin, /lib, /usr/lib; • файлы SSH; • файлы конфигурации времени; • сертификаты; • файлы пользовательских записей. Проверка КС осуществляется каждые 10 минут, по запросу пользователя или при выполнении следующих операций с ESXi-сервером: • Power On; • Shut Down; • Reboot; • Enter Standby Mode
Сервер vCenter	Исполняемые модули vGate	Как на сервере авторизации, за исключением остановки службы аутентификации vGate (aupa.exe) из-за нарушения КЦ
vCSA	Файлы конфигурации	Контролируются файлы конфигурации vCSA. Возможен контроль следующих файлов: • файлы VMware; • файлы каталогов /bin, /lib, /usr/lib. Проверка КС осуществляется каждые 10 минут, по запросу пользователя или при выполнении следующих операций с vCSA: • Power On; • Shut Down; • Suspend; • Reset

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".

Настройка объектов контроля

vGate позволяет выполнить детальную настройку контроля целостности ВМ:

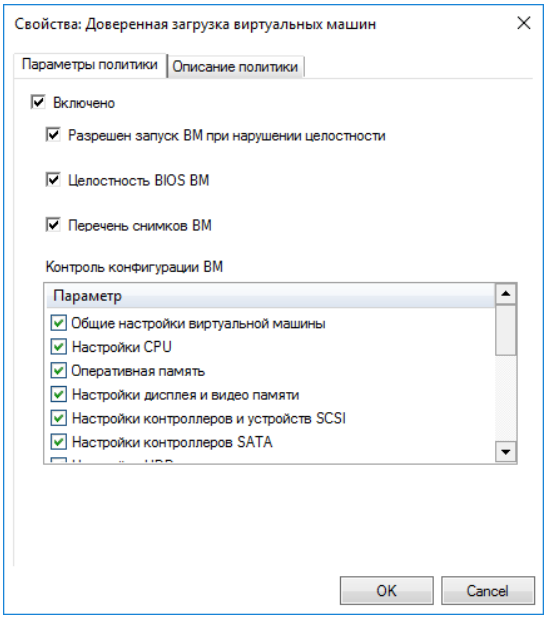
- разрешить или запретить запуск ВМ при нарушении целостности конфигурации;
- выбрать файлы конфигурации ВМ (файлы VMX, NVRAM, VMSD), для которых будет осуществляться проверка соответствия контрольных сумм;
- выбрать параметры конфигурации ВМ (параметры VMX-файла), изменение значений которых будет контролироваться политикой "Доверенная загрузка виртуальных машин".

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

Для настройки параметров политики:

1. Выберите политику "Доверенная загрузка виртуальных машин" 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
Целостность BIOS ВМ	По умолчанию данный пункт отмечен. Удалите отметку, чтобы выключить контроль целостности файлов конфигурации BIOS (файлов NVRAM)
Перечень снимков ВМ	По умолчанию данный пункт отмечен. Удалите отметку, чтобы выключить контроль целостности файлов конфигурации снимков ВМ (файлов VMSD)
Контроль конфигурации ВМ	Список параметров конфигурации ВМ (атрибутов VMX-файла), контролируемых политикой (подробнее о соответствии контролируемых параметров и конкретных атрибутов VMX-файла см. ниже). Удалите отметку в нужной строке списка, чтобы отменить контроль за изменением значений соответствующего свойства ВМ

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

Внимание! Для всех виртуальных машин, которым назначена политика "Доверенная загрузка виртуальных машин", блокируются операции удаления и конвертации ВМ в шаблон.

Внимание! При редактировании параметров политики "Доверенная загрузка виртуальных машин" нужно повторить назначение данной политики виртуальной машине. При конвертации виртуальной машины в шаблон для контроля целостности полученного шаблона нужно назначить ему политику "Контроль целостности шаблонов виртуальных машин" (см. стр.**162**).

Расчет контрольных сумм

Целостность ВМ контролируется компонентами защиты, установленными на ESXi-сервер (см. стр.**100**).

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.**165**), иначе будет зафиксировано нарушение целостности.

Контроль изменений и статус ВМ

На ESXi-сервере 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.

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.**165**). 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 vGateAdmin.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.**169**). 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
Изменен VMX-файл	VMX-файл был изменен. Можно выполнить согласование или отклонение изменений

Контролируемые атрибуты VMX-файла

Политика "Доверенная загрузка виртуальных машин" может быть настроена для контроля параметров VMX-файла (отмечены один или несколько пунктов в списке "Контроль конфигурации ВМ", см. стр.**158**). В этом случае при проверке изменений параметров ВМ сравниваются не только контрольные суммы файлов конфигурации, но и значения отдельных атрибутов VMX-файла. Проверка изменения значений выполняется для набора предопределенных атрибутов и атрибутов, соответствующих регулярному выражению.

В таблице ниже перечислены параметры политики "Доверенная загрузка виртуальных машин" и соответствующие им атрибуты VMX-файла.

Параметр политики	Атрибуты VMX-файла
Общие настройки виртуализации	• bios.bootdelay, bios.bootretry.delay, bios.bootretry.enabled, bios.forcesetuponce, chipset.onlinestandby, disable_acceleration, displayname, firmware, guestos, logging, monitor.virtual_exec, monitor.virtual_mmu, powertype.poweroff, powertype.poweron, powertype.reset, powertype.suspend, sched.swap.hostlocal, tools.synctime, tools.upgrade.policy, toolscripts.afterpoweron, toolscripts.afterresume, toolscripts.beforepoweroff, toolscripts.beforesuspend, uuid.bios, vmx.buildtype, wwn.enabled, wwn.node, wwn.port, wwn.type, bios440.filename, config.version, extendedconfigfile, nvram, sched.swap.derivedname, vc.uuid, virtualhw.version • атрибуты, соответствующие регулярному выражению hpet\d+\.present
Настройки CPU	• numvcpus, cpuid.corespersocket, vcpu.hotadd, sched.cpu.affinity, sched.cpu.htsharing, sched.cpu.shares, sched.cpu.max, sched.cpu.min, sched.cpu.units • атрибуты, соответствующие регулярному выражению cpuid\.(?:0|1|80000001)\.e[a-d]x(?:\.amd)
Оперативная память	memsize, mem.hotadd, sched.mem.max, sched.mem.min, sched.mem.minsize, sched.mem.shares
Настройки дисплея и видеопамяти	mks.enable3d, svga.autodetect, svga.maxheight, svga.maxwidth, svga.numdisplays, svga.present, svga.vramsize

Параметр политики	Атрибуты VMX-файла
Настройки контроллеров SCSI	Атрибуты, соответствующие регулярному выражению scsi(\d+)\.(?:present|sharedbus|virtualdev)
Настройки контроллеров SATA	Атрибуты, соответствующие регулярному выражению sata(\d+)\.(?:present|pcislotnumber)
Настройки HDD	Атрибуты, соответствующие регулярному выражению (?:scsi|sata|ide)(\d+:\d+)\..+
Настройки CD/DVD	Атрибуты, соответствующие регулярному выражению (?:ide|sata)(\d+:\d+)\..+
Дисковод Floppy	Атрибуты, соответствующие регулярному выражению floppy(\d+)\..+
Шина PCI	Атрибуты, соответствующие регулярному выражению pcipassthru(\d+)\..+
Настройки сетевых адаптеров	Атрибуты, соответствующие регулярному выражению ethernet(\d+)\..+
Последовательный порт	Атрибуты, соответствующие регулярному выражению serial(\d+)\..+
Параллельный порт	Атрибуты, соответствующие регулярному выражению parallel(\d+)\..+
Настройки USB	• ehci.present, usb.present, usb_xhci.present • атрибуты, соответствующие регулярному выражению usb\.autoconnect\.device\d+
Контроль протокола VMCI	vmci.filter.enable, vmci0.id, vmci0.present, vmci0.unrestricted
Параметры, контролируемые политиками безопасности vGate	isolation.bios.bbs.disable, isolation.device.connectable.disable, isolation.device.edit.disable, isolation.ghi.host.shellaction.disable, isolation.monitor.control.disable, isolation.tools.autoinstall.disable, isolation.tools.diskshrink.disable, isolation.tools.diskwiper.disable, isolation.tools.disptoporequest.disable, isolation.tools.dnd.disable, isolation.tools.getcreds.disable, isolation.tools.ghi.autologon.disable, isolation.tools.ghi.launchmenu.change, isolation.tools.ghi.protocolhandler.info.disable, isolation.tools.ghi.trayicon.disable, isolation.tools.guestdndversionset.disable, isolation.tools.memschedfakesamplestats.disable, isolation.tools.paste.disable, isolation.tools.setguioptions.enable, isolation.tools.trashfolderstate.disable, isolation.tools.unity.disable, isolation.tools.unity.push.update.disable, isolation.tools.unity.taskbar.disable, isolation.tools.unity.windowcontents.disable, isolation.tools.unityactive.disable, isolation.tools.unityinterlockoperation.disable, isolation.tools.vixmessage.disable, isolation.tools.vmxdndversionget.disable, log.keepold, log.rotatesize, remotedisplay.maxconnections, remotedisplay.vnc.enabled, tools.guestlib.enablehostinfo, tools.setinfo.sizelimit, vmsafe.agentaddress, vmsafe.agentport, vmsafe.enable

Настройка контроля целостности шаблона ВМ

Контроль целостности осуществляется только для шаблонов ВМ, которым назначена политика "Контроль целостности шаблонов виртуальных машин".

Настройка объектов контроля

vGate позволяет выполнить детальную настройку контроля целостности шаблона ВМ:

- разрешить или запретить операции с шаблоном ВМ при нарушении целостности конфигурации;

Внимание! Для всех шаблонов, которым назначена политика "Контроль целостности шаблонов виртуальных машин", блокируются операции удаления и конвертации шаблона в ВМ.

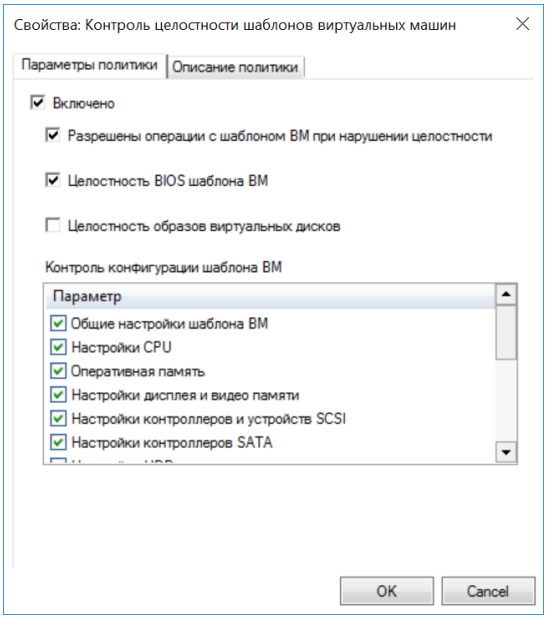
- выбрать файлы конфигурации шаблона ВМ (файлы VMDK, NVRAM), для которых будет осуществляться проверка соответствия контрольных сумм;
- выбрать параметры конфигурации шаблона ВМ (параметры VMTX-файла), изменение значений которых будет контролироваться политикой.

Настройка выполняется в диалоге редактирования параметров политики "Контроль целостности шаблонов виртуальных машин".

Для настройки параметров политики:

1. Выберите политику "Контроль целостности шаблонов виртуальных машин" в списке политик и нажмите кнопку "Изменить".

   На экране появится диалог настройки параметров политики.



2. Отредактируйте параметры политики.

Параметр	Описание
Разрешены операции с шаблоном ВМ при нарушении целостности	По умолчанию данный пункт отмечен. Удалите отметку, чтобы запретить операции с шаблоном при несоответствии контрольных сумм файлов шаблона их эталонным значениям
Целостность BIOS шаблона ВМ	По умолчанию данный пункт отмечен. Удалите отметку, чтобы выключить контроль целостности файлов конфигурации BIOS (файлов NVRAM) шаблона ВМ
Целостность образов виртуальных дисков	Отметьте этот пункт, чтобы включить контроль целостности образов виртуальных дисков шаблона ВМ (файлов VMDK). Операция подсчета контрольных сумм образов дисков может занять длительное время
Контроль конфигурации шаблона ВМ	Список параметров конфигурации шаблона ВМ (атрибутов VMTX-файла), контролируемых политикой, аналогичен списку параметров конфигурации ВМ (см. стр.**158**). Удалите отметку в нужной строке списка, чтобы отменить контроль за изменением значений соответствующего свойства шаблона ВМ

Поддерживается контроль целостности образов виртуальных дисков до 10 шаблонов ВМ с общим объемом дисков до 500 ГБ.

Пример.

- Если в виртуальной инфраструктуре 4 шаблона ВМ, общий объем дисков шаблонов с включенным КЦ может составлять 400 ГБ (при размере каждого образа 100 ГБ).
- Если в виртуальной инфраструктуре 10 шаблонов ВМ, общий объем дисков шаблонов с включенным КЦ может составлять 500 ГБ (при размере каждого образа 50 ГБ).

Внимание! При включении параметра "Целостность образов виртуальных дисков" выполняется пересчет контрольных сумм для шаблонов ВМ, которым назначена политика "Контроль целостности шаблонов виртуальных машин".

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

Внимание! При редактировании параметров политики "Контроль целостности шаблонов виртуальных машин" нужно повторить назначение данной политики шаблону ВМ. При конвертации шаблона в виртуальную машину для контроля целостности полученной ВМ нужно назначить ей политику "Доверенная загрузка виртуальных машин" (см. стр.**158**).

Расчет контрольных сумм и контроль изменений шаблона

Для каждого шаблона, которому назначается политика "Контроль целостности шаблонов виртуальных машин", рассчитывается эталонная контрольная сумма (КС), которая используется для контроля целостности.

Сравнение эталонной КС шаблона ВМ с текущей выполняется каждые 30 минут или при проверке политик вручную (кнопка-ссылка "Проверить политики" на странице "Развертывание").

При несовпадении контрольных сумм шаблона ВМ фиксируется нарушение целостности, изменяется статус шаблона ВМ (значение в колонке "Контроль целостности") и могут быть запрещены операции с данным шаблоном, если в настройках политики "Контроль целостности шаблонов виртуальных машин" отмечен пункт "Разрешены операции с шаблоном ВМ при нарушении целостности".

Администратор может в зависимости от статуса шаблона ВМ принять изменения (согласовать) либо отклонить их аналогично согласованию изменений ВМ (см. стр.**165**).

Примечание. При подсчете контрольных сумм образов виртуальных дисков возможно появление статуса шаблона ВМ "Требует согласования". Данный статус не требует выполнения действий.

Настройка контроля целостности файлов конфигурации ESXi-сервера

Контроль целостности (КЦ) осуществляется для защищаемых ESXi-серверов, которым назначена политика "Контроль целостности файлов конфигурации ESXi-сервера".

Настройка объектов контроля

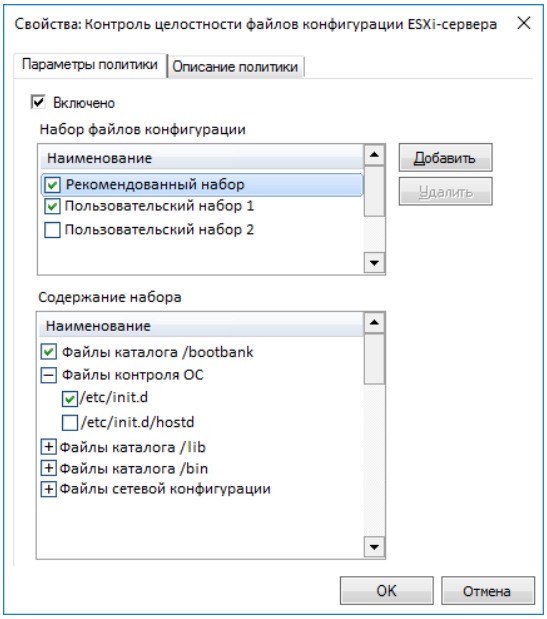
vGate позволяет выбрать рекомендованный или создать пользовательский набор файлов конфигурации ESXi-сервера, для которого будет осуществляться проверка соответствия контрольных сумм.

Настройка выполняется в диалогах редактирования параметров политики "Контроль целостности файлов конфигурации ESXi-сервера".

Для настройки параметров политик:

1. Выберите политику "Контроль целостности файлов конфигурации ESXi-сервера" в списке политик и нажмите кнопку "Изменить".

   На экране появится диалог настройки параметров политики.



2. Отметьте параметр "Включено", чтобы активировать политику.
3. По умолчанию в настройках политики есть рекомендованный набор файлов конфигурации. Чтобы добавить новый набор файлов для контроля целостности, нажмите кнопку "Добавить". Откроется окно добавления файла.
4. Выберите файл и нажмите "Открыть".

   Текстовый файл в кодировке UTF-8 должен содержать пути к файлам конфигурации защищаемого сервера, расположенные в разных строках.
5. В поле "Содержание набора" выберите файлы, для которых нужно выполнять контроль целостности, и нажмите кнопку "OK".

Расчет контрольных сумм и контроль изменений

Целостность файлов конфигурации защищаемых серверов контролируется компонентами защиты, установленными на ESXi-серверы. Для каждого файла конфигурации рассчитывается эталонная контрольная сумма (КС), которая используется для контроля целостности.

КС и путь к файлу конфигурации хранятся в базе и проверяются каждые 10 минут и по запросу пользователя. При несовпадении контрольных сумм фиксируется нарушение целостности, изменяется статус ESXi-сервера (значение в колонке "Контроль целостности").

Администратор может в зависимости от статуса защищаемого сервера принять изменения (согласовать) либо отклонить их аналогично согласованию изменений ВМ (см. стр.**165**).

Согласование и отклонение изменений

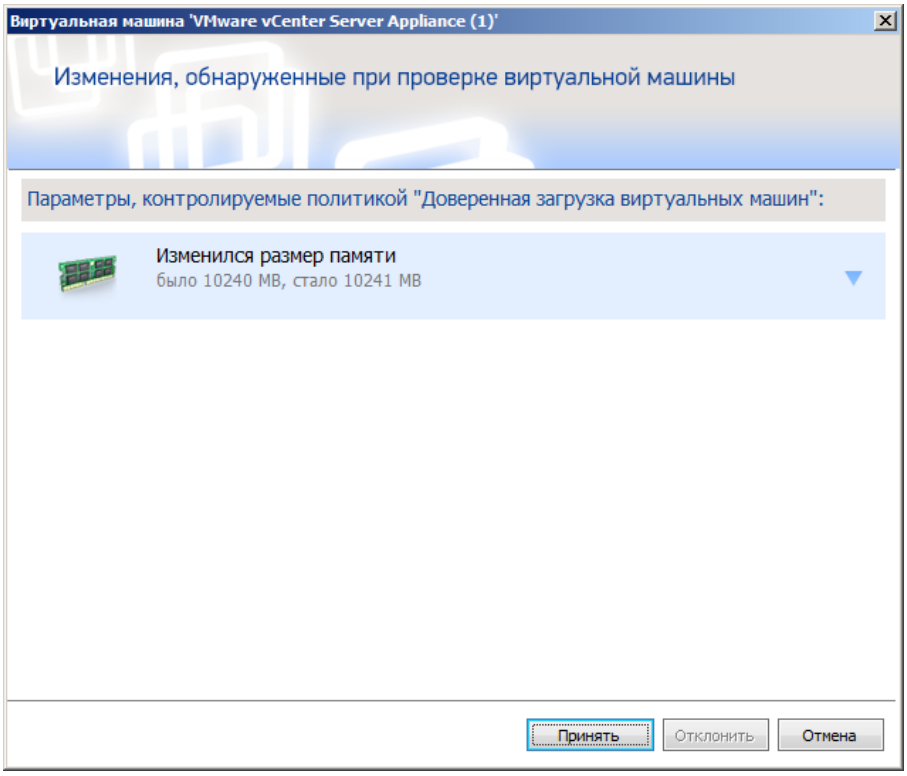
Внимание! Операции согласования и отклонения изменений рекомендуется выполнять, предварительно выключив виртуальную машину.

Для согласования и отклонения изменений:

1. В консоли управления выберите функцию "Виртуальные машины".
2. Выберите в списке интересующую вас ВМ.

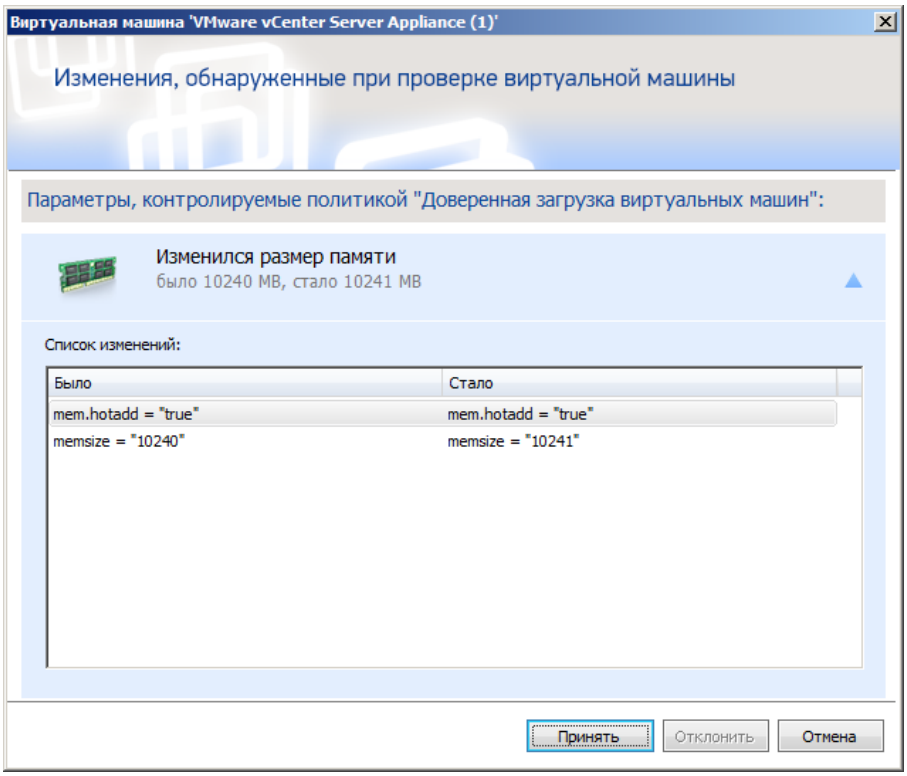
   Примечание. Аналогично можно выполнять согласование и отклонение изменений шаблона ВМ. Для этого выберите функцию "Виртуальные машины" и нажмите кнопку-ссылку "Список" для отображения шаблонов ВМ в списке, затем выберите нужный шаблон.
3. Для согласования изменений нажмите кнопку-ссылку "Согласовать".

   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 ESX-сервере 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 ESXi-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 контроля доступа к vCenter	События, связанные с работой службы контроля доступа к vCenter, установленной на сервере авторизации vGate
Компонент защиты VMware ESXi	События, связанные с работой компонента защиты ESXi-сервера
Компонент защиты VMware vCenter	События, связанные с работой компонента защиты vCenter
Служба аутентификации	События аутентификации
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	События, касающиеся разрешения или запрета запуска виртуальных машин
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 ESXi-сервера
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	

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

Характеристика	Описание
Предупреждение	Предупреждение о неудачном выполнении действий, представляющих угрозу для безопасности системы
Успех	Сообщение об успешном выполнении действий, связанных с безопасностью системы
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.
ESXi-сервер
События нарушения КЦ на ESXi-серверах регистрируются в базе данных vGate. Интервал проверки задается в конфигурационном файле /etc/config/vgate/vgate.cfg, секция vagentd:, параметр interval (в секундах). По умолчанию интервал равен 600 сек.
Сервер vCenter
События нарушения КЦ на серверах vCenter 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.

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

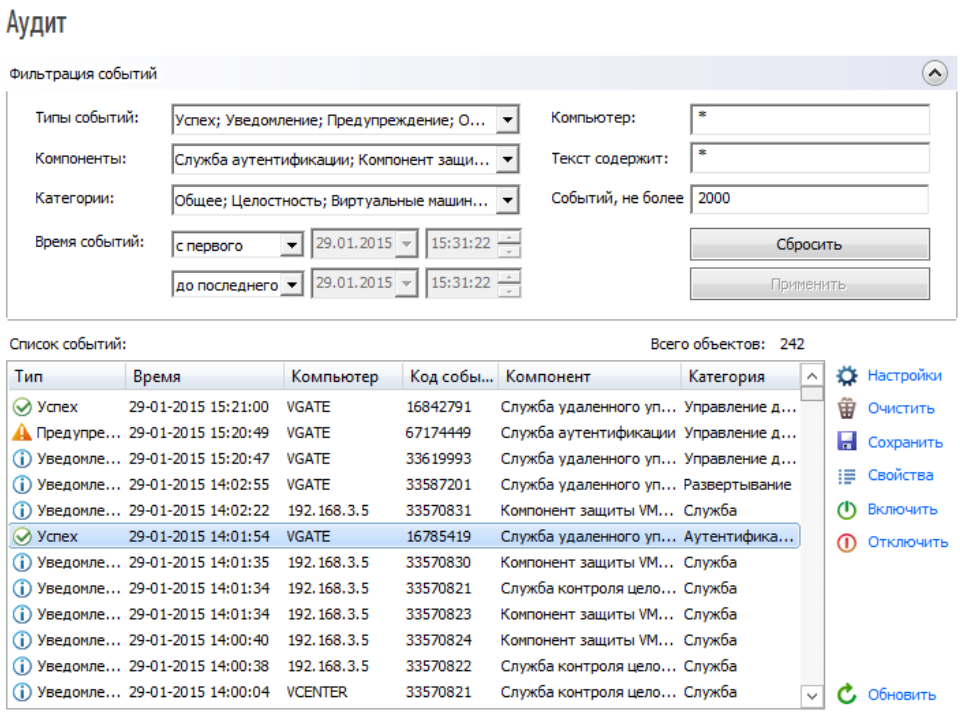
Список записей в журнале событий безопасности обновляется автоматически при выборе функции "Аудит" в консоли управления и через определенный период времени (по умолчанию равен 30 секундам). Отключить автоматическое обновление списка или изменить период между обновлениями можно в разделе "Конфигурация" (см. стр.**172**).

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.**167**). 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.**170**).

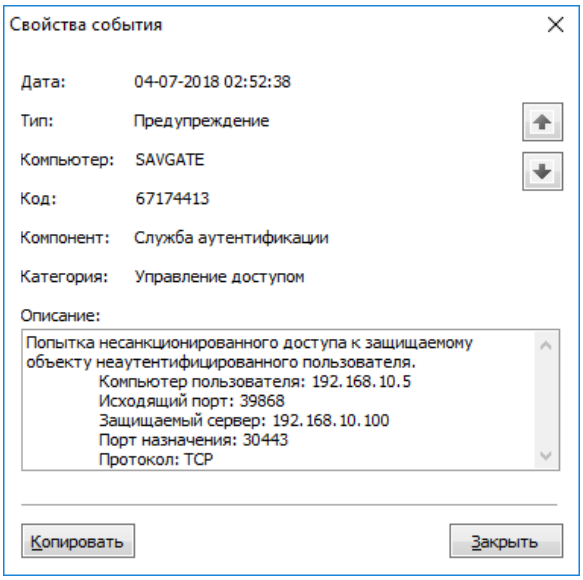
3. Нажмите кнопку "Применить".

   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, 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", "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: 564D01E8-E243-F215-F3A9-F660C20D13D4
Хранилище данных	Идентификатор хранилища данных. Например: 5267bb719a7783a6eaf4000c29936a9e
Виртуальная сеть	Идентификатор виртуальной сети (VLAN ID). Например: VLAN ID: 1
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.

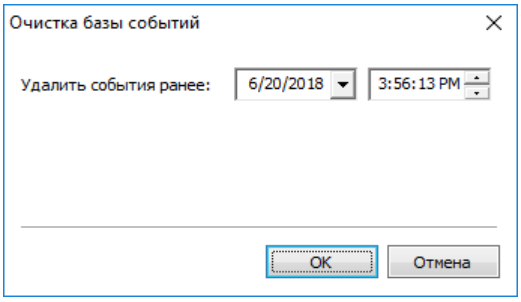
Примечание. Сохранение большого количества событий может занять длительное время.

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).

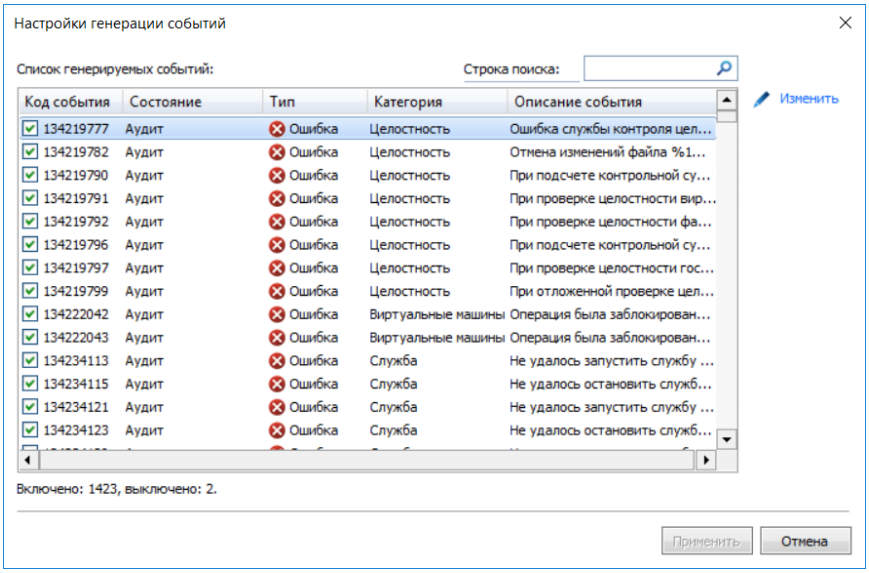
Примечание. События, соответствующие неудачным попыткам аутентификации пользователя Active Directory, не регистрируются в журнале сервера авторизации vGate. Для регистрации таких событий требуется настроить на контроллере домена политику "Аудит событий входа в систему" (Audit account logon events). Просмотр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

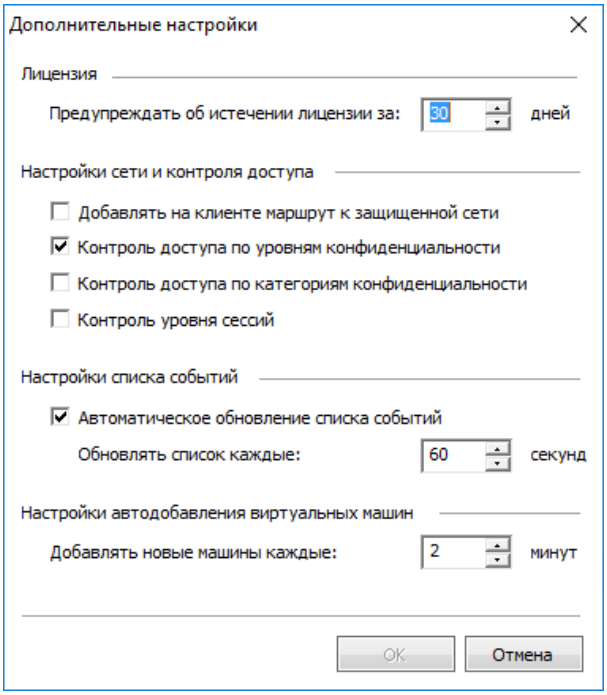
Настройка автоматического обновления списка событий

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 7
Подготовка отчетов

Функция просмотра отчетов о событиях безопасности vGate доступна в vGate Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Виды отчетов

vGate позволяет подготовить следующие виды отчетов.

Название	Описание
Инциденты в мониторинге	Данный отчет показывает статистику по последним 10 инцидентам, произошедшим в системе мониторинга vGate
Наиболее активные пользователи в vGate для vSphere	Данный отчет показывает статистику по наиболее активным пользователям. Отображается процентное соотношение событий аутентификации для выбранного количества учетных записей пользователей за указанный период
Наиболее используемые виды доступа к защищаемым объектам в vGate для vSphere	Данный отчет показывает статистику по наиболее используемым видам доступа к защищаемым объектам (наиболее часто используемым протоколам и портам)
Наиболее частые события ИБ в системе vGate для vSphere	Данный отчет показывает статистику по наиболее частым событиям информационной безопасности
Панель мониторинга	Данный отчет отображает состояние виртуальной инфраструктуры в виде графиков по произошедшим событиям мониторинга
События сегментирования	Данный отчет содержит статистику по последним событиям в разделе "Сегментирование"
Статистика запусков виртуальных машин VMware vSphere	Данный отчет отображает информацию о событиях запуска виртуальных машин за указанное число дней
Настройки доступа к защищаемым объектам	Данный отчет отображает информацию о результирующих настройках доступа к защищаемым объектам в vGate для VMware vSphere
Настройка правил сетевой безопасности в vGate для vSphere	Данный отчет отображает информацию о настройках правил разграничения доступа к защищаемым серверам
Политики безопасности, назначенные на объекты в vGate для vSphere	Данный отчет показывает, какие политики безопасности назначены на объекты виртуальной инфраструктуры
Правила мониторинга	Данный отчет содержит информацию о включенных правилах корреляции
Сегментирование	Данный отчет содержит информацию о статусе компонента фильтрации трафика на защищаемых объектах и настроенных правилах фильтрации

Название	Описание
Доступ в нерабочее время	Данный отчет показывает информацию о событиях входа в систему в нерабочее время
Изменение конфигурации политик безопасности в vGate для vSphere	Данный отчет показывает, какие изменения произошли в настройках политик безопасности за указанный период
Изменение мандатных правил доступа	Данный отчет показывает, какие изменения произошли в настройках vGate для VMware vSphere в части полномочного управления доступом за указанный период
Изменение сетевых правил доступа в vGate	Данный отчет показывает, какие изменения произошли в настройках vGate в части правил разграничения доступа к защищаемым серверам за указанный период
Использование учетных записей VMware	Данный отчет показывает, какие учетные записи VMware используются пользователями vGate
Попытки несанкционированного изменения настроек, контролируемых политиками в vGate для vSphere	Данный отчет отображает информацию о событиях несанкционированного изменения настроек, контролируемых политиками
Применение политик безопасности в vGate для vSphere	Данный отчет отображает информацию о событиях применения и отмены политик безопасности за указанный период
Проблемы доступа в vGate	Данный отчет отображает информацию о событиях неудачных попыток аутентификации в vGate за указанный период
Проблемы доступа в vSphere	Данный отчет отображает информацию о событиях неудачных попыток аутентификации в vSphere под учетной записью VMware за указанный период
Проблемы с доверенной загрузкой виртуальных машин в vGate для vSphere	Данный отчет показывает, какие виртуальные машины не удалось запустить из-за нарушения целостности их конфигурации
Проблемы со сменой пароля в vGate для vSphere	Данный отчет показывает информацию о неудачных попытках смены пароля учетных записей vGate за указанный период
Создание, изменение, удаление учетных записей vGate	Данный отчет отображает информацию о событиях создания, удаления или изменения учетных записей vGate
Управление виртуальной инфраструктурой	Данный отчет отображает информацию об активности пользователей за указанный период
Соответствие стандартам безопасности	Данная группа отчетов отображает детальную информацию о соответствии серверов стандартам безопасности. Для постоения отчета необходимо предварительно назначить нужный набор политик на ESXi-сервер

Предварительная настройка

План действий

Для генерации отчетов с помощью vGate необходимо выполнить следующие предварительные настройки:

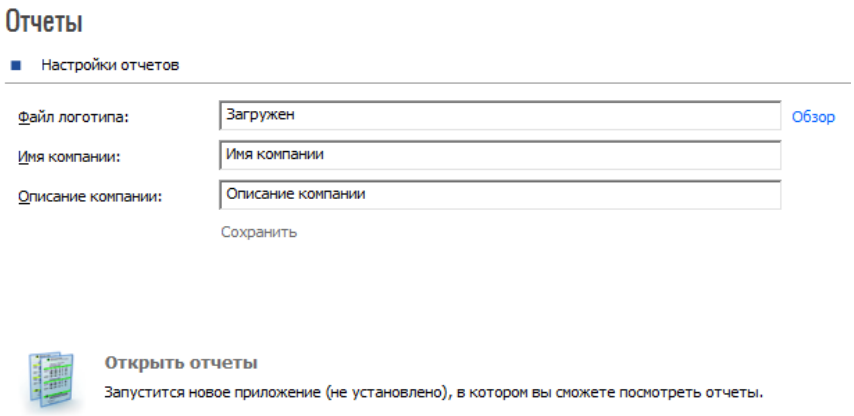
№	Шаг	Особенности	Описание
1.	**Установка компонента для просмотра отчетов**	На тех рабочих местах АИБ, на которых предполагается работать с отчетами, необходимо установить Microsoft Report Viewer 2010 SP1 Redistributable Package	См. стр.9
2.	**Настройка параметров**	Параметры формирования отчетов задаются в консоли управления сервера авторизации	См. стр.177
3.	**Настройка прав доступа**	Если рабочее место АИБ находится вне защищаемого периметра, необходимо настроить ПРД. При установке сервера авторизации в список защищаемых серверов автоматически добавляется IP-адрес сетевого адаптера защищаемого периметра и для него создается ПРД с параметрами "Компьютер: Любой", "Протокол: TCP", "Исходящий порт: 0", "Порт назначения: 902". Это ПРД позволяет учетной записи главного АИБ просматривать отчеты на любом компьютере. Для других учетных записей аналогичное ПРД нужно создать вручную. Кроме того, перед запуском консоли управления АИБ в обязательном порядке должен пройти процедуру авторизации с помощью агента аутентификации	См. стр.137

Настройка параметров отчетов

Для настройки параметров отчетов:

1. В консоли управления выберите функцию "Отчеты".

   На экране появится диалог для настройки параметров отчетов.



2. При необходимости укажите значения параметров оформления отчетов и нажмите кнопку "Сохранить".

Параметр	Описание
Файл логотипа	Путь к файлу с логотипом компании. Поддерживается загрузка файлов только в формате *.bmp. Логотип будет размещен на титульном листе отчетов
Имя компании	Название компании, виртуальная инфраструктура которой защищается vGate. Это название будет указано на титульном листе отчетов
Описание компании	Описание компании, виртуальная инфраструктура которой защищается vGate. Это описание будет указано на титульном листе отчетов

Примечание. Кнопка "Сохранить" становится активной только после изменения какого-либо параметра.

Формирование отчетов

Формирование отчетов возможно в консоли управления или в агенте аутентификации vGate (см. раздел "Аутентификация пользователей" в документе [**4**]).

Для формирования отчетов:

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

   На экране появится диалог для настройки параметров отчетов.

2. Активируйте ссылку "Открыть отчеты".

   На экране появится окно со списком всех имеющихся отчетов.

   Названия отчетов являются ссылками для перехода к просмотру отчетов.

3. Выберите название нужного отчета.

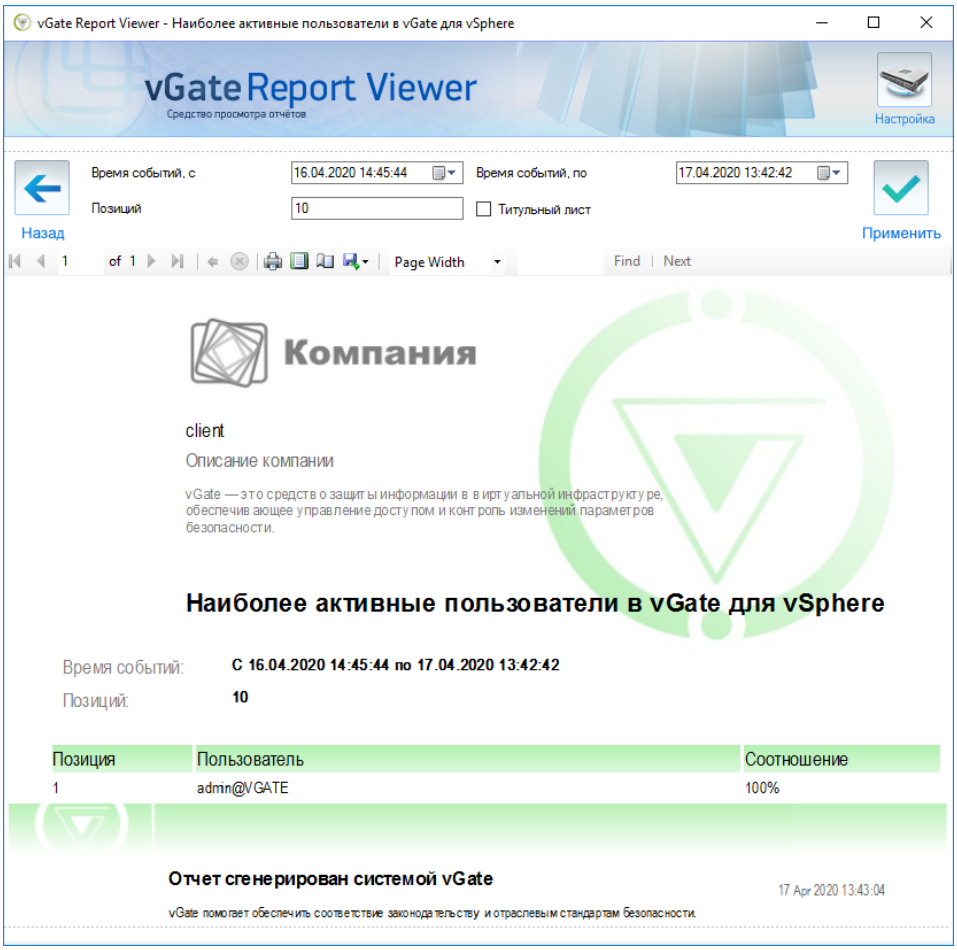
   Появится сформированный отчет с параметрами по умолчанию. Также станет доступна панель настройки параметров формирования отчета.

4. Задайте параметры формирования отчета и нажмите кнопку "Применить".

Время событий, с:/по:
Период, за который были зафиксированы события. По умолчанию рассматриваются события за весь период
Рабочее время, с:/по:
Период, который следует считать рабочим днем при формировании отчета. По умолчанию рабочим временем считается период с 9:30 по 18:00. Указывается для отчета "Вход в систему в нерабочее время"
Последние, дней
Количество дней, за которое необходимо сформировать отчет
Пользователи vGate
Учетные записи vGate, по которым необходимо сформировать отчет
Учетные записи VMware
Учетные записи VMware, по которым необходимо сформировать отчет
Титульный лист
Вариант оформления отчета. Для отключения титульного листа удалите отметку. По умолчанию все отчеты формируются с титульным листом. Указывается для всех отчетов
Количество позиций
Количество позиций в приводимой статистике
Защищаемые серверы
Перечень защищаемых серверов, по которым необходимо сформировать отчет. По умолчанию в отчет включаются все защищаемые серверы. Указывается для отчета "Доступ к файлам ВМ"
Наборы политик
Наборы политик, по которым необходимо сформировать отчет. По умолчанию отчет формируется по всем наборам политик. Указывается для отчета "Изменение конфигурации политик безопасности"
Группировка
Способ группировки сведений в отчете. Данный параметр является обязательным. Без указания этого параметра отчет не сформируется. Возможные варианты группировки зависят от типа отчета
Учетные записи VMware
Учетные записи VMware, по которым необходимо сформировать отчет. Указывается для отчета "Использование учетных записей VMware"
Действия
Действия с данными, которые необходимо включить в отчет. Возможные значения зависят от вида отчета. По умолчанию в отчет включаются все возможные действия
Тип объекта
Типы объектов доступа, по которым необходимо сформировать отчет. Возможные значения типов объектов зависят от типа отчета. По умолчанию в отчет включаются все типы объектов

Объекты доступа
Объекты доступа, по которым необходимо сформировать отчет
Интервал (минут)
Длительность интервала регистрации события. Указывается для отчета "Попытки несанкционированного изменения настроек, контролируемых политиками"
Количество попыток
Количество попыток, по которым следует сформировать отчет
Раскрывать группы
Стандарты безопасности, сведения о соответствии которым будут отражены в отчете. Указывается для отчетов "Соответствие стандартам безопасности"
Приложить описание политик
Вариант оформления отчета. Для отключения параметра удалите отметку. По умолчанию все отчеты формируются с описанием политик

Отчет будет сформирован.



Сформированный отчет можно распечатать или выгрузить в различные форматы. Для работы с отчетом используйте панель инструментов, находящуюся ниже панели настройки параметров отчета.

Действия с отчетами

При отображении отчета одновременно с ним в окне программы появляется панель инструментов для навигации по многостраничному отчету и выполнения с ним ряда других действий.

Навигация
Используйте соответствующие кнопки для перехода к первой, последней, предыдущей или следующей страницам отчета. Для перехода к странице с определенным номером введите ее номер в поле ввода "Текущая страница" и нажмите клавишу "Ввод"
Масштабирование
Для масштабирования отчета выберите необходимое значение масштаба в списке
Поиск
Для поиска нужной строки символов введите строку в поле "Найти текст" и нажмите "Найти". Нажмите "Далее" для поиска последующих вхождений строки
Экспорт
Вы можете экспортировать отчет в один из предложенных форматов (PDF, Excel). Выберите нужный формат в списке "Выбрать формат" и нажмите "Экспорт"
Настройки страницы
Чтобы настроить параметры страницы отчета, нажмите "Настройки страницы"
Печать
Чтобы распечатать отчет, нажмите "Печать", укажите параметры печати и нажмите "ОК"

Глава 8
Веб-консоль

ПО vGate 4.4 включает в себя веб-консоль для управления настройками функции "Сегментирование" 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:

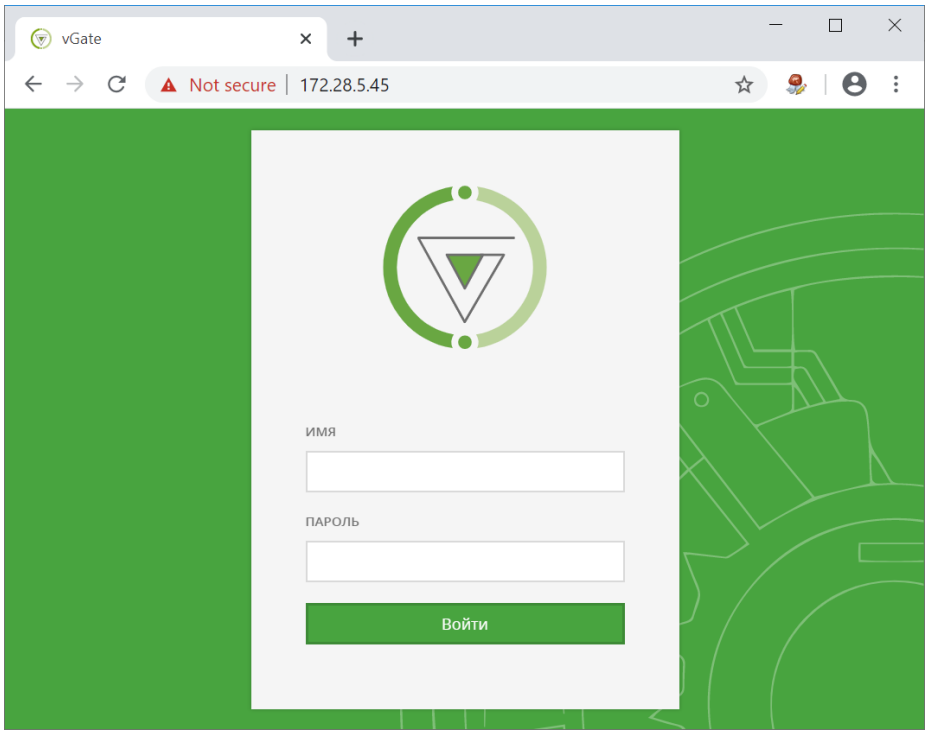
- Chrome версии 83.0.4103.61 (64-bit);
- Firefox версии 76.0.1 (64-bit);
- Opera версии 67.0.3575.79;
- Яндекс.Браузер версии 20.4.3.255 (64-bit).

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.137). 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.212).

Главное меню веб-консоли состоит из следующих разделов:

- Сегментирование (см. стр.**183**);
- Мониторинг (см. стр.**191**);
- Отчеты (см. стр.**201**);
- Журнал событий (см. стр.**203**);
- Учетные записи (см. стр.**203**);
- Соответствие политикам (см. стр.**205**);
- Настройки (см. стр.**207**).

Сегментирование

ПО vGate 4.4 включает в себя инструмент "Сегментирование", который позволяет осуществлять фильтрацию сетевого трафика в сети виртуальных машин VMware vSphere, в том числе и расположенных на разных серверах виртуализации.

Данная функция доступна только в vGate Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Сегментирование обеспечивается компонентом фильтрации трафика виртуальных машин. Компонент фильтрации устанавливается по умолчанию вместе с компонентом защиты ESXi-сервера (см. стр.**100**).

Внимание! Если правила фильтрации (см. стр.187) созданы с указанием MAC-/IP-адресов отправителя или получателя, они перестанут работать в случае изменения у виртуальной машины этих параметров. vGate отслеживает изменение этих параметров для правил фильтрации, назначенных виртуальным машинам и сегментам, но для корректной работы функции "Сегментирование" рекомендуется запретить изменение MAC-адреса. Для этого в настройках виртуальных коммутаторов (vSwitch) /VDS выберите значение "Reject" для параметров "Forged Transmits" и "MAC Address Change" или назначьте ESXi-серверу политику "Настройки безопасности для виртуальных коммутаторов". Также назначьте распределенному виртуальному коммутатору политики "Проверка соответствия параметра MAC Address Change значению Reject" и "Проверка соответствия параметра Forged Transmits значению Reject" для отслеживания изменений политик безопасности виртуального коммутатора.

Для настройки сегментирования:

1. Установите компонент защиты vGate на ESXi-серверы (см. стр.**100**).
2. Включите компонент фильтрации трафика на защищаемых ESXi-серверах (см. стр.**183**).
3. Выберите из списка виртуальные машины, трафик которых необходимо контролировать (см. стр.**184**).

   Внимание! Для отображения актуального списка виртуальных машин в консоли управления vGate должны быть сохранены параметры подключения к серверу виртуализации (см. стр.77).
4. При необходимости объедините виртуальные машины в сегменты виртуальной инфраструктуры (см. стр.**185**).
5. Создайте правила фильтрации сетевого трафика (см. стр.**187**).
6. Для просмотра данных об активных сессиях перейдите на страницу "Активные сессии" (см. стр.**190**).

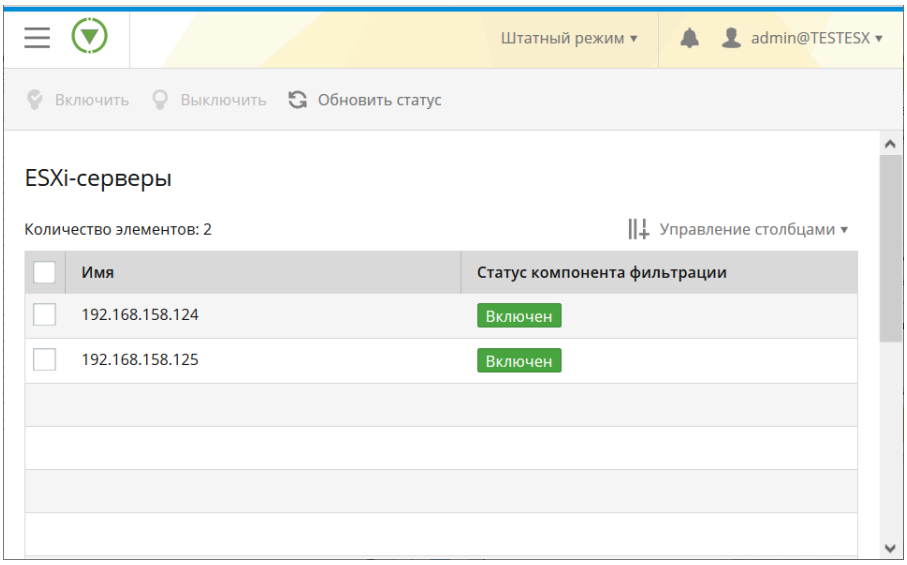
Включение компонента фильтрации трафика на ESXi-серверах

По умолчанию компонент фильтрации трафика vGate на защищаемых ESXi-серверах выключен.

Чтобы включить компонент фильтрации трафика:

1. В главном меню выберите раздел "Сегментирование", а затем "ESXi-серверы".

На экране появится следующее окно.



2. Выберите из списка серверы виртуализации, на которых необходимо включить компонент фильтрации трафика, и нажмите кнопку "Включить".

   Компонент фильтрации будет активирован.

Примечание.

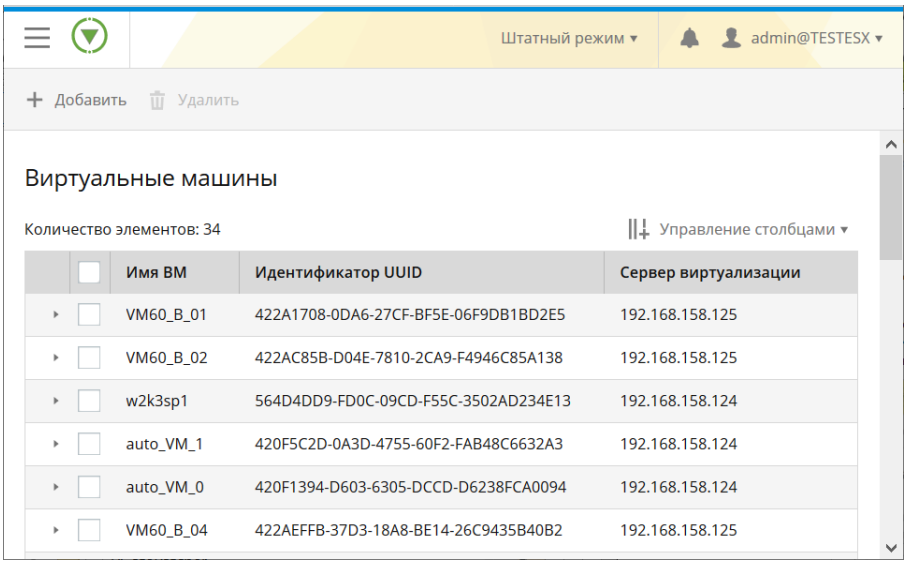
- Чтобы выключить компонент фильтрации, выберите ESXi-серверы и нажмите кнопку "Выключить". Нажмите кнопку "Обновить статус", чтобы обновить информацию о состоянии компонентов фильтрации на этих серверах.
- Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.

Включение контроля трафика виртуальных машин

Чтобы включить контроль трафика ВМ:

1. В главном меню выберите раздел "Сегментирование", а затем "Виртуальные машины".

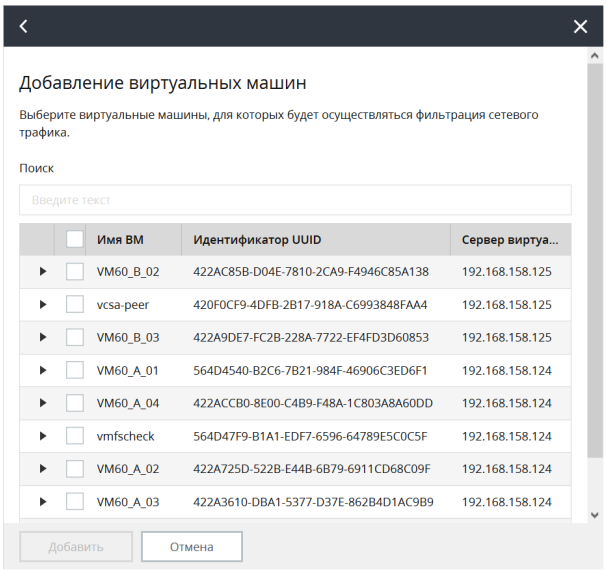
   На экране появится следующее окно.



Внимание!
- Для отображения актуального списка виртуальных машин в консоли управления vGate должны быть сохранены параметры подключения к серверу виртуализации (см. стр.77).
- Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.

2. В списке отображаются виртуальные машины, для которых осуществляется контроль трафика. Чтобы добавить виртуальную машину в список защищаемых, нажмите кнопку "Добавить".

   В правой части окна откроется панель выбора виртуальных машин.



3. В данном списке отображаются все виртуальные машины, расположенные на ESXi-серверах, на которых включен компонент фильтрации трафика vGate. Выделите нужные виртуальные машины и нажмите кнопку "Добавить".

   Примечание. Если в виртуальной машине установлены VMware Tools, в таблице также будет отображаться дополнительная информация о ВМ: виртуальная сеть и IP-адрес.

   ВМ будут добавлены в список контролируемых компонентом фильтрации.

Внимание! Для активации компонента фильтрации трафика на запущенных виртуальных машинах их необходимо перезапустить с помощью команд Suspend и Resume или Power off и Power on.

Внимание! Не включайте контроль трафика для виртуальной машины, если на ней расположен сервер авторизации vGate. Это может привести к неработоспособности системы.

Для выключения контроля трафика виртуальной машины, выделите ее в списке и нажмите кнопку "Удалить". Действие распространяется только на ВМ, выделенные на текущей странице списка.

Сегменты

Чтобы создать правило для нескольких виртуальных машин, можно объединить ВМ из списка защищаемых в сегменты виртуальной инфраструктуры.

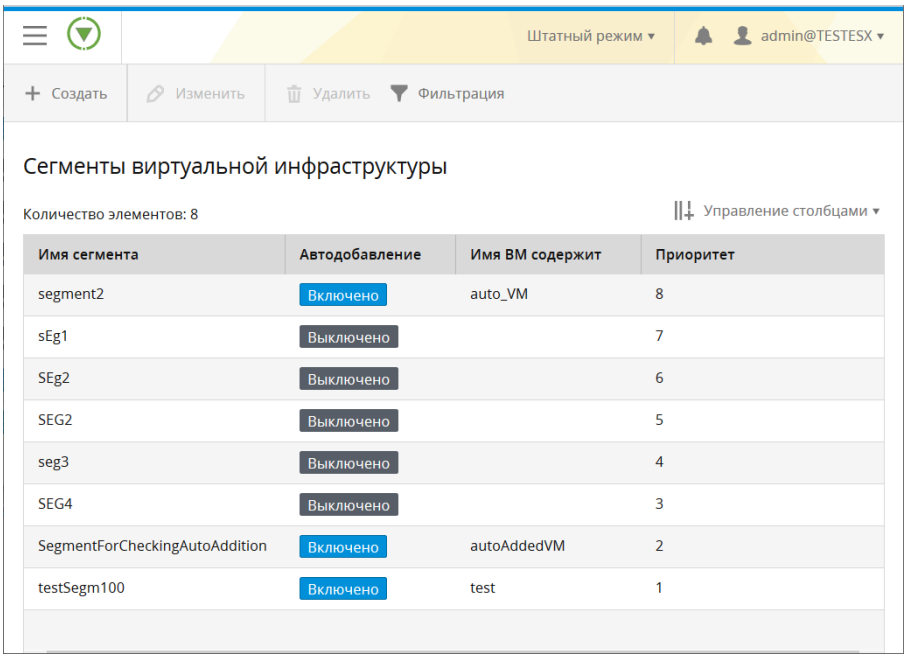
Внимание! Виртуальная машина не может входить более чем в один сегмент виртуальной инфраструктуры.

Внимание! Сегмент виртуальной инфраструктуры не может быть пустым. Если в результате редактирования в сегменте не остается ни одной виртуальной машины, такой сегмент автоматически удаляется.

Чтобы создать сегмент виртуальной инфраструктуры:

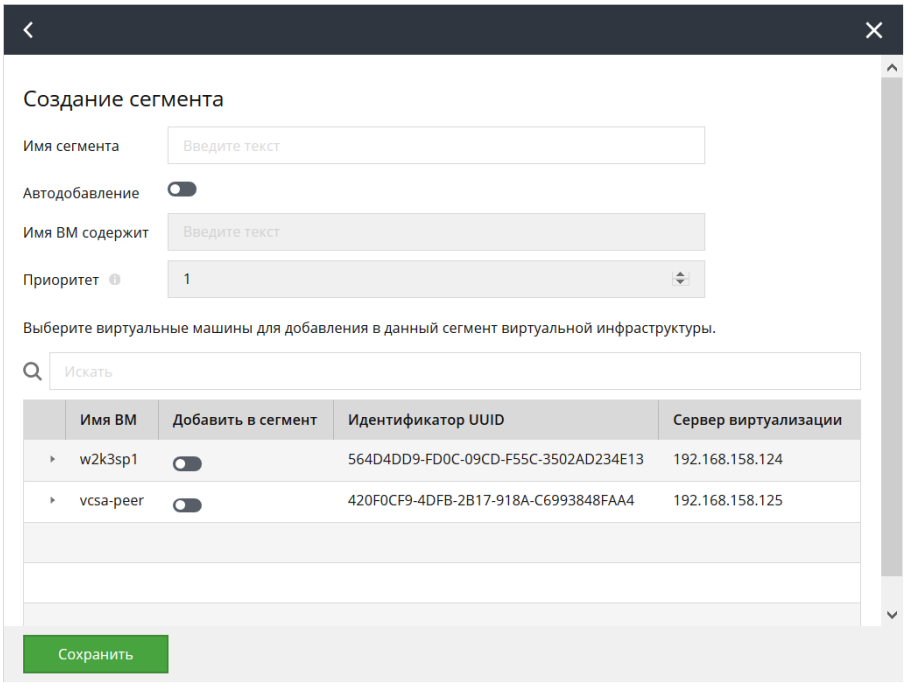
1. В главном меню выберите раздел "Сегментирование", а затем "Сегменты".

На экране появится следующее окно.



2. Нажмите кнопку "Создать".

В правой части окна откроется панель выбора виртуальных машин для добавления в сегмент виртуальной инфраструктуры. В списке отображаются все виртуальные машины, на которых включен контроль трафика (см. стр.**184**).



3. Укажите параметры нового сегмента, для добавляемых в сегмент виртуальных машин переведите переключатель в столбце "Добавить в сегмент" в положение "Вкл" и нажмите кнопку "Сохранить".

Параметр	Описание
Имя сегмента	Укажите уникальное имя сегмента
Автодобавление	Установите переключатель в положение "Вкл", чтобы настроить автоматическое добавление виртуальных машин в сегмент виртуальной инфраструктуры по параметру "Имя ВМ содержит"
Имя ВМ содержит	Введите текст, по которому будет выполняться поиск в именах виртуальных машин для их автодобавления в сегмент виртуальной инфраструктуры
Приоритет	Укажите приоритет, согласно которому определяется сегмент, в который будет добавлена виртуальная машина при соответствии ее имени нескольким сегментам. При изменении приоритета одного из сегментов происходит автоматический пересчет приоритетов остальных сегментов таким образом, чтобы избежать дублирования приоритетов, а также чтобы между значениями приоритетов не было промежутков

Внимание! Имя сегмента может содержать только латинские и кириллические символы, цифры, пробелы, дефисы и нижние подчеркивания.

Примечание.

- Для просмотра информации об адаптерах ВМ нажмите ▶ рядом с именем виртуальной машины.
- Для быстрого поиска виртуальных машин введите текст в поле "Искать". Поиск осуществляется по всем столбцам таблицы.

ВМ будут добавлены в созданный сегмент виртуальной инфраструктуры.

Примечание. Чтобы разрешить сетевой трафик между виртуальными машинами, находящимися в одном сегменте виртуальной инфраструктуры, необходимо добавить разрешающее правило (см. стр.187), указав этот сегмент в качестве источника и получателя.

Управление правилами фильтрации

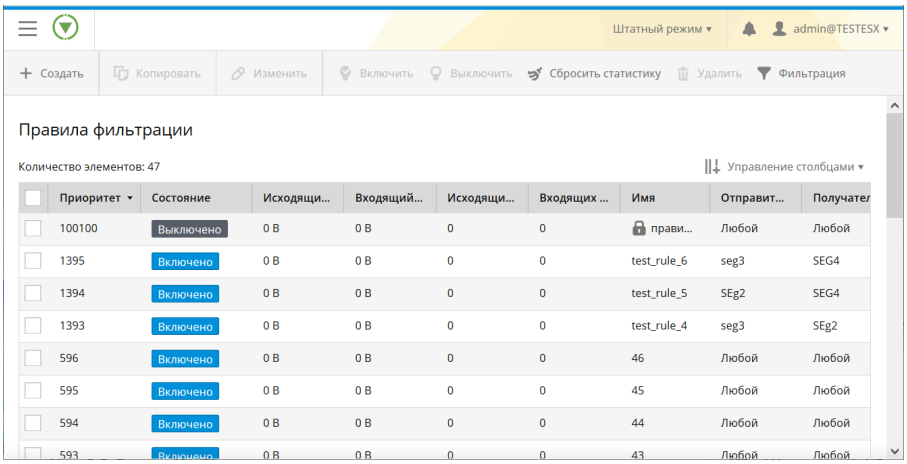
Для настройки фильтрации сетевого трафика используются правила фильтрации. По умолчанию список содержит правила, разрешающие весь входящий и исходящий трафик в штатном, тестовом и аварийном режимах vGate. Правила для тестового и аварийного режимов не могут быть отредактированы.

Правила фильтрации могут создаваться для конкретной виртуальной машины (см. ниже) или для нескольких виртуальных машин. Чтобы создать правило для нескольких ВМ из списка защищаемых, нужно объединить их в сегменты (см. стр.185).

Чтобы создать правило фильтрации:

1. В главном меню выберите раздел "Сегментирование", а затем "Правила фильтрации".

На экране появится окно.

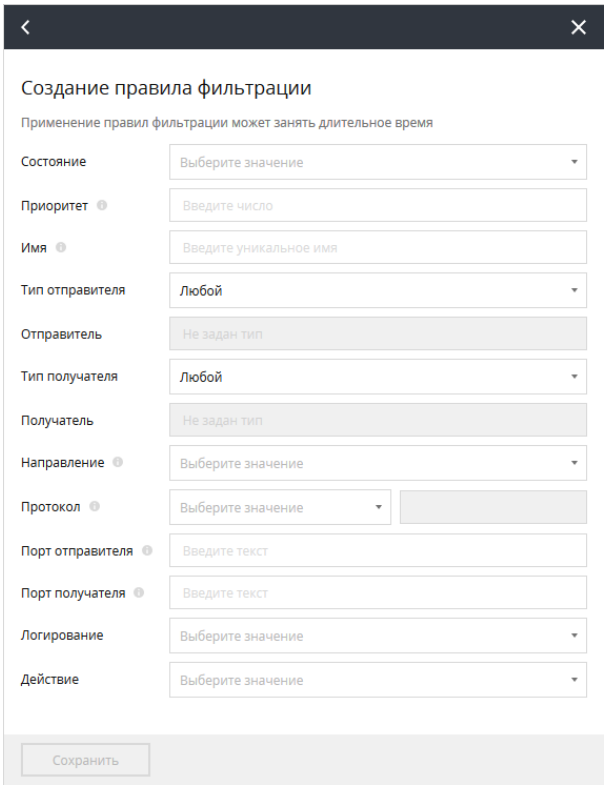


Примечание.

- Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.
- В правилах фильтрации возможно некоторое преувеличение количества переданных пакетов и объема сетевого трафика.

2. Для создания нового правила нажмите кнопку "Создать".

Откроется панель создания правила фильтрации.



3. Задайте параметры правила и нажмите кнопку "Сохранить".

Параметр	Описание
Состояние	Выберите состояние правила (включено/выключено)
Приоритет	Правила фильтрации обрабатываются с учетом указанных приоритетов. Поле должно содержать уникальное значение в диапазоне от 100 до 2100. Правило аварийного режима имеет максимальный приоритет, правило тестового режима — минимальный приоритет
Имя	Уникальное название правила
Тип отправителя	Типы объектов — отправителей сетевых пакетов, для которых должно использоваться правило: • IP-адрес; • подсеть; • диапазон IP-адресов; • MAC-адрес; • виртуальная машина; • сегмент виртуальной инфраструктуры; • любой
Отправитель	Введите данные отправителя указанного выше типа
Тип получателя	Типы объектов — получателей сетевых пакетов, для которых должно использоваться правило: • IP-адрес; • подсеть; • диапазон IP-адресов; • MAC-адрес; • виртуальная машина; • сегмент виртуальной инфраструктуры; • любой
Получатель	Введите данные получателя указанного выше типа
Направление	Определяет направление прохождения пакета при проверке правила фильтрации
Протокол	Определяет используемый протокол
Порт отправителя	Исходящий порт, для которого действует правило, или "*" (звездочка), если правило действует для всех портов. Номер порта должен быть в диапазоне 1–65535
Порт получателя	Порт назначения, для которого действует правило, или "*" (звездочка), если правило действует для всех портов
Логирование	Отвечает за включение логирования правила фильтрации. Лог-файлы хранятся на ESXi-серверах, откуда отправляются на сервер авторизации vGate. Если данное поле отмечено, сетевой трафик будет отображаться в активных сессиях компонента "Сегментирование" (см. стр.**190**)
Действие	Выберите действие, которое будет осуществлять правило

Правило фильтрации будет добавлено в список.

Примечание.

- Чтобы включить/выключить правило фильтрации, выделите правило в списке и нажмите кнопку "Включить"/"Выключить". Чтобы отредактировать настройки правила, нажмите кнопку "Изменить".
- Для удаления правила выделите его в списке и нажмите кнопку "Удалить". Действие распространяется только на правила, выделенные на текущей странице.
- Чтобы скопировать правило фильтрации, выберите его в списке и нажмите кнопку "Копировать". Откроется панель создания нового правила фильтрации с указанными параметрами копируемого правила.
- Чтобы сбросить статистику по переданным по правилу пакетам трафика, выделите правило фильтрации и нажмите "Сбросить статистику".

Внимание! При удалении виртуальной машины или сегмента виртуальной инфраструктуры, которые указаны в качестве отправителя или получателя в правилах фильтрации, правила будут выключены, а в соответствующие поля будет установлено значение по умолчанию "Любой".

Активные сессии

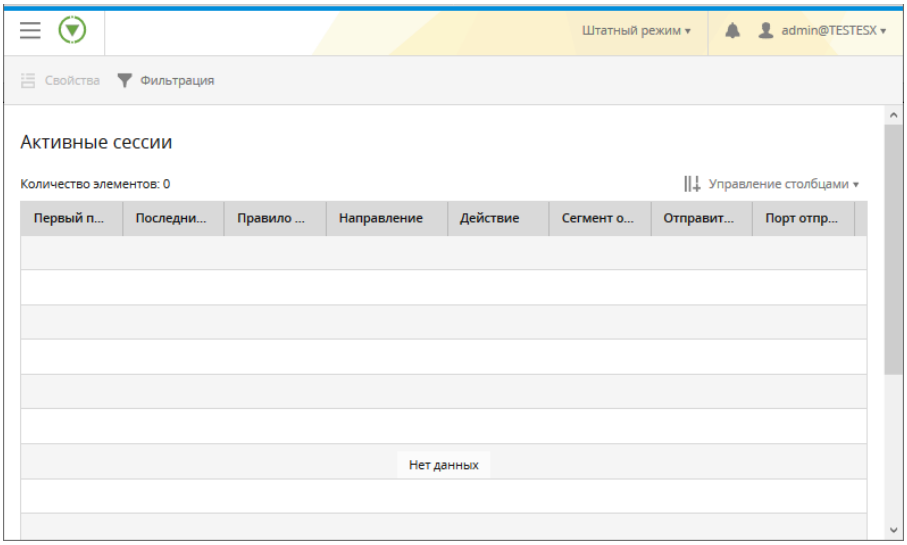
Активные сессии компонента "Сегментирование" содержат информацию о сетевом трафике, переданном или заблокированном в соответствии с правилами фильтрации.

Примечание. Сетевой трафик по правилу фильтрации учитывается в статистике активных сессий, если для правила включено логирование (см. стр.187).

Для просмотра активных сессий:

1. В главном меню выберите раздел "Сегментирование", а затем "Активные сессии".

   На экране появится следующее окно.



   Примечание.
   - Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.
   - Для использования фильтров нажмите кнопку "Фильтрация", в появившемся окне введите текст для поиска в нужное поле и нажмите кнопку "Принять".

2. Выберите из списка нужную сессию и нажмите кнопку "Свойства".

   На экране появится окно с детальной информацией о данной сессии. Чтобы сохранить свойства сессии в буфер обмена, нажмите кнопку "Копировать".

   Примечание. При передаче или блокировании сетевого трафика между двумя виртуальными машинами, в разделе "Активные сессии" будут отображаться две сессии, если обе ВМ контролируются компонентом "Сегментирование". Если же только одна из ВМ контролируется компонентом "Сегментирование", будет отображаться одна сессия.

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.**54**). Настройка подключения описана на стр.**210**.

Панель мониторинга

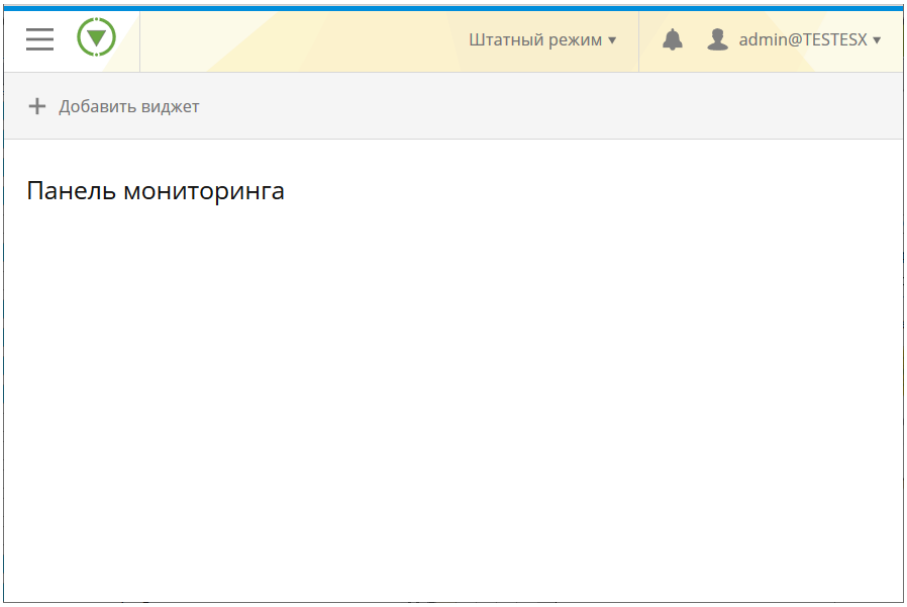
Панель мониторинга представляет собой настраиваемый набор виджетов-диаграмм. Диаграммы в графическом виде отображают данные о событиях и инцидентах, происходящих в виртуальной инфраструктуре.

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

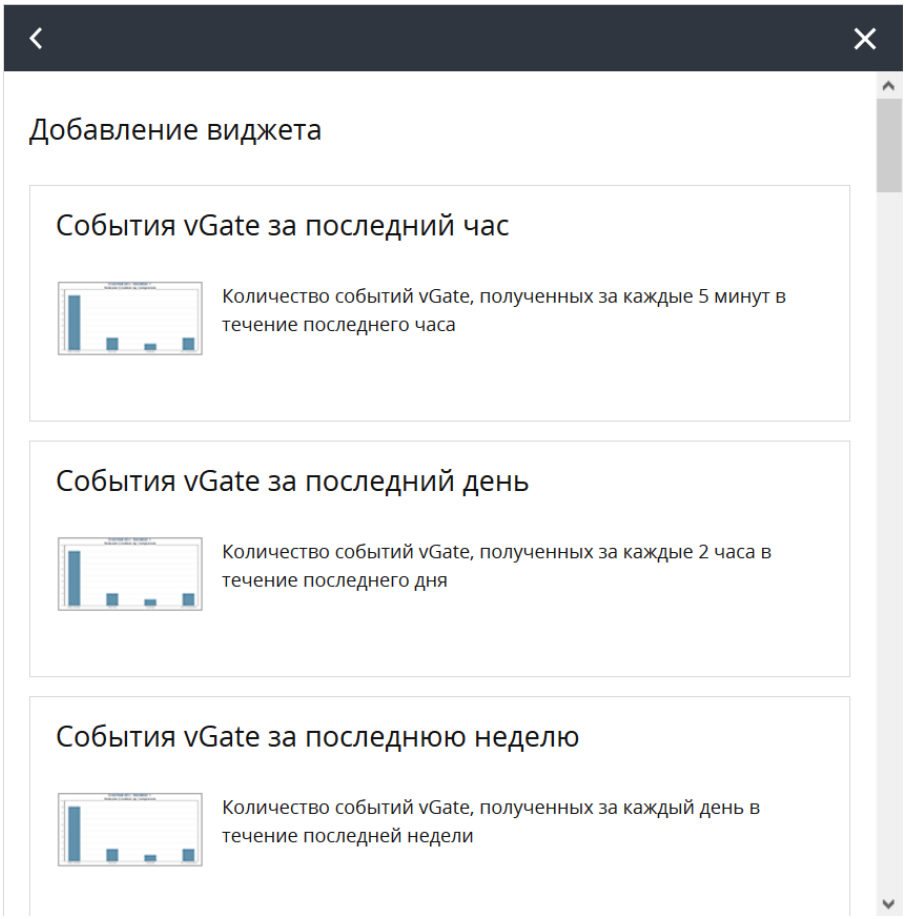
Чтобы настроить панель мониторинга:

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

   На экране появится окно.



2. Нажмите кнопку "Добавить виджет".
   Откроется панель добавления виджетов.



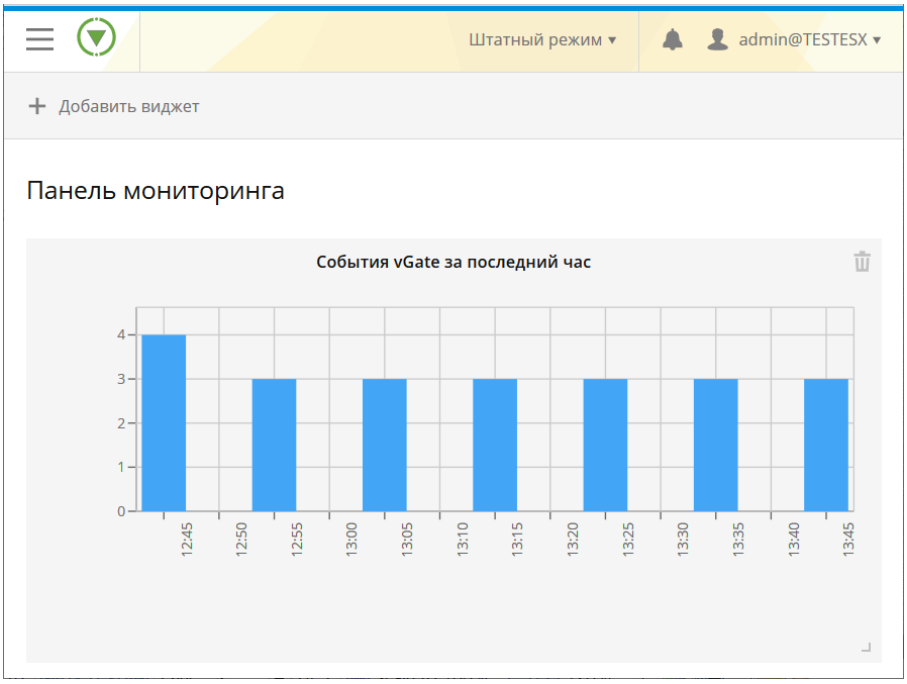
3. Выберите из списка виджет, который необходимо отображать на панели мониторинга.

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

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

Виджет	Описание
Разрешенный трафик между сегментами	Выберите тип виджета: • Топ-10 сегментов по разрешенному трафику — информация о сегментах виртуальной инфраструктуры, для которых передано больше всего сетевого трафика. В статистике учитываются 10 сегментов с наибольшим объемом трафика. • Разрешенный трафик выбранного сегмента — информация о разрешенном сетевом трафике выбранного сегмента виртуальной инфраструктуры. Выберите один сегмент, для которого будет показана статистика. • Разрешенный трафик между выбранными сегментами — информация о разрешенном сетевом трафике между выбранными сегментами виртуальной инфраструктуры. Выберите от двух до 10 сегментов
Заблокированный трафик между сегментами	Выберите тип виджета: • Топ-10 сегментов по заблокированному трафику — информация о сегментах виртуальной инфраструктуры, для которых заблокировано больше всего сетевого трафика. В статистике учитываются 10 сегментов с наибольшим объемом трафика. • Заблокированный трафик выбранного сегмента — информация о заблокированном сетевом трафике выбранного сегмента виртуальной инфраструктуры. Выберите один сегмент, для которого будет показана статистика. • Заблокированный трафик между выбранными сегментами — информация о заблокированном сетевом трафике между выбранными сегментами виртуальной инфраструктуры. Выберите от двух до 10 сегментов

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.

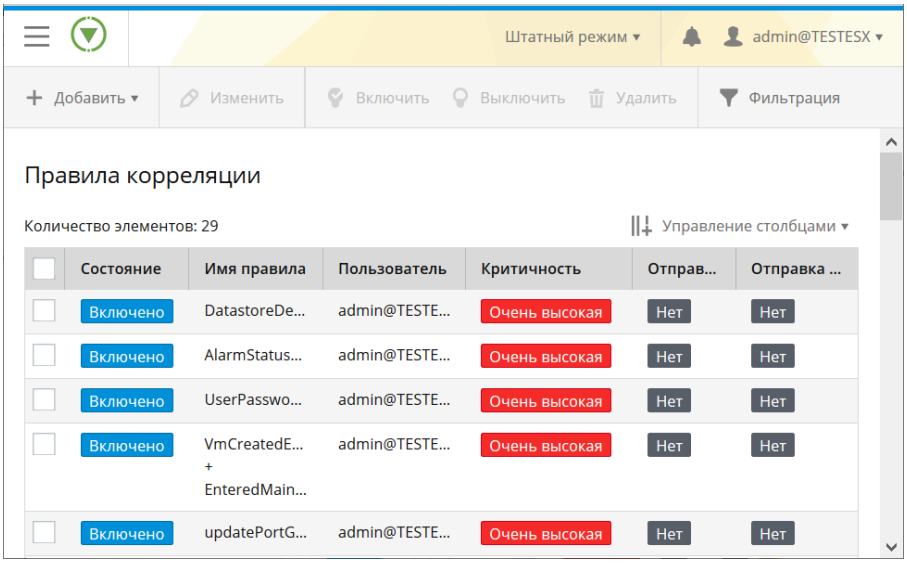
Создание правил корреляции

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.

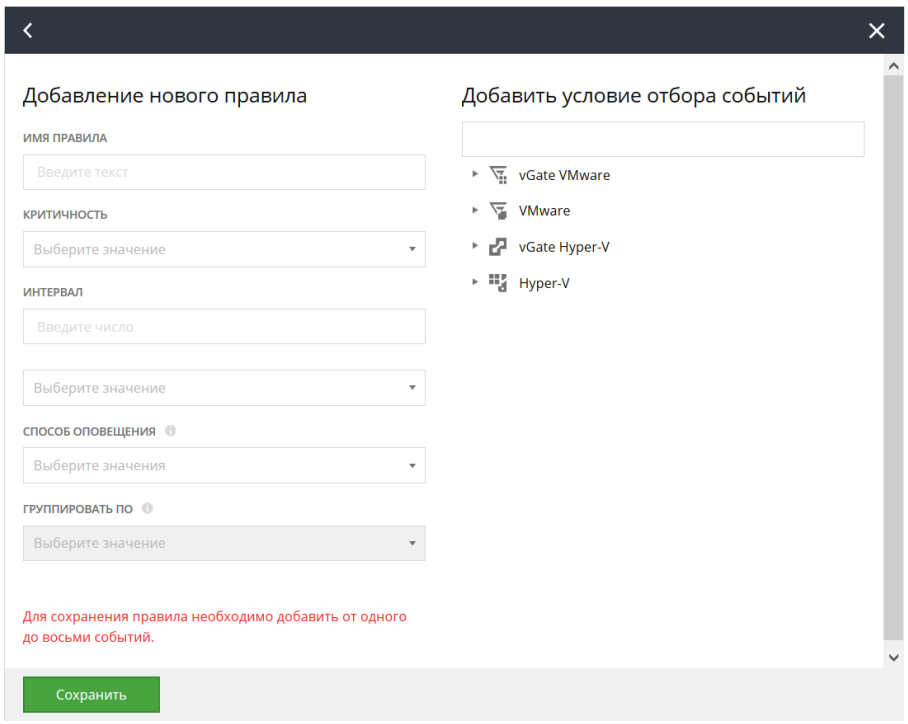


2. Нажмите кнопку "Добавить", в выпадающем списке выберите нужное действие:
   - Добавить правило (см. стр.**196**);
   - Добавить правило по шаблону (см. стр.**198**);
   - Добавить правило в обход vGate (см. стр.**200**).

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

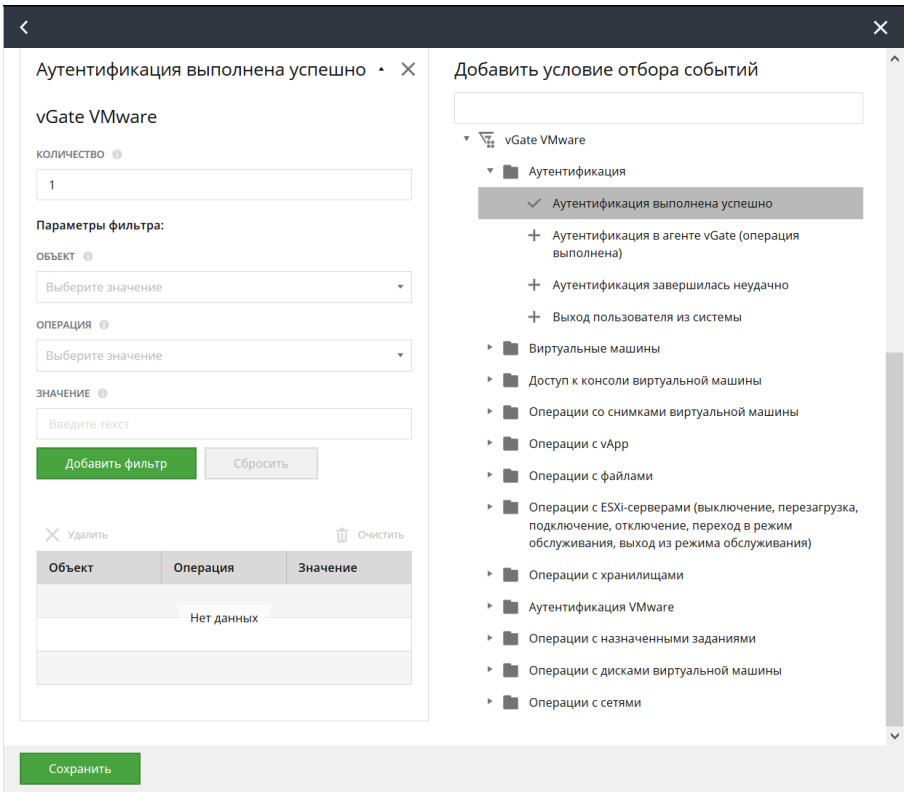


Для добавления правила:

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".

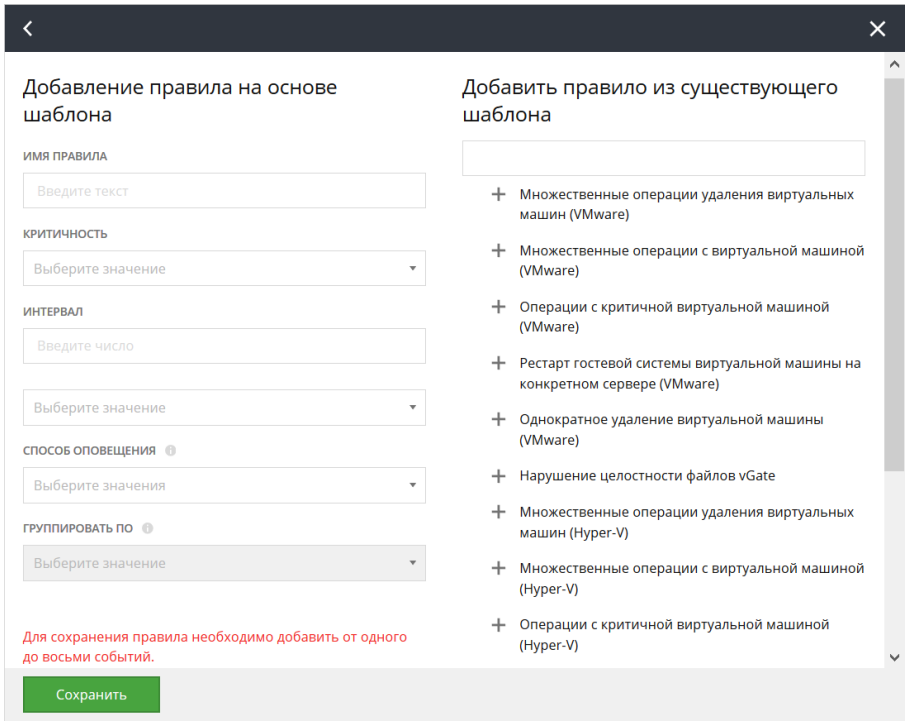
Параметр	Описание
Объект	Выберите один из параметров события
Операция	Выберите из выпадающего списка выражение, подходящее для создания условия: • Содержит; • Равен; • Не равен
Значение	Укажите значение, которое должен принимать выбранный параметр события для срабатывания правила

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

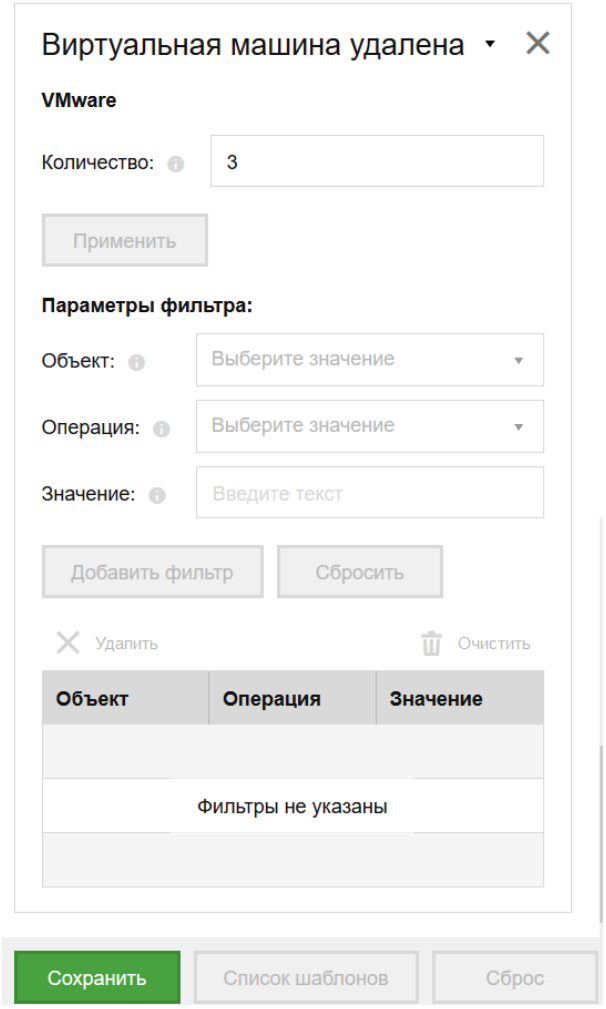


Для добавления правила по шаблону:

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.

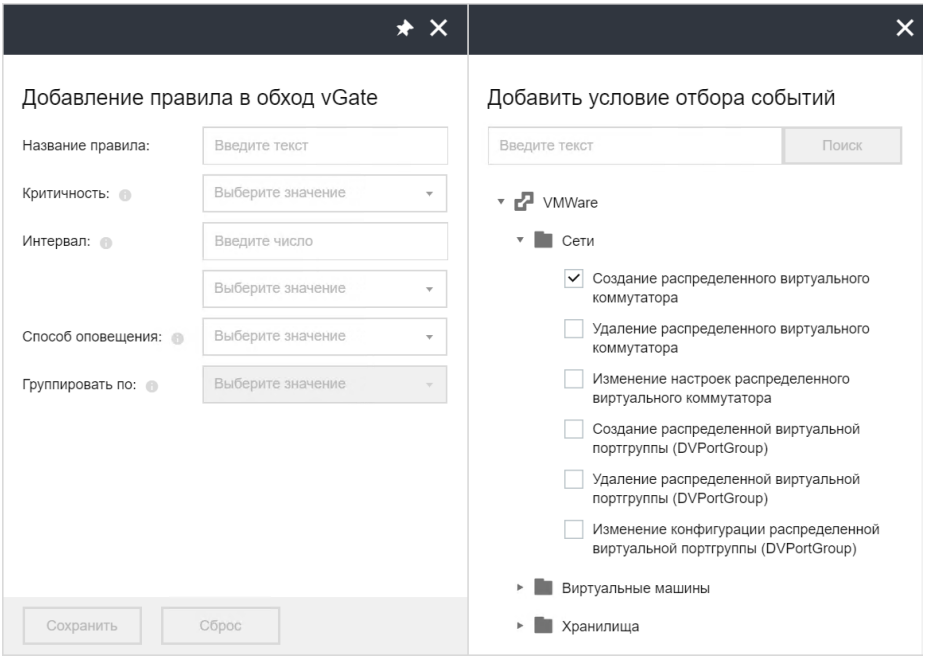
2. Укажите количество событий, необходимых для срабатывания правила, и добавьте фильтры (см. пп. 4, 5 на стр.**196**).

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.

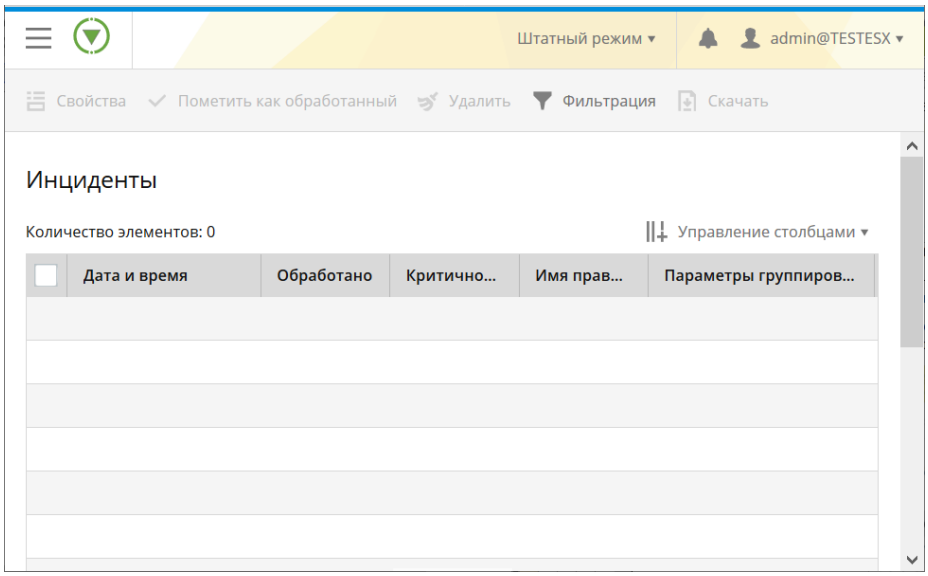
Примечание. Так как информация о событиях на сервере vCenter запрашивается каждые 60 секунд, при создании правила рекомендуется задавать интервал от 90 секунд.

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.191).

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.

Отчеты

В веб-консоли доступен просмотр отчетов о событиях безопасности vGate для vSphere.

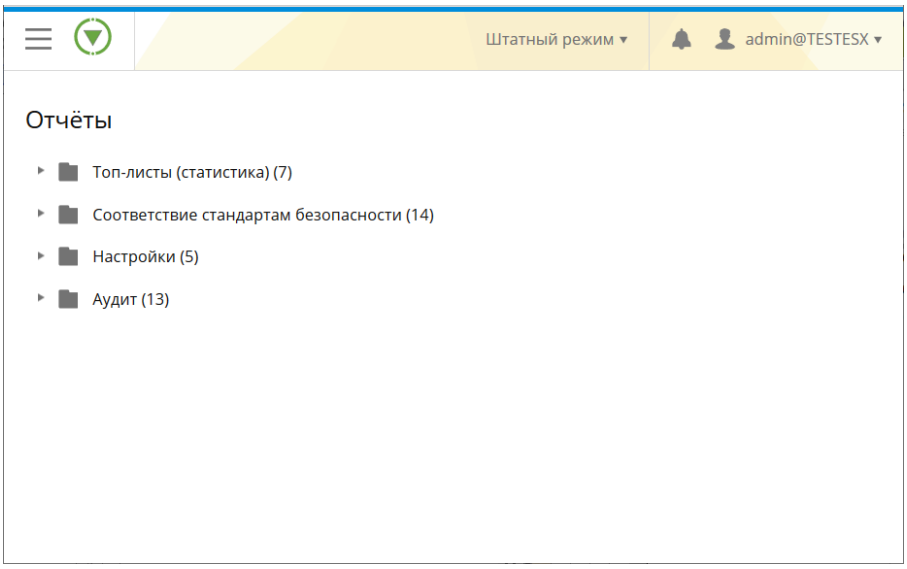
Функция просмотра отчетов о событиях безопасности vGate доступна только в vGate Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

Создание отчетов

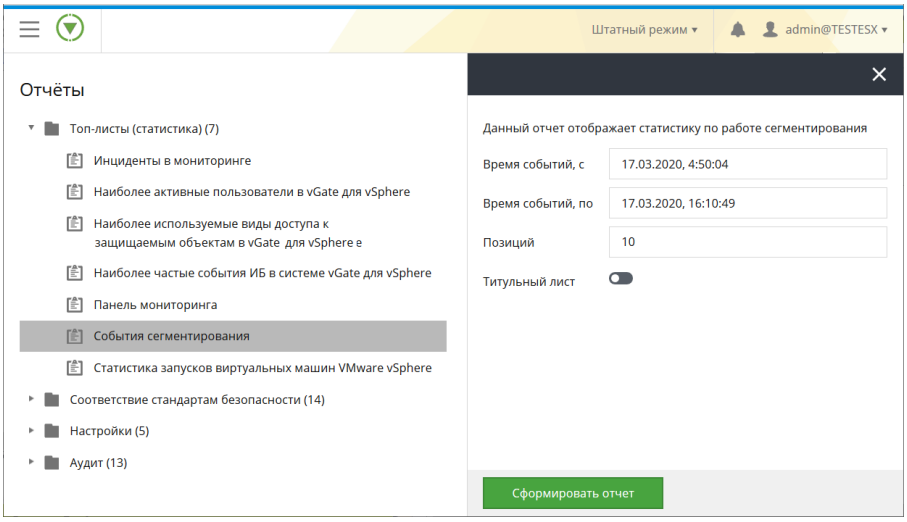
Для создания отчета:

1. В главном меню выберите пункт "Отчеты".

На экране появится окно.



2. Выберите нужный отчет в одной из категорий. В нижней части экрана появятся параметры отчета.



3. При необходимости измените параметры отчета и нажмите кнопку "Сформировать отчет". Отчет будет сформирован на основании заданных настроек (см. стр.**211**).

Журнал событий

Журнал событий vGate аналогичен журналу в консоли управления vGate (см. стр. **169**). В журнале отображается информация об операциях с сегментами виртуальной инфраструктуры, правилах фильтрации трафика и об изменении статусов компонентов защиты vGate . Подробную информацию о заблокированных сетевых пакетах можно просмотреть на ESXi-серверах с помощью утилиты drvmgr.exe.

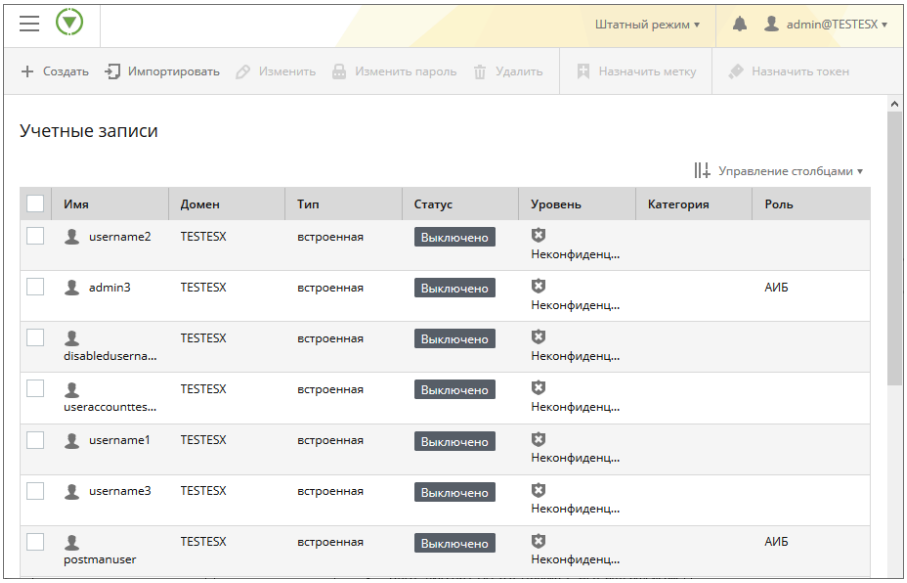
Учетные записи

В веб-консоли доступно управление учетными записями пользователей vGate (подробнее об учетных записях см. стр.**102**).

Для создания учетной записи:

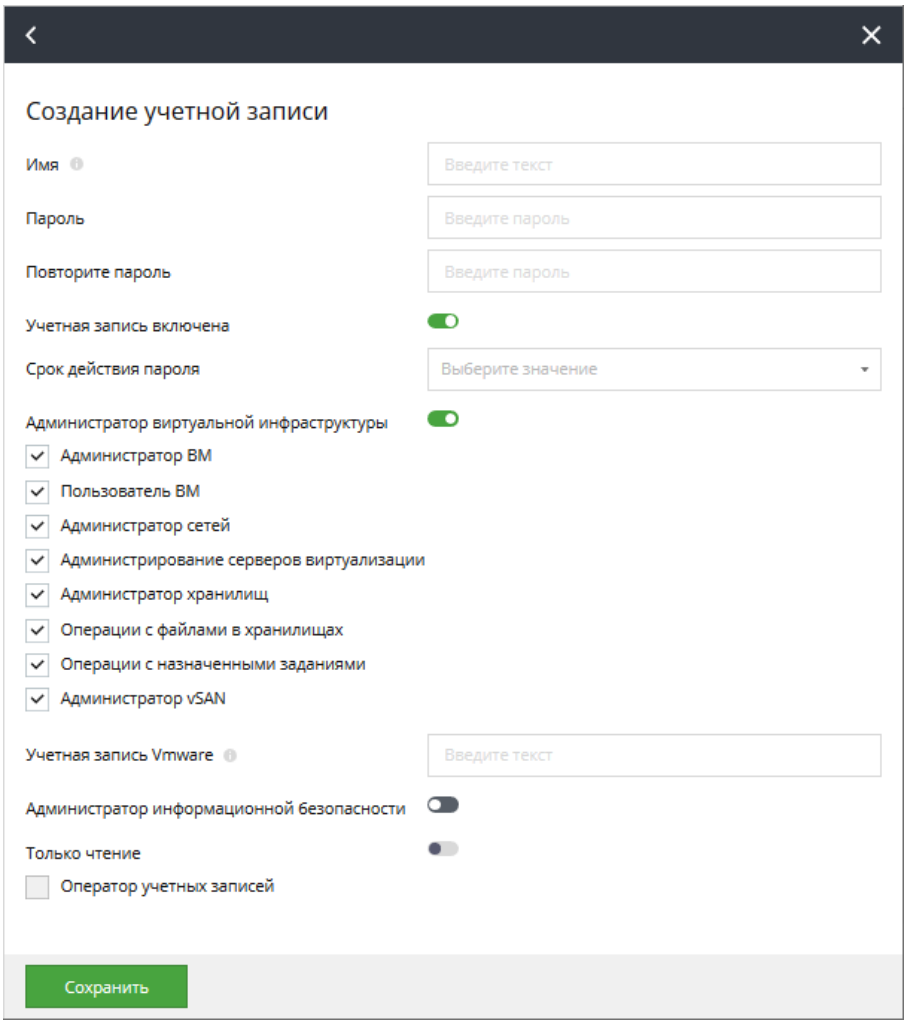
1. В главном меню выберите пункт "Учетные записи".

   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	Для контроля доступа пользователя к среде VMware vSphere укажите в поле "Учетная запись VMware " имя учетной записи администратора vSphere (см. стр.**106**)
Администратор информационной безопасности	Установите переключатель в положение "Вкл" для создания учетной записи администратора информационной безопасности и выберите в списке полномочия, которые будут предоставлены АИБ

Параметр	Описание
Только чтение	Установите переключатель в положение "Вкл", чтобы разрешить создаваемой учетной записи АИБ доступ к vGate только для чтения
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.

Соответствие политикам

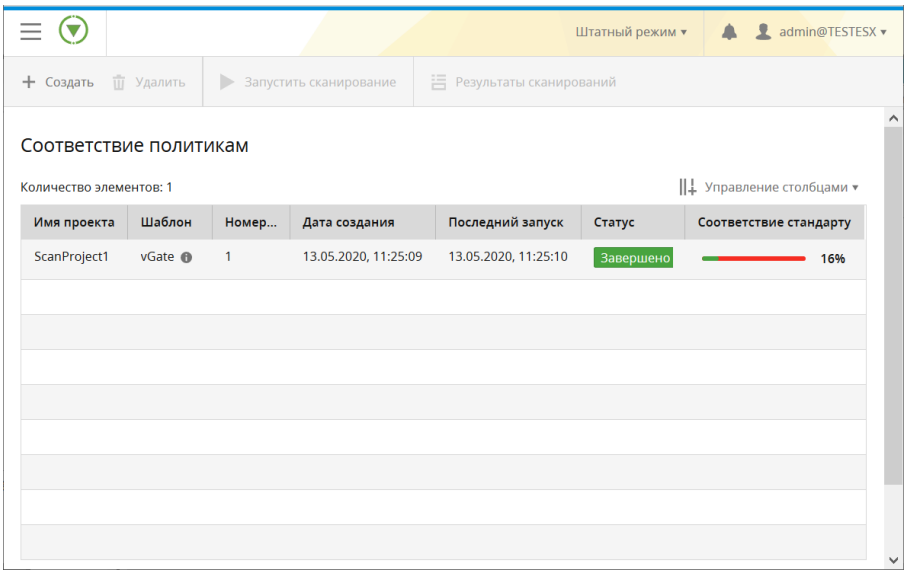
Данная функция доступна только в vGate Enterprise Plus (см. раздел "Функциональные возможности" в документе [1]).

vGate позволяет осуществлять проверку на соответствие защищаемых ESXi-серверов политикам безопасности. Чтобы выполнить проверку, нужно создать проект сканирования.

Для создания проекта сканирования:

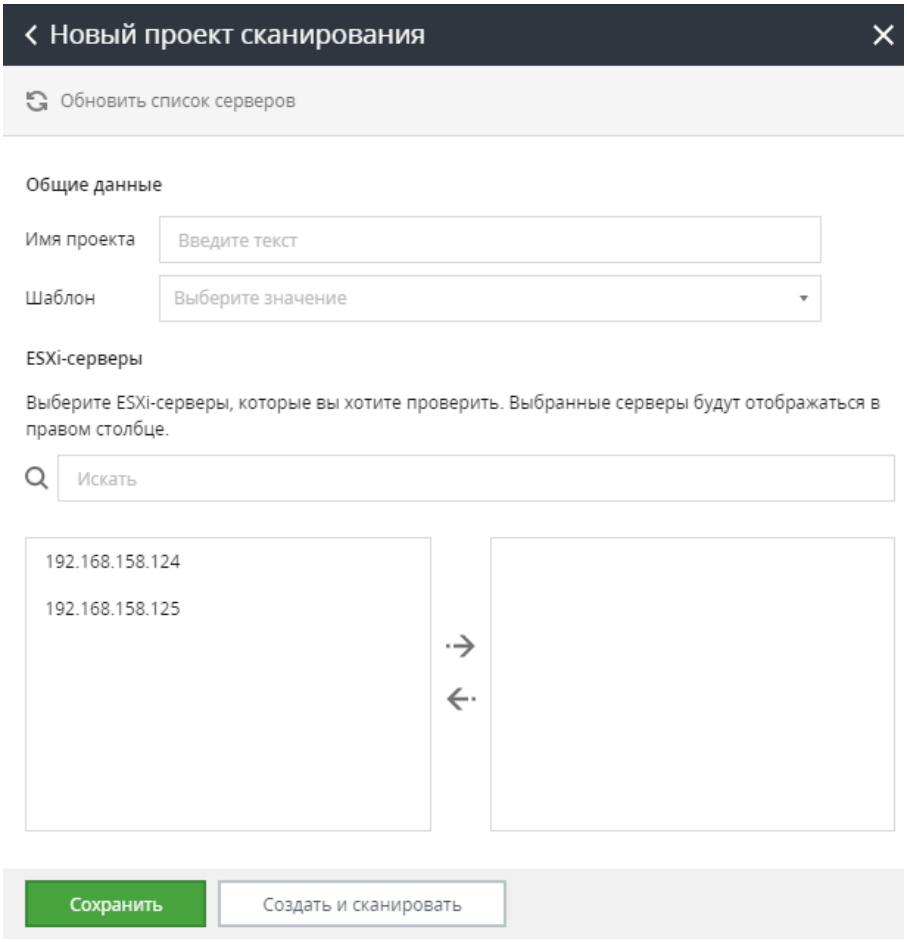
1. В главном меню выберите пункт "Соответствие политикам".

На экране появится окно.



2. Нажмите кнопку "Создать".

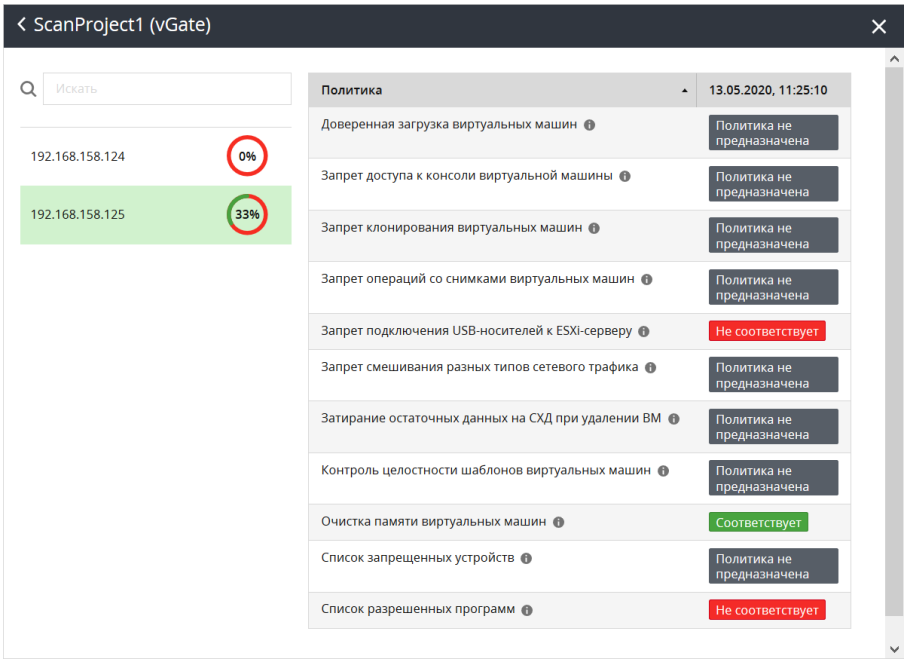
   В правой части окна откроется панель создания проекта сканирования.



3. Укажите имя проекта и выберите шаблон (набор политик безопасности), соответствие которому будет проверяться.
4. Выделите в списке ESXi-серверы, которые необходимо проверить на соответствие выбранному ранее шаблону, и нажмите →.
5. Нажмите кнопку "Сохранить", чтобы сохранить проект или кнопку "Создать и сканировать", чтобы сохранить проект и запустить сканирование.

Для просмотра результатов сканирования:

1. На странице "Соответствие политикам" выделите нужный проект сканирования в списке.
2. Нажмите кнопку "Результаты сканирований". В правой части экрана откроется панель с отчетом о соответствии ESXi-серверов политикам безопасности.



Настройки

В веб-консоли возможно редактирование некоторых настроек vGate. В главном меню выберите раздел "Настройки", а затем перейдите на нужную вкладку:

- Общие (см. стр.**208**);
- Сервер виртуализации (см. стр.**208**);
- Защищаемые подсети (см. стр.**209**);
- Доверенные домены (см. стр.**209**);
- Журнал событий (см. стр.**209**);
- Мониторинг (см. стр.**210**);
- Отчеты (см. стр.**211**);
- Уведомления (см. стр.**211**);
- Лицензия (см. стр.**211**);
- Политики паролей (см. стр.**212**);
- Мандатный контроль доступа (см. стр.**212**).

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.**83**)
Настройки сети и контроля доступа	
Добавлять на клиенте маршрут к защищенной сети	Отметьте, чтобы добавить маршрут к защищенной сети (см. стр.**84**)
Контроль доступа по уровням конфиденциальности	Отметьте, чтобы включить контроль доступа по уровням конфиденциальности (см. стр.**84**)
Контроль доступа по категориям конфиденциальности	Отметьте, чтобы включить контроль доступа по категориям конфиденциальности (см. стр.**84**)
Контроль уровня сессий	Отметьте, чтобы включить контроль уровня сессий (см. стр.**85**)
Настройки автодобавления виртуальных машин	
Включить автодобавление виртуальных машин	Установите выключение в положение "Выкл", чтобы отключить автодобавление для всех групп (см. стр.**112**). 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.**85**)
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

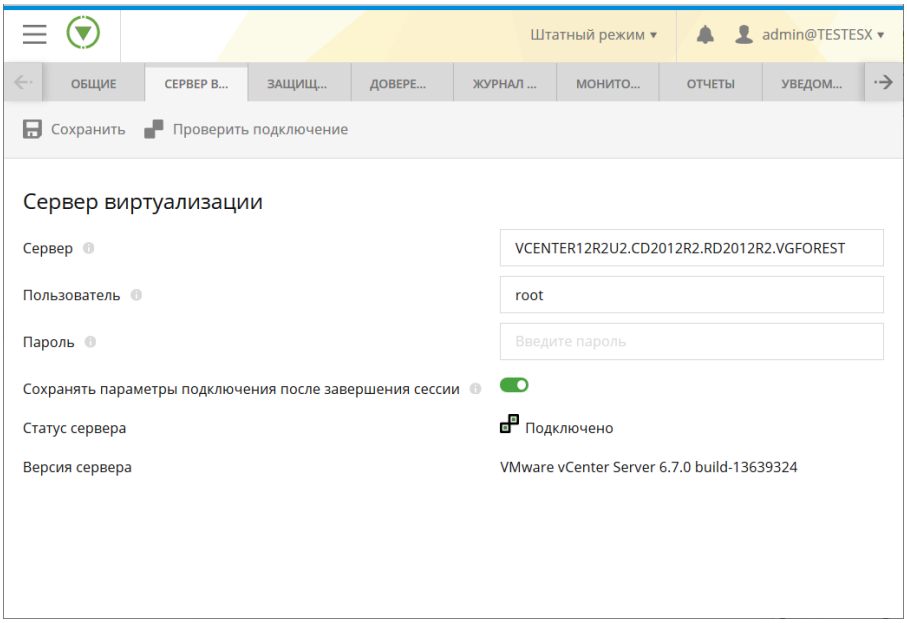
Нажмите кнопку "По умолчанию", чтобы указать значение для параметра, равное 15 минутам.

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.**77**) 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.**78**).

Добавление доверенных доменов

Добавление доверенных доменов в веб-консоли выполняется аналогично добавлению доверенных доменов в консоли управления vGate (см. стр.**85**).

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.**203**)
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.**81**)
Включить Syslog/ Отключить Syslog	Включение/Выключение отправки выбранного сообщения аудита на сервер Syslog. Настройка параметров Syslog выполняется в консоли управления vGate (см. стр.**82**)
Фильтрация	Фильтрация событий аудита. Выполняется аналогично фильтрации в консоли управления vGate (см. стр.**169**)

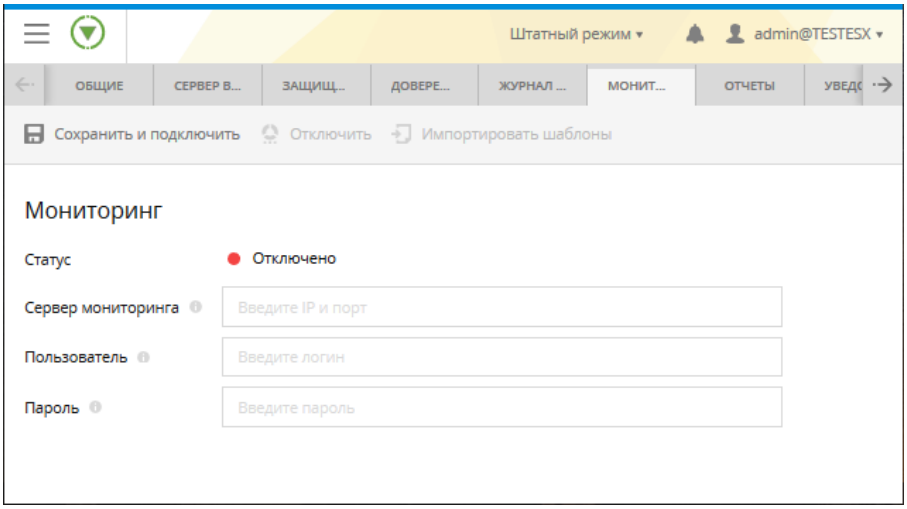
Примечание. Чтобы настроить отображение столбцов в таблице, нажмите "Управление столбцами" и отметьте нужные параметры.

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.**54**)
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.

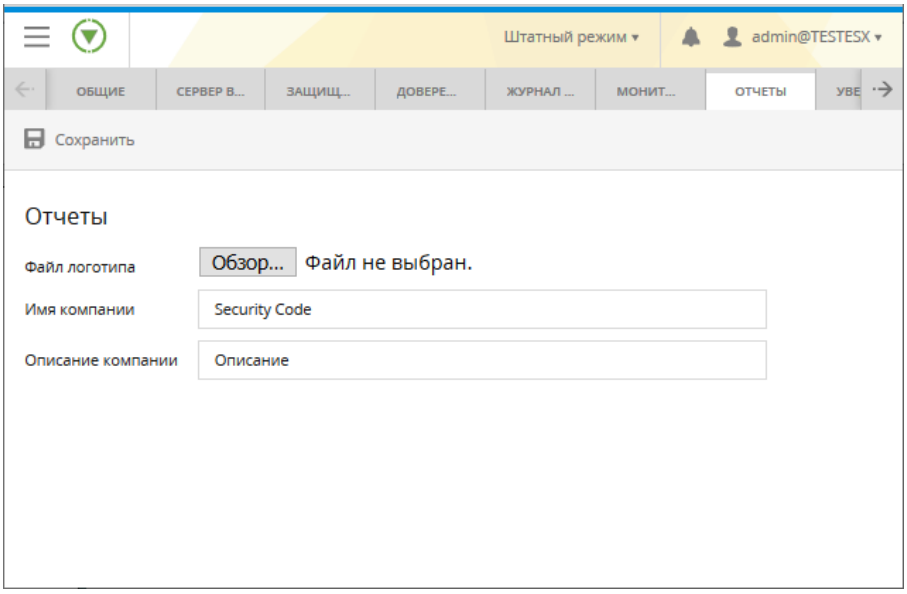
vGate 4.4 поддерживает импорт шаблонов правил корреляции. Для этого нажмите кнопку "Импортировать шаблоны" и выберите нужный файл. Новые шаблоны появятся в списке (см. стр.**198**).

Настройка отчетов

Чтобы настроить параметры создания отчетов:

1. В разделе "Настройки" перейдите на вкладку "Отчеты".

   На экране появится окно.



2. Укажите параметры создания отчетов.

Параметр	Описание
Файл логотипа	Путь к файлу с логотипом компании. Поддерживается загрузка файлов в следующих форматах: *.bmp, *.bzlib, *.cairo, *.flif, *.freetype, *.gslib, *.heic, *.img, *.jp2, *.jpeg, *.lcms, *.lqr, *.lzma, *.openexr, *.pangocairo, *.png, *.ps, *.raw, *.rsvg, *.tiff, *.webp, *.xml, *.zlib размером 150x30 пикселей. Логотип будет размещен на титульном листе отчетов
Имя компании	Название компании, виртуальная инфраструктура которой защищается vGate. Это название будет указано на титульном листе отчетов
Описание компании	Описание компании, виртуальная инфраструктура которой защищается vGate. Это описание будет указано на титульном листе отчетов

3. Нажмите кнопку "Сохранить", чтобы сохранить настройки.

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.**81** и стр.**82**).

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.**107**).

Настройка мандатного контроля доступа

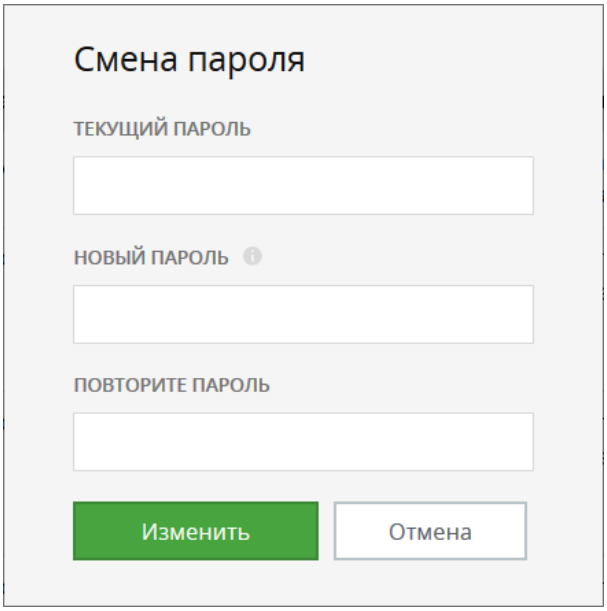
vGate предоставляет возможность определить перечень типов объектов, в отношении которых действует механизм полномочного управления доступом (см. стр.**87**).

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.

Глава 9
Настройка работы View Connection Server

Для корректной работы View Connection Server, входящего в состав ПО VMware View, необходимо выполнить настройку vGate. Порядок настройки различается в зависимости от способа маршрутизации управляющего трафика: с помощью сервера авторизации vGate или с использованием существующего маршрутизатора в сети.

Внимание! Перед выполнением настройки убедитесь в работоспособности всех компонентов VMware View в существующей сетевой инфраструктуре.

Настройка при маршрутизации трафика через сервер авторизации vGate

План действий

Если при развертывании сервера авторизации vGate выбран способ маршрутизации трафика "Маршрутизацию осуществляет сервер авторизации vGate", то для корректной работы View Connection Server необходимо выполнить следующие действия.

№	Шаг	Особенности	Описание
1.	**Размещение View Connection Server**	View Connection Server размещается во внешнем периметре сети администрирования	См. ниже
2.	**Установка агента аутентификации**	Для доступа внутрь защищаемого периметра на View Connection Server необходимо установить агент аутентификации	См. стр.**49**
3.	**Настройка учетной записи**	Для View Connection Server необходимо настроить учетную запись компьютера в vGate	См. стр.**102**
4.	**Настройка ПРД**	Для созданной в предыдущем шаге учетной записи компьютера View Connection Server необходимо настроить определенный набор ПРД для vCenter	См. стр.**213**
5.	**Настройка доступа к vCenter**	Данный шаг необходим, только если на vCenter уже установлен компонент защиты и для доступа к нему View Connection Server используются порты, отличные от заданных по умолчанию. В этом случае следует задать правила доступа View Connection Server к vCenter по нужным портам	См.стр.**143**

Размещение View Connection Server

На компьютере, на котором установлен View Connection Server, должно быть не менее двух Ethernet-интерфейсов, один из которых будет подключен к внешнему периметру сети администрирования виртуальной инфраструктуры, а другой — к сети ВМ, где находятся рабочие места пользователей.

Настройка ПРД для View Connection Server

Для предоставления доступа View Connection Server к vCenter необходимо настроить определенный набор ПРД к vCenter для учетной записи компьютера, где находится View Connection Server. Набор ПРД для предоставления доступа View Connection Server к vCenter содержится в шаблоне "Доступ View Connection сервера к vCenter".

В этом шаблоне указаны порты доступа View Connection Server к vCenter, заданные по умолчанию (8443, 443 и 18443). Если используются порты, отличные от стандартных, необходимо указать номера этих портов в ПРД.

Внимание! При добавлении набора ПРД на основе шаблона "Доступ View Connection сервера к vCenter" убедитесь, что на сервер vCenter не назначено правило доступа к порту 443, действующее для любого пользователя. Если такое правило существует, следует его удалить и создать вместо него аналогичные правила, действующие для определенных пользователей.

Если планируется поддержка View Client with Local Mode, то необходимо настроить еще одно ПРД для учетной записи компьютера, где находится View Connection Server. Это правило должно разрешить доступ к ESXi-серверу, на котором исполняется ВМ с View Transfer Server, по TCP-порту 902.

Подробнее о настройке ПРД см. стр.**137**.

Внимание!

- Для поддержки View Client with Local Mode необходимо в свойствах учетной записи компьютера, на котором находится View Connection Server, отметить пункт "Операции с файлами в хранилищах".
- В целях безопасности настоятельно не рекомендуется предоставлять доступ к другим объектам (или по другим портам) защищаемого периметра для учетной записи компьютера, где находится View Connection Server.

Настройка при использовании стороннего маршрутизатора

Если при развертывании сервера авторизации vGate выбран способ маршрутизации трафика "С помощью существующего маршрутизатора в сети", то реконфигурация существующей сети не требуется. Для корректной работы View Connection Server необходимо выполнить следующие действия.

Для настройки работы View Connection Server:

1. Разместите View Connection Server внутри защищаемого периметра сети администрирования.

   Совет. Защищаемый периметр сети администрирования может состоять из различных подсетей, маршрутизируемых существующим оборудованием. View Connection Server и сервер авторизации vGate могут находиться в одной или в разных подсетях.

2. Добавьте View Connection Server в список защищаемых серверов.

   Совет. Для добавления сервера используйте кнопку-ссылку "Автономный сервер" (см. стр.**98**).

3. Настройте ПРД для доступа АВИ к View Connection Server из внешнего периметра сети администрирования.

   Для управления View Connection Server из внешнего периметра сети администрирования необходимо настроить для View Connection Server набор ПРД на основе шаблона "Доступ администратора к View Connection серверу". В этом шаблоне указаны порты доступа к View Connection Server, заданные по умолчанию (80 и 443). Если используются порты, отличные от стандартных, необходимо указать номера этих портов в ПРД.

   Подробнее о настройке ПРД см. стр.**137**.

4. Настройте существующее сетевое оборудование таким образом, чтобы исключить возможность доступа с рабочих мест АВИ к View Connection Server. Убедитесь в доступности сервера авторизации vGate с рабочих мест АВИ (см. стр.**240**). В этом случае администраторы View Connection Server смогут управлять VMware View только после авторизации в vGate с помощью агента аутентификации.

Приложение

Привилегии пользователей

Разным типам пользователей vGate доступны различные операции в виртуальной инфраструктуре.

Роль	Доступные операции
Администрирование виртуальных машин	**Виртуальные машины** • Включение, выключение, перезагрузка ВМ. • Приостановка работы ВМ. • Доступ к консоли ВМ. • Доступ к консоли ВМ по VMRC. • Изменение конфигурации ВМ. • Перезагрузка гостевой операционной системы. • Выключение гостевой операционной системы. • Клонирование ВМ. • Клонирование ВМ в шаблон. • Конвертация ВМ в шаблон. • Конвертация шаблона в ВМ. • Клонирование шаблона в шаблон. • Миграция ВМ. • Создание ВМ. • Создание ВМ из шаблона. • Удаление ВМ. • Удаление шаблона с диска. • Удаление ВМ из инвентаризации vCenter. • Экспорт ВМ (дополнительно необходимо наличие привилегии "Операции с файлами в хранилищах"). • Удаление каталога для ВМ. • Импорт ВМ. • Импорт ВМ из OVF. • Экспорт ВМ в OVF (дополнительно необходимо наличие привилегии "Операции с файлами в хранилищах"). • Действия со снимками (snapshots) ВМ (создание снимка, переименование снимка, удаление снимка, удаление всех снимков ВМ). • Возврат к последнему снимку ВМ. • Возврат к определенному снимку ВМ. • Консолидация дисков ВМ. • Регистрация ВМ из хранилища. • Регистрация ВМ из хранилища в vApp. • Операции с назначенными заданиями: запуск ВМ, выключение гостевой ОС, перезагрузка гостевой ОС, выключение ВМ, приостановка ВМ, перезагрузка ВМ, миграция ВМ, клонирование ВМ, изменение настроек ВМ, создание снимка ВМ, создание новой ВМ (не поддерживается наследование меток), изменение настроек ВМ, изменение назначенного задания, запуск назначенного задания, удаление назначенного задания. Для выполнения данных операций дополнительно необходимо наличие привилегии "Операции с назначенными заданиями". • Перемещение ВМ в/из vApp или пула ресурсов. **vApp (группа виртуальных машин)** • Запуск, остановка, приостановка vApp. • Клонирование vApp. • Создание vApp. • Удаление vApp с диска. • Удаление каталога для vApp. • Удаление vApp из инвентаризации vCenter. • Экспорт и импорт vApp

Роль	Доступные операции
Пользователь виртуальных машин	**Виртуальные машины** • Включение ВМ. • Выключение ВМ. • Выключение гостевой операционной системы. • Доступ к консоли ВМ. • Перезагрузка гостевой операционной системы. • Перезапуск ВМ. • Приостановка ВМ. • Снятие снимков с консоли ВМ. • Удаление каталога для ВМ. • Операции с назначенными заданиями: запуск ВМ, выключение гостевой ОС, перезагрузка гостевой ОС, выключение ВМ, приостановка ВМ, перезагрузка ВМ, изменение настроек ВМ, изменение назначенного задания, запуск назначенного задания, удаление назначенного задания. Для выполнения данных операций дополнительно необходимо наличие привилегии "Операции с назначенными заданиями". **vApp (группа виртуальных машин)** • Запуск vApp. • Остановка vApp. • Приостановка vApp
Администрирование сетей	• Создание групп портов (port groups). • Изменение групп портов. • Удаление каталога для ВМ. • Изменение настроек виртуальных коммутаторов
Администрирование серверов виртуализации	• Ввод сервера в состав кластера. • Управление режимом обслуживания (Maintenance mode) сервера виртуализации. • Управление режимом Lockdown (Lockdown mode) сервера виртуализации. • Отключение сервера виртуализации от vCenter. • Подключение/переподключение сервера виртуализации к vCenter. • Выключение сервера виртуализации. • Перезагрузка сервера виртуализации. • Управление режимом ожидания сервера виртуализации. • Просмотр лог-файлов ESXi-серверов. • Загрузка файлов в хранилище AutoDeploy. • Удаление сервера в составе кластера из инвентаризации vCenter. • Удаление кластера из инвентаризации vCenter. • Удаление каталога для сервера. • Удаление каталога для ВМ. • Добавление автономного сервера к vCenter. • Добавление сервера в кластер к vCenter. • Запуск/остановка/перезапуск службы сервера. • Изменение политик службы сервера. • Включение, изменение, отключение правил брандмауэра. • Изменение расширенных настроек сервера. • Изменение настроек времени.

Роль	Доступные операции
	• Изменение времени. • Управление запуском ВМ. • Управление уровнем доверия пакетов. • Установка обновлений пакетов. • Изменение настроек шифрования дампов. • Перемещение сервера в кластер/из кластера. • Создание/изменение/удаление профиля сервера. • Назначение/применение/открепление профиля сервера. • Назначение/применение/открепление профиля сервера (применение в кластере). • Включение/изменение/отключение правил брандмауэра. • Изменение индивидуальных настроек сервера. • Изменение индивидуальных настроек сервера (применение в кластере). • Сброс индивидуальных настроек сервера. • Увеличение емкости vFlash-ресурса. • Операции с назначенными заданиями: добавление сервера в кластер, изменение настроек пула ресурсов, изменение назначенного задания, запуск назначенного задания, удаление назначенного задания. Для выполнения данных операций дополнительно необходимо наличие привилегии "Операции с назначенными заданиями"
Администрирование хранилищ	• Просмотр содержимого хранилищ. • Удаление хранилища (дополнительно нужна привилегия "Администрирование серверов виртуализации"). • Операции с файлами в хранилищах. • Форматирование дисков ВМ. • Изменение объема хранилищ. • Изменение объема дисков виртуальных машин. • Создание хранилища (дополнительно нужна привилегия "Администрирование серверов виртуализации"). • Переименование хранилища. • Монтирование хранилища (дополнительно нужна привилегия "Администрирование серверов виртуализации"). • Размонтирование хранилища (дополнительно нужна привилегия "Администрирование серверов виртуализации"). • Монтирование/Переименование/Удаление NFS - хранилища (дополнительно нужна привилегия "Администрирование серверов виртуализации"). • Расширение хранилища. • Очистка таблицы разделов. • Удаление каталога для ВМ

Роль	Доступные операции
Администратор vSAN	• Включение/выключение кластера vSAN. • Включение/выключение дедупликации и сжатия. • Включение/выключение шифрования. • Изменение настроек шифрования. • Генерация новых ключей шифрования. • Изменение опции "Разрешить уменьшенную избыточность". • Включение/выключение vSAN iSCSI Target Service. • Изменение vSAN Advanced Options. • Запрос неиспользуемых дисков. • Создание группы дисков. • Добавление дисков в группу. • Удаление диска из группы/удаление группы дисков. • Монтирование группы дисков. • Размонтирование группы дисков. • Пересоздание группы дисков. • Конфигурирование отказоустойчивого домена. • Добавление хоста в домен. • Удаление хоста из домена. • Удаление отказоустойчивого домена. • Конфигурирование Stretched Cluster. • Отключение Stretched Cluster. • Изменение Witness host. • Добавление vSAN iSCSI Target. • Редактирование vSAN iSCSI Target. • Удаление vSAN iSCSI Target. • Добавление Allowed Initiators в vSAN iSCSI Target. • Удаление Allowed Initiator из vSAN iSCSI Target. • Создание, изменение и удаление vSAN iSCSI LUN. • Подключение и отключение vSAN iSCSI LUN. • Создание и удаление vSAN iSCSI Initiator Group. • Добавление vSAN iSCSI Initiator в Initiator Group. • Удаление vSAN iSCSI Initiator из Initiator Group. • Добавление Accessible Target для клиента/группы. • Удаление Accessible Target для клиента/группы
Операции с файлами в хранилищах	• Загрузка файлов и папок в хранилище. • Скачивание файлов и папок из хранилища. • Импорт ВМ из OVF. • Экспорт ВМ в OVF (дополнительно необходимо наличие привилегии "Администрирование виртуальных машин").

Доступ к файлам виртуальных машин

Для доступа к файлам виртуальных машин, находящимся в системе хранения данных (СХД), необходимо выполнить настройку ПО 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.**104**).
2. Для нужного ESXi-сервера создайте правило "Управление виртуальной инфраструктурой ESXi", действующее для пользователя, в отношении которого выполнено действие **1**.

Если серверов ESXi несколько, то правило нужно создать для каждого из них.

TCP- и UDP-порты, используемые в среде vSphere

ESXi-сервер

Порт	Протокол	Отправитель	Получатель	Назначение
9	UDP	vCenter Server	ESXi Host	Wake-on-LAN
22	TCP	SSH Client	ESXi Host	SSH
53	UDP	ESXi Host	DNS Server	DNS-клиент
68	UDP	DHCP Server	ESXi Host	DHCP-клиент для IPv4
80	TCP	Web Browser	ESXi Host	Приветственная страница со ссылками на скачивание для различных интерфейсов
161	UDP	SNMP Server	ESXi Host	Позволяет ESXi-серверам подключаться к SNMP-серверу
427	TCP/UDP	CIM Server	ESXi Host	CIM-клиент использует Service Location Protocol, version 2 (SLPv2), чтобы найти серверы CIM
443	TCP	vSphere Web Client	ESXi Host	Подключения клиента
546	TCP/UDP	DHCP Server	ESXi Host	DHCP-клиент для IPv4
547	TCP/UDP	ESXi Host	DHCP Server	DHCP-клиент для IPv4
902	TCP/UDP	VMware vCenter Agent	ESXi Host	Компонент защиты сервера vCenter
2233	TCP	ESXi Host	vSAN Transportr	vSAN reliable datagram transport. Использует TCP и используется для ввода-вывода хранилища vSAN. Если отключено, vSAN не работает
3260	TCP	ESXi Host	Software iSCSI Client	ПО для iSCSI
5671	TCP	ESXi Host	rabbitmqproxyr	Прокси-сервер на ESXi-сервере, который позволяет приложениям, работающим внутри виртуальных машин, связываться с AMQP-брокерами в сетевом домене vCenter. Виртуальная машина не обязательно должна находиться в сети, то есть сетевой адаптер не требуется. Прокси-сервер подключается к брокерам в сетевом домене vCenter, поэтому IP-адреса исходящих соединений должны включать, по крайней мере, текущих используемых брокеров или будущих брокеров. Брокеры могут быть добавлены, если клиент хочет выполнить масштабирование

Порт	Протокол	Отправитель	Получатель	Назначение
5988, 8889	TCP	CIM Server 8889-OpenWSMAN Daemon	ESXi Host	5988 — сервер CIM (Common Information Model). 8889 — WS-Management (Web Services Management)
5989	TCP	CIM Secure Server	ESXi Host	Сервер CIM secure
6999	UDP	NSX Distributed Logical Router Service	ESXi Host	Служба виртуального распределенного маршрутизатора NSX (NSX Virtual Distributed Router or NSX Distributed Logical Router in earlier versions of the product). Порт брандмауэра, связанный с этой службой, открывается при установке NSX VIBs и создании модуля VDR. Если с хостом не связаны никакие экземпляры VDR, порт не обязательно должен быть открыт
8000	TCP	ESXi Host	ESXi Host	Требуется для миграции виртуальной машины с помощью vMotion. ESXi-серверы прослушивают порт 8000 для TCP-соединений с удаленных ESXi-серверов для трафика vMotion
8080	TCP	vsanvp	ESXi Host	VSAN VASA Vendor Provider. Используется службой управления хранилищами (SMS), входящей в состав vCenter, для доступа к информации о профилях vSAN, возможностях и соответствии требованиям. Если этот параметр отключен, управление профилем vSAN (SPBM) не работает
8100, 8200, 8300	TCP/UDP	Fault Tolerance	ESXi Host	Трафик между серверами для vSphere Fault Tolerance (FT)
8301, 8302	UDP	DVSSync	ESXi Host	Порты DVSSync используются для синхронизации состояний распределенных виртуальных портов между серверами, на которых включена запись/воспроизведение VMware FT. Эти порты должны быть открыты только для серверов, на которых работают основные или резервные виртуальные машины. На хостах, которые не используют VMware FT, эти порты не обязательно должны быть открыты
12345, 23451	UDP	ESXi Host	vSAN Clustering Service	Cluster Monitoring, Membership, and Directory Service, используемые vSAN

Порт	Протокол	Отправитель	Получатель	Назначение
44046, 31031	TCP	ESXi Host	HBR	Используется vSphere Replication и VMware Site Recovery Manager для исходящего трафика репликации
80, 9000	TCP	ESXi Host	vCenter Server	vSphere Update Manager

vCenter

Порт	Протокол	Назначение
22	TCP	Системный порт для SSHD
53	TCP/UDP	Порт службы DNS
80	TCP	Сервер vCenter требует порт 80 для прямых HTTP-соединений. Порт 80 перенаправляет запросы на HTTPS-порт 443
88	TCP	Сервер Active Directory. Этот порт должен быть открыт для подключения сервера к Active Directory
123	UDP	Порт NTP-клиента
135	UDP	Порт vCenter Server Appliance, предназначенный для аутентификации Active Directory
161	UDP	Порт SNMP-сервера
389	TCP/UDP	Порт LDAP для служб каталогов группы серверов vCenter. Порт должен быть открыт на локальном и всех удаленных серверах vCenter
443	TCP	Порт, используемый системой vCenter Server по умолчанию для прослушивания подключений от клиента vSphere. Нужен для получения данных о доступе сторонних клиентов к серверам
514	TCP/UDP	Порт vSphere Syslog Collector для сервера vCenter на Windows и порт vSphere Syslog Service для vCenter Server Appliance
636	TCP	Порт vCenter Single Sign-On LDAPS Только для обратной совместимости с vSphere 6.0
902	TCP/UDP	Порт, используемый сервером vCenter по умолчанию для отправки данных на управляемые хосты. Управляемые хосты также регулярно отправляют данные через UDP-порт 902 на сервер vCenter. Этот порт не должен быть заблокирован брандмауэрами между сервером и хостами или между хостами
1514	TCP	Порт vSphere Syslog Collector TLS для vCenter Server на Windows и порт vSphere Syslog Service TLS для vCenter Server Appliance
2012	TCP	Порт интерфейса управления RPC для vCenter Single Sign-On
2014	TCP	RPC-порт для всех VMCA (VMware Certificate Authority) APIs
2015	TCP	Порт для управления DNS
2020	TCP/UDP	Порт для управления аутентификацией
5480	TCP	Порт Appliance Management Interface
6500	TCP/UDP	Порт ESXi Dump Collector
6501	TCP	Порт службы Auto Deploy

Порт	Протокол	Назначение
6502	TCP	Порт управления Auto Deploy
7080, 12721	TCP	Внутренние порты Secure Token Service
7081	TCP	Внутренний порт VMware Platform Services Controller Web Client
7475, 7476	TCP	Порт VMware vSphere Authentication Proxy
8109	TCP	Порт службы VMware Syslog Collector. Служба нужна для организации централизованного сбора лог-файлов
8200, 8201, 8300, 8301	TCP	Appliance management Note: Internal ports
8084	TCP	vSphere Update Manager SOAP port for vSphere v6.x vSphere Lifecycle Manager SOAP port for vSphere v7.x
9084	TCP	vSphere Update Manager Web Server Port for vSphere v6.x vSphere Lifecycle Manager Web Server Port for vSphere v7.x The HTTP port used by ESXi hosts to access host patch files from vSphere Update Manager server.
9087	TCP	vSphere Update Manager Web SSL Port for vSphere v6.x vSphere Lifecycle Manager Web SSL Port for vSphere v7.x The HTTPS port used by vSphere Update Manager client plug-in to upload host upgrade files to vSphere Update Manager server.
9443	TCP	vSphere Client HTTPS
15007, 15008	TCP	vService Manager (VSM). This service registers vCenter Server extensions. Open this port only if required by extensions that you intend to use.
15080	TCP	Analytics service internal port
31031, 44046 (по умолчанию)	TCP	vSphere Replication.
5355	UDP	The systemd-resolve process uses this port to resolve domain names, IPv4 and IPv6 addresses, DNS resource records and services.

Порты vCenter для внутреннего взаимодействия

Порт	Протокол	Назначение
5443	TCP	Внутренний порт для графического пользовательского интерфейса сервера vCenter
5444, 5432		Внутренний порт для мониторинга vPostgreSQL
5090	TCP	Внутренний порт для графического пользовательского интерфейса сервера vCenter
7080	TCP	Внутренний порт Secure Token Service
7081	UDP	Внутренний порт Platform Services Controller
8000	UDP	Внутренний порт ESXi Dump Collector
8006	UDP	Мониторинг работоспособности Virtual SAN
8085	TCP/UDP	Внтутренни епорты, используемые службой vCenter VPXD SDK
8095	TCP	Порт для служб VMware vCenter
8098, 8099	TCP/UDP	Порт, используемый VMware Image Builder Manager

Порт	Протокол	Назначение
8190, 8191, 22000, 22100, 21100	TCP	Порт службы VMware vSphere Profile-Driven Storage
8200, 8201, 5480	TCP/UDP	Внутренние порты Appliance Management
8300, 8301	TCP	Зарезервированные порты Appliance Management
8900	TCP	Внутренний порт мониторинга API
9090	TCP	Внутренний порт для vSphere Web Client
10080	TCP	Внутренний порт службы Inventory
10201	TCP/UDP	Внутренний порт Message Bus Configuration Service
11080	TCP	Внутренние порты vCenter Server Appliance для HTTP и заставки экрана
12721	TCP/UDP	Внутренний порт службы Secure Token
12080	TCP	Внтутренний порт службы лицензирования
12346, 12347, 4298	TCP	Внутренний порт для VMware Cloud Management SDKs (vAPI)
13080, 6070	TCP	Порт, используемый службой Performance Charts
14080	TCP	Порт, используемый службой Syslog
15005, 15006	TCP	Внутренний порт ESX Agent Manager
16666, 16667	TCP	Порты Content Library

Список шаблонов правил доступа

Протокол	Исходящий порт	Порт назначения
Управление виртуальной инфраструктурой ESXi-сервера		
TCP	Любой	443
TCP	Любой	902
Доступ к консоли виртуальной машины		
TCP	Любой	902
Доступ к ESXi по протоколу SSH		
TCP	Любой	22
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
UDP	Любой	53
UDP	Любой	88
UDP	Любой	135
UDP	Любой	138
UDP	Любой	389

Протокол	Исходящий порт	Порт назначения
UDP	Любой	445
UDP	Любой	464
Проверка доступности хоста (команда ping)		
ICMP	Любой	Любой
Разрешить поиск DNS-имен		
UDP	Любой	53
Доступ пользователя к vCenter		
TCP	Любой	80
TCP	Любой	443
TCP	Любой	514
TCP	Любой	1514
TCP	Любой	6500
TCP	Любой	6501
TCP	Любой	6502
TCP	Любой	8000
TCP	Любой	8001
TCP	Любой	8084
TCP	Любой	9084
TCP	Любой	9087
TCP	Любой	8098
TCP	Любой	8099
TCP	Любой	8109
Доступ View Connection сервера к vCenter		
TCP	Любой	443
TCP	Любой	8443
TCP	Любой	18443
Доступ администратора к View Connection Server		
TCP	Любой	443
TCP	Любой	80
Доступ к отчетам для vGate Report Viewer		
TCP	Любой	902
Администрирование сервера авторизации vGate		
TCP	Любой	3802
TCP	Любой	3803
TCP	Любой	443
Администрирование сервера авторизации vGate через веб-консоль		
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

Протокол	Исходящий порт	Порт назначения
Разрешить доступ к службе авторизации vGate		
TCP	Любой	3801
UDP	Любой	3801
TCP	Любой	3800
UDP	Любой	3800
UDP	Любой	88
UDP	Любой	750

Протокол	Исходящий порт	Порт назначения
Подключение пользователя с помощью vSphere Web Client v6.x/v7.x		
TCP	Любой	443
Доступ Web Client Remote Console Plug-in к vCenter		
TCP	Любой	443
Доступ пользователя к vRealize Operations Manager		
TCP	Любой	443
Доступ пользователя к серверу Platform Services Controller без vCenter		
TCP	Любой	443

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.**85**). 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**
VM PowerOn (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 ESXi-сервера должен быть не меньше уровня конфиденциальности ВМ. Иначе уровень конфиденциальности ESXi-сервера должен быть равен уровню конфиденциальности ВМ	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Список категорий ESXi-сервера должен включать хотя бы одну из категорий ВМ
VM PowerOff/Reset/Suspend (останов, приостановка, возобновление ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ
Restart Guest/Shutdown Guest (перезапуск, завершение ОС ВМ)	
Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ	Список категорий пользователя должен включать хотя бы одну из категорий ВМ
VM Migrate (VMMotion) (миграция, перемещение ВМ)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ESXi-сервера, на который перемещается ВМ (целевого). **2.** Если для целевого ESXi-сервера отмечено поле "Разрешено исполнять ВМ с меньшим уровнем", то уровень конфиденциальности целевого ESXi-сервера должен быть не меньше уровня конфиденциальности ВМ. Иначе уровень конфиденциальности целевого ESXi-сервера должен быть равен уровню конфиденциальности ВМ	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ESXi-сервера, на который перемещается ВМ (целевого). **2.** Список категорий целевого ESXi-сервера должен включать хотя бы одну из категорий ВМ
VM Delete from Disk (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**
VM Create (создание ВМ)	
ВМ автоматически назначается уровень конфиденциальности хранилища, выбранного для хранения дисков ВМ. **1.** Уровень сессии пользователя должен быть равен уровню конфиденциальности ESXi-сервера. **2.** Если на последнем шаге создания ВМ выбрано Edit the virtual machine settings before completion, то уровень конфиденциальности ВМ должен быть равен уровню конфиденциальности виртуальной сети, к которой подключена ВМ (при наличии виртуальной сети)	ВМ автоматически назначается категория из списка категорий хранилища, совпадающая с категорией из списка категорий пользователя. Если таковых несколько, то ВМ назначается список категорий. **1.** Список категорий пользователя должен включать хотя бы одну из категорий ESXi-сервера. **2.** Если на последнем шаге создания ВМ выбрано Edit the virtual machine settings before completion, то список категорий ВМ должен включать хотя бы одну из категорий каждой из виртуальных сетей, к которым подключена ВМ (при их наличии)
Relocate VM (Change Datastore) (перемещение ВМ, смена хранилища)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности целевого ESXi-сервера, на который перемещается ВМ. **2.** Если для целевого ESXi-сервера отмечено поле "Разрешено исполнять ВМ с меньшим уровнем", то уровень конфиденциальности целевого ESXi-сервера должен быть не меньше уровня конфиденциальности ВМ. Иначе уровень конфиденциальности целевого ESXi-сервера должен быть равен уровню конфиденциальности ВМ. **3.** Если для целевого хранилища отмечено поле "Разрешено хранить ВМ с меньшим уровнем", то уровень конфиденциальности хранилища должен быть не меньше уровня конфиденциальности ВМ. Иначе уровень конфиденциальности целевого хранилища должен быть равен уровню конфиденциальности ВМ	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ESXi-сервера, на который перемещается ВМ (целевого). **2.** Список категорий целевого ESXi-сервера должен включать хотя бы одну из категорий ВМ. **3.** Список категорий целевого хранилища должен включать хотя бы одну из категорий ВМ
VM Edit settings (редактирование параметров 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**
VM Edit Network VM Properties->Edit Settings->Hardware->Add->Ethernet Adapter (добавление сетевого адаптера). VM Properties->Edit Settings->Hardware->[выбор адаптера]->Remove (удаление сетевого адаптера). VM Properties->Edit Settings->Hardware->[выбор адаптера]->Network Label (изменение группы портов)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности ВМ. **2.** Если для ВМ отмечено поле "Разрешено подключаться к сетям с меньшим уровнем", уровень конфиденциальности ВМ должен быть не меньше уровней конфиденциальности каждой из виртуальных сетей, к которым подключена ВМ, или физического адаптера (если виртуальные сети не используются). Если поле "Разрешено подключаться к сетям с меньшим уровнем" не отмечено, то уровень конфиденциальности ВМ должен быть равен уровню конфиденциальности виртуальной сети, к которой подключена ВМ, или физического адаптера (если виртуальные сети не используются)	**1.** Список категорий пользователя должен включать хотя бы одну из категорий ВМ. **2.** Список категорий ВМ должен включать хотя бы одну из категорий каждой из виртуальных сетей, к которым подключена ВМ (при их наличии), или физического сетевого адаптера (если виртуальные сети не используются)
Update Network Config Host Properties->Configuration->Networking->Add Networking (добавление виртуальной сети). Host Properties->Configuration->Networking->[выбор vSwitch]->Properties->Ports->Add (добавление порта на виртуальном коммутаторе)	
Если поле "Разрешен трафик для VLAN с меньшим уровнем" не отмечено, то уровень конфиденциальности виртуальной сети должен быть равен уровню конфиденциальности физического сетевого адаптера. Если поле отмечено, то уровень конфиденциальности каждой виртуальной сети должен быть не выше уровня конфиденциальности физического сетевого адаптера	Список категорий виртуальной сети должен включать хотя бы одну из категорий физического сетевого адаптера
Add Port Group (добавление группы портов)	
Если поле "Разрешен трафик для VLAN с меньшим уровнем" не отмечено, то уровень конфиденциальности виртуальной сети должен быть равен уровню конфиденциальности физического сетевого адаптера	Список категорий виртуальной сети должен включать хотя бы одну из категорий физического сетевого адаптера
Update Port Group Host Properties->Configuration->Networking->[выбор vSwitch]->Properties->Ports-> [выбор портгруппы]->Edit (редактирование параметров портгруппы)	
Если поле "Разрешен трафик для VLAN с меньшим уровнем" не отмечено, то при попытке изменить виртуальную сеть проверяется, что уровни конфиденциальности исходной виртуальной сети и новой равны	Список категорий виртуальной сети должен включать хотя бы одну из категорий физического сетевого адаптера

Условия выполнения операций	
Уровень конфиденциальности	**Категории конфиденциальности**
Update Virtual Switch Host Properties->Configuration->Networking->[выбор vSwitch]->Properties->Network Adapter-> Add (добавление сетевого адаптера). Host Properties->Configuration->Networking->[выбор vSwitch]->Properties->Network Adapter-> Remove (удаление сетевого адаптера)	
Если поле "Разрешен трафик для VLAN с меньшим уровнем" не отмечено, то уровень конфиденциальности виртуальной сети должен быть равен уровню конфиденциальности нового физического сетевого адаптера	Список категорий виртуальной сети должен включать хотя бы одну из категорий физического сетевого адаптера
VM Add Virtual Disk (добавление виртуального диска)	
Если для хранилища отмечено поле "Разрешено хранить ВМ с меньшим уровнем", то уровень конфиденциальности хранилища должен быть не меньше уровня конфиденциальности ВМ. Иначе уровень конфиденциальности целевого хранилища должен быть равен уровню конфиденциальности ВМ	Список категорий ВМ должен включать хотя бы одну из категорий хранилища
ESXi Browse data storage (доступ к хранилищу)	
Уровень конфиденциальности пользователя[2] должен быть не меньше уровня конфиденциальности хранилища	Список категорий пользователя должен включать хотя бы одну из категорий хранилища
Delete file in Browse data store dialog (удаление файла ВМ через диалог "Browse data store")	
Уровень конфиденциальности сессии должен быть равен уровню конфиденциальности хранилища	Список категорий пользователя должен включать хотя бы одну из категорий хранилища
Copy/Move file in Browse data store dialog (копирование/перемещение файла ВМ через диалог "Browse data store")	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности исходного хранилища. **2.** Если для целевого хранилища отмечено поле "Разрешено хранить ВМ с меньшим уровнем", то уровень конфиденциальности целевого хранилища должен быть не меньше уровня конфиденциальности исходного. Иначе уровни конфиденциальности исходного и целевого хранилищ должны быть равны	**1.** Список категорий пользователя должен включать хотя бы одну из категорий хранилища. **2.** Список категорий исходного хранилища должен включать хотя бы одну из категорий целевого хранилища

[2] Не путайте уровень сессии пользователя и его уровень конфиденциальности. Уровень конфиденциальности пользователя задает АИБ посредством консоли управления. Уровень сессии определяет АВИ перед началом работы в защищенном режиме.

Условия выполнения операций	
Уровень конфиденциальности	**Категории конфиденциальности**
Copy/Move file in Browse data store file from VMware Remote Command Line Interface (RCLI) (копирование/перемещение файла ВМ через RCLI в другое хранилище)	
1. Уровень сессии пользователя должен быть равен уровню конфиденциальности хранилища. **2.** Если для целевого хранилища отмечено поле "Разрешено хранить ВМ с меньшим уровнем", то уровень конфиденциальности целевого хранилища должен быть не меньше уровня конфиденциальности исходного. Иначе уровни конфиденциальности исходного и целевого хранилищ должны быть равны	**1.** Список категорий пользователя должен включать хотя бы одну из категорий хранилища. **2.** Список категорий исходного хранилища должен включать хотя бы одну из категорий целевого хранилища

Параметры настраиваемых политик безопасности

При формировании набора политик может потребоваться настройка некоторых политик безопасности. Политики, настройка которых обязательна, перечислены в начале списка со статусом "Не настроено". Их параметры необходимо задать перед сохранением создаваемого набора.

Примечание. До тех пор пока для всех политик со статусом "Не настроено" не будут настроены дополнительные параметры (например, пароль, IP-адрес и т. д.), сохранить набор политик будет невозможно (на месте кнопки "Завершить" будет расположена недоступная кнопка "Далее").

Для большей части политик безопасности, у которых есть настраиваемые параметры, обязательная настройка при формировании набора не требуется. Такие политики следует настраивать в зависимости от требований к выполняемым ими проверкам.

Настраиваемые политики безопасности с описанием их параметров перечислены в таблицах ниже.

Параметры политик, настройка которых обязательна

Параметр	Описание
Контроль за доступом через VMSafe CPU/Mem API	
Разрешить VMSafe API	Отметьте этот пункт, чтобы разрешить доступ к виртуальным машинам через программный интерфейс VMSafe
IP-адрес виртуальной машины защиты VMSafe	IP-адрес виртуальной машины, которая используется для защиты других ВМ с помощью технологий VMSafe
TCP-порт виртуальной машины защиты VMSafe	TCP-порт виртуальной машины защиты VMSafe (по умолчанию 65535)
Настройка брандмауэра ESXi-сервера для ограничения доступа к службам, работающим на сервере	
Правила фильтрации сетевых пакетов	Для добавления правила выберите службу в раскрывающемся списке, укажите диапазон IP-адресов или подсетей, с которых разрешен доступ к портам этой службы, и нажмите кнопку "Добавить". Правила задаются в формате: "Ruleset Name: 1.1.1.1, 2.2.2.2/24, 3.3.3.3". Например: DNS Client: 192.168.3.0/24, 172.28.0.0/16
Настройка постоянного журналирования на ESXi-сервере	
Путь к	Путь к файлу журнала на ESXi-сервере. Например: [datastore name]/logfiles/hostname.log

Параметр	Описание
Отсылка событий сервера виртуализации на syslog-сервер	
IP-адрес сервера syslog	IP-адрес удаленного сервера syslog
Порт сервера syslog	Порт сервера syslog. По умолчанию 514

Параметры прочих настраиваемых политик

Параметр	Описание
Аудит модулей ядра гипервизора без цифровой подписи	
Модули ядра без подписи	Список неподписанных модулей ядра гипервизора, разрешенных к загрузке. Для добавления модуля в список укажите его название и нажмите кнопку "Добавить"
Группы портов не настроены на значения native VLAN	
Значение идентификатора native VLAN	Значение идентификатора native VLAN (по умолчанию 1), который запрещается использовать на группах портов виртуального коммутатора ESXi-сервера
Доверенная загрузка виртуальных машин	
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
Целостность BIOS ВМ	Отметьте этот пункт, чтобы включить контроль целостности файлов конфигурации BIOS (файлов NVRAM)
Перечень снимков ВМ	Отметьте этот пункт, чтобы включить контроль целостности файлов конфигурации снимков ВМ (файлов VMSD)
Контроль конфигурации ВМ	Список контролируемых параметров конфигурации ВМ (параметров файла VMX). Отметьте нужные пункты списка, чтобы задать перечень параметров, изменение значений которых будет контролироваться политикой. Подробнее о соответствии параметров из данного списка и конкретных параметров VMX-файла см. стр.**158**
Контроль целостности шаблонов виртуальных машин	
Разрешены операции с шаблоном ВМ при нарушении целостности	По умолчанию данный пункт отмечен. Удалите отметку, чтобы запретить операции с шаблоном при несоответствии контрольных сумм файлов шаблона их эталонным значениям
Целостность BIOS шаблона ВМ	По умолчанию данный пункт отмечен. Удалите отметку, чтобы выключить контроль целостности файлов конфигурации BIOS (файлов NVRAM) шаблона ВМ
Целостность образов виртуальных дисков	Отметьте этот пункт, чтобы включить контроль целостности образов виртуальных дисков шаблона ВМ (файлов VMDK). Операция подсчета контрольных сумм образов дисков может занять длительное время
Задать ограничение допустимого времени простоя сессий ESXi Shell и SSH	
Ограничение времени простоя сессий Shell и SSH (в секундах)	Период времени, по окончании которого автоматически завершаются неиспользуемые сессии Shell и SSH. По умолчанию равен 300 секундам
Задать ограничение допустимого времени работы служб ESXi Shell и SSH	
Ограничение времени работы служб Shell и SSH (в секундах)	Период времени, по окончании которого автоматически останавливаются службы ESXi Shell и SSH. По умолчанию равен 600 секундам

Параметр	Описание
Запрет некоторых скрытых возможностей	
Остановить HGFS-сервер	Отметьте этот пункт, чтобы запретить использование сервера HGFS (Host Guest File System). Остановка HGFS-сервера приведет к тому, что API, использующие его для отправки/приема файлов на/с гостевую систему (некоторые VIX-команды или VMware Tools auto-upgrader), не будут работать
Затирание остаточных данных на СХД при удалении ВМ	
Тайм-аут операции зануления (в минутах)	Период времени, отведенный на выполнение операции зануления, по истечении которого она считается неудавшейся и требующей перезапуска. По умолчанию равен 60 минутам
Затирание остаточных данных на СХД при удалении ВМ (двукратная запись)	
Тайм-аут операции зануления (в минутах)	Период времени, отведенный на выполнение операции зануления, по истечении которого она считается неудавшейся и требующей перезапуска. По умолчанию равен 60 минутам
Использование протокола CHAP для iSCSI-устройств	
Проверить двустороннюю аутентификацию CHAP	Отметьте это поле, чтобы включить проверку использования двусторонней аутентификации CHAP
Контроль за доступом через dvfilter Network API	
Список фильтров в формате "ethernetX.filterN.name = filter name"	Список фильтров доступа в формате "ethernet0.filter1.name = dv-filter1", где "ethernet0" — сетевой адаптер виртуальной машины, "filter1" – номер фильтра, "dv-filter1" — имя модуля ядра, реализующего защиту ВМ. Для добавления правила в список укажите его в данном поле и нажмите кнопку "Добавить"
Настроить централизованное хранилище для сбора дампов памяти ESXi-сервера с помощью ESXi Dump Collector	
Сервер хранения дампов памяти (IP-адрес:порт)	IP-адрес и порт сервера для хранения дампов памяти (в качестве разделителя используется символ ":")
Активный интерфейс сетевого хранилища дампов памяти	Имя сетевого адаптера ESXi-сервера (например, vmk0)
Настройки логирования виртуальных машин на ESXi-сервере	
Количество файлов	Количество лог-файлов для одновременного хранения на ESXi-сервере (по умолчанию 10)
Размер файла (байт)	Размер лог-файла в байтах. Значение по умолчанию — 1 000 000 байт
Ограничение размера информационных сообщений от виртуальной машины в VMX-файл	
Максимальный размер VMX-файла (байт)	Максимальный размер VMX-файла в байтах. Значение по умолчанию — 1 048 576 байт

Параметр	Описание
Отключение ненужных устройств	
IDE	Отметьте этот пункт для проверки подключения к ESXi-серверу устройств через интерфейс IDE
Floppy	Отметьте этот пункт для проверки подключения к ESXi-серверу дисководов гибких магнитных дисков
Parallel	Отметьте этот пункт для проверки подключения к ESXi-серверу устройств через параллельный порт
Serial	Отметьте этот пункт для проверки подключения к ESXi-серверу устройств через последовательный порт
USB	Отметьте этот пункт для проверки подключения к ESXi-серверу устройств через порт USB
Проверка настроек SNMP-агента (только для ESXi)	
SNMP-агент включен	Отметьте этот пункт при использовании рассылки уведомлений о событиях аудита по протоколу SNMP
Порт SNMP-агента	Порт SNMP-агента. По умолчанию 161
SNMP-сообщества (communities)	Имя сообщества SNMP. При указании нескольких сообществ в качестве разделителя используйте символ ";"
Адреса для приема данных SNMP (в виде server@port/community)	Адрес сервера для приема SNMP-сообщений в формате server@port/community. При указании нескольких серверов в качестве разделителя используйте символ ";"
Проверка описаний и уровней поддерживаемости VIB-пакетов	
Уровень поддержки (acceptance level)	Уровень поддерживаемости (acceptance level), которому должны соответствовать VIB-пакеты, разрешенные к установке на ESXi-сервер. Доступные значения: PartnerSupported, VMwareAccepted или VMwareCertified
Синхронизация времени	
Пул NTP-серверов	Список NTP-серверов, используемых для синхронизации времени. Для добавления нового сервера в пул NTP-серверов укажите его адрес и нажмите кнопку "Добавить". Для ESXi-сервера версии 7.0 допускается добавление только IP-адреса NTP-сервера. Для удаления сервера из списка нажмите "Удалить"
Создание политики сложности паролей	
PAM module arguments	Параметры модуля pam_passwdqc.so, используемые в политике сложности паролей. Значение по умолчанию — retry=5 min=disabled,disabled,disabled,disabled,14
Список запрещенных устройств	
Список устройств	Список виртуальных устройств, запрещенных для подключения к виртуальной машине. Для добавления нового типа устройств укажите его название или выберите нужное значение из раскрывающегося списка и нажмите "Добавить"

Параметр	Описание
Список разрешенных программ	
Список программ	Список программ, которые разрешено запускать на ESXi-сервере. Для добавления программы в список нажмите кнопку "Добавить"
Принудительно завершать неразрешенные программы	Отметьте этот пункт, чтобы предотвратить возможность запуска неразрешенных программ. В противном случае при запуске программы из списка регистрируется событие аудита без запрета на запуск программы
Установить доверенным пользователям DCUI.Access для обхода запрета на вход	
Доверенные пользователи	Укажите в данном поле имя учетной записи пользователя, которому будет разрешен прямой доступ к ESXi-серверу, и нажмите кнопку "Добавить". По умолчанию в список включен администратор ESXi-сервера (пользователь root)

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 и на рабочем месте АИБ. Для вызова подробной информации об утилите откройте редактор командной строки и введите следующую команду:

```
clacl.exe –H
```

Экспорт и импорт конфигурации vGate

С помощью утилиты clacl.exe можно выполнить экспорт или импорт конфигурации vGate.

Для экспорта конфигурации:

- Откройте редактор командной строки и выполните следующую команду:

  clacl common export-objects -x **<путь к файлу>** -k **<администратор>** -s **<пароль>**

  где

  - x **<путь к файлу>** — путь к файлу в формате XML, в который будет записана конфигурация vGate;
  - **<администратор>** — имя АИБ;
  - **<пароль>** — пароль АИБ.

Для импорта конфигурации:

- Откройте редактор командной строки и выполните следующую команду:

  clacl common import-objects -x **<путь к файлу>** -e **<true/false>** -k **<администратор>** -s **<пароль>**

  где

  - x **<путь к файлу>** — путь к файлу в формате XML, из которого нужно произвести импорт конфигурации;
  - e **<true/false>** — если параметр указан с аргументом **true**, то конфигурация будет обновлена даже при возникновении конфликтов с текущей конфигурацией vGate.

Примечание. Во время работы утилиты может появляться сообщение о необходимости указать дополнительные параметры, например, адрес сервера vCenter и данные учетной записи администратора vSphere.

Выборочная установка компонента защиты vCenter

С помощью утилиты clacl.exe можно осуществить выборочную установку компонента защиты vCenter.

Для первоначальной установки без компонента "Контроль доступа vSphere":

- Откройте редактор командной строки и выполните следующую команду:

  clacl.exe deploy install-vpx --features drv –h **<vCenter>** –u **<пользователь Windows>** –w **<пароль Windows>** --vc-user **<администратор>** --vc-password **<пароль>** –i **<сервер авторизации>** –k **<АИБ>** –s **<пароль АИБ>**

  где

  - drv — имя компонента "Контроль сетевых подключений";
  - **<vCenter>** — имя или IP-адрес сервера vCenter ;
  - **<пользователь Windows>** — имя пользователя Windows для доступа к компьютеру с vCenter;
  - **<пароль Windows>** — пароль пользователя Windows для доступа к компьютеру с vCenter;
  - **<администратор>** — имя администратора vGate;
  - **<пароль>** — пароль администратора vGate;
  - **<сервер авторизации>** — имя или IP-адрес сервера авторизации vGate;
  - **<АИБ>** — имя АИБ;
  - **<пароль АИБ>** — пароль АИБ vGate.

Для переустановки без компонента "Контроль доступа vSphere":

- Откройте редактор командной строки и выполните следующую команду:

  clacl.exe deploy modify-vpx - d vcp –h **<vCenter>** –u **<пользователь Windows>** –w **<пароль Windows>** --vc-user **<администратор>** --vc-password **<пароль>** –i **<сервер авторизации>** –k **<АИБ>** –s **<пароль АИБ>**

  где

  vcp — имя компонента "Контроль доступа vSphere".

Для установки без компонента "Контроль сетевых подключений":

- Откройте редактор командной строки и выполните следующую команду:

  clacl.exe deploy modify-vpx -d drv -h **<vCenter>** –u **<пользователь Windows>** –w **<пароль Windows>** --vc-user **<администратор>** --vc-password **<пароль>** –i **<сервер авторизации>** –k **<АИБ>** –s **<пароль АИБ>**.

Для установки всех компонентов:

- Откройте редактор командной строки и выполните следующую команду:

  clacl.exe deploy install-vpx --features vcp,drv -h **<vCenter>** – u **<пользователь Windows>** – w **<пароль Windows>** - - vc- user **<администратор>** --vc-password **<пароль>** –i **<сервер авторизации>** –k **<АИБ>** –s **<пароль АИБ>**.

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 drvmgr.exe

Правила фильтрации сетевых соединений сервера vCenter можно создать с помощью специальной утилиты командной строки drvmgr.exe.

Внимание! Если на vCenter установлена операционная система Windows Server 2012 R2 и 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 vCenter, 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	

Например, для добавления правила, разрешающего входящие соединения из сети 172.28.36.0 по любому протоколу на любой входящий порт vCenter, формат команды следующий:

```
>drvmgr A any 172.28.36.0:any,255.255.255.0 any 4
```

Для удаления вышеуказанного правила следует использовать команду:

```
>drvmgr R any 172.28.36.0:any,255.255.255.0 any 4
```

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 наличии сервера vCenter команда может содержать следующие ключи:

- vc (-v) — имя или IP-адрес сервера vCenter;
- user (-u) — имя пользователя для доступа к серверу vCenter;
- pwd (-w) — пароль пользователя для доступа к серверу vCenter.

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.

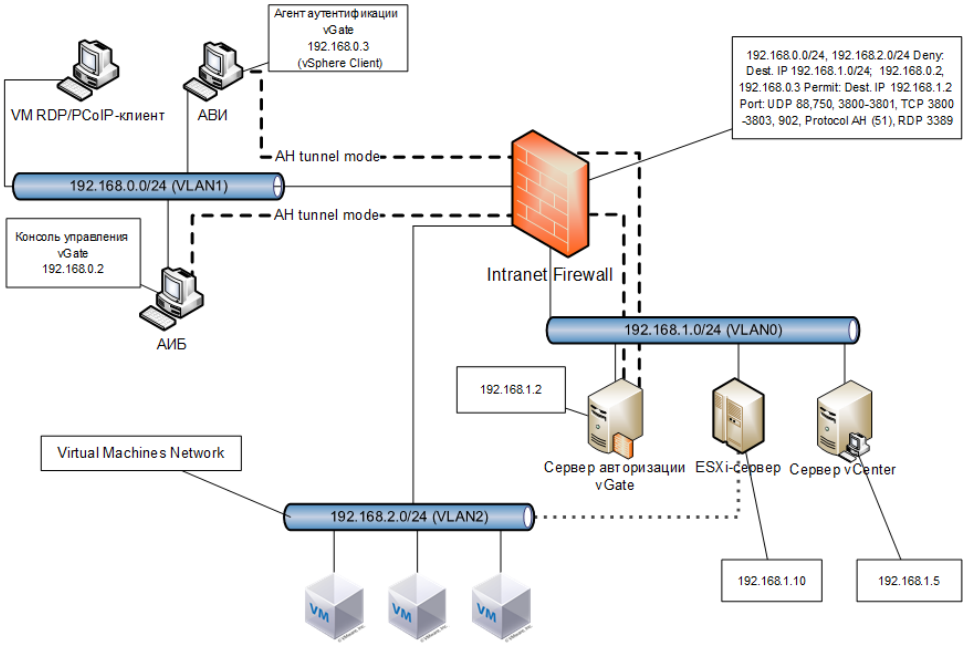
Настройки маршрутизатора

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 3806;
- порт TCP 3808 (при резервировании сервера авторизации vGate);
- порт TCP 3814;
- порт TCP 902;
- 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 Veritas Backup Exec 21.0

Для настройки совместной работы vGate 4.4 и системы восстановления данных Veritas Backup Exec 21.0 следуйте рекомендациям, указанным в документации к продукту Veritas Backup Exec 21.0 (см. разделы "Применение программы Backup Exec совместно с брандмауэрами" и "Порты Backup Exec").

Внимание!

- В процессе восстановления виртуальных машин из резервных копий в консоли управления могут появляться сообщения аудита о нарушении политик безопасности. Чтобы избежать появления данных сообщений, можно приостановить работу модуля защиты ESXi-серверов с помощью кнопки-ссылки "Приостановить агент" в разделе "Развертывание" консоли управления vGate.
- По окончании операции восстановления может потребоваться согласование контроля целостности виртуальных машин.

Совместная работа vGate и Антивируса Касперского

Настройка Kaspersky Endpoint Security 11

Для доступа к vCenter 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.

Настройка vGate для работы с Kaspersky Security для виртуальных сред

Для совместной работы vGate и решения "Kaspersky Security для виртуальных сред 5.0" необходимо произвести настройку vGate.

Если на сервере vCenter установлен компонент контроля сетевых подключений, то для компонентов "Kaspersky Security для виртуальных сред 5.0", расположенных внутри защищаемого периметра, необходимо создать правила для следующих подключений к vCenter:

- входящие соединения с сервера VMware vShield на TCP-порты 443 и 7444;
- входящие соединения с ВМ, на которой установлен компонент "Файловый Антивирус", на TCP-порт 443;
- входящие соединения с ВМ, на которой установлен компонент Kaspersky Security Center, на TCP-порты 139, 443 и 445.

Подробнее о настройке правил см. стр.**143**.

При обращении к защищаемым серверам из внешнего периметра сети администрирования через консоль администрирования Kaspersky Security Center необходимо добавить ПРД в разделе "Защищаемые серверы" консоли управления vGate:

- для сервера VMware vShield: протокол TCP, порт назначения 443;
- для сервера Kaspersky Security Center: протокол TCP, порты назначения 8060, 13000 и 14000;
- для ESXi-сервера: протокол TCP, порт назначения 443;
- для сервера vCenter: протокол TCP, порт назначения 443.

В качестве пользователя, для которого действуют правила, следует указать учетную запись АВИ, использующего консоль администрирования Kaspersky Security Center.

Подробнее о настройке ПРД см. стр.**137**.

Внимание! Не следует назначать политику безопасности "Доверенная загрузка виртуальных машин" на виртуальные машины, используемые в решении "Kaspersky Security для виртуальных сред 5.0":

- виртуальная машина VMware vShield;
- виртуальная машина защиты с установленным компонентом "Файловый Антивирус";
- виртуальная машина защиты с установленным компонентом "Обнаружение сетевых угроз".

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.

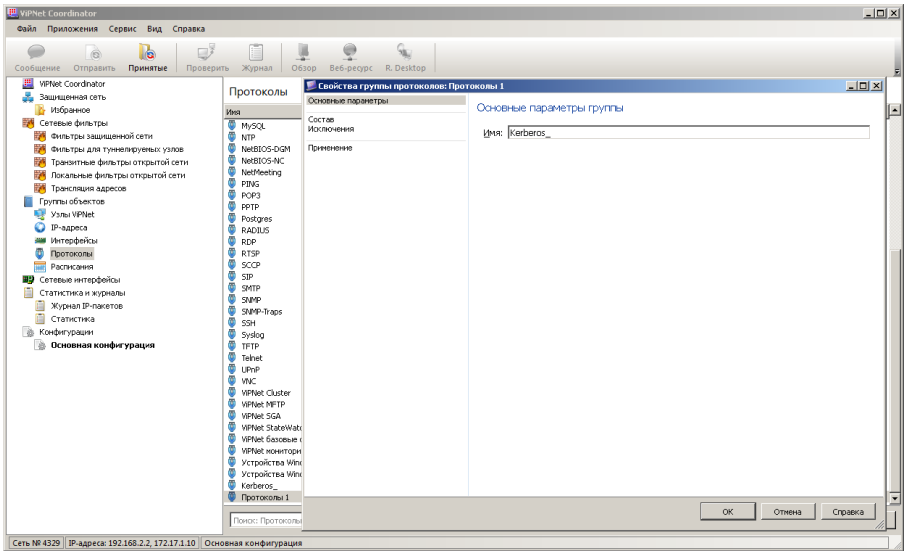
В примерах ниже рассматривается настройка ПО ViPNet следующих версий:

- Client 4.3 (4.53803);
- Coordinator 4.3 (2.37189).

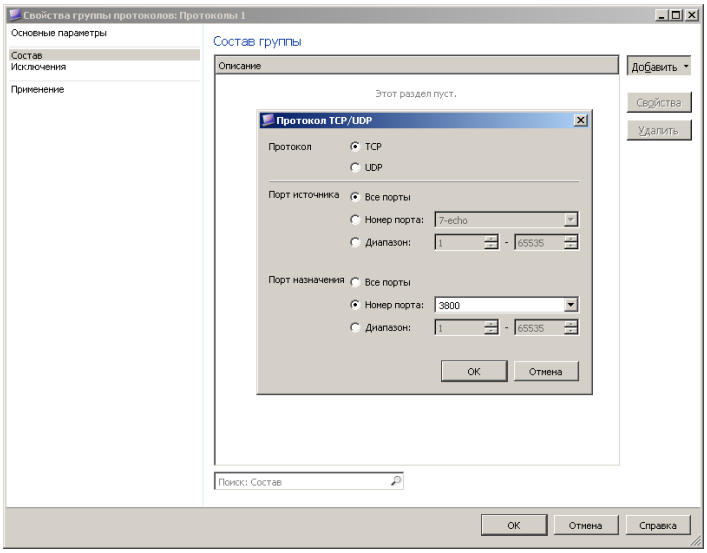
Вариант 1

Для настройки ViPNet:

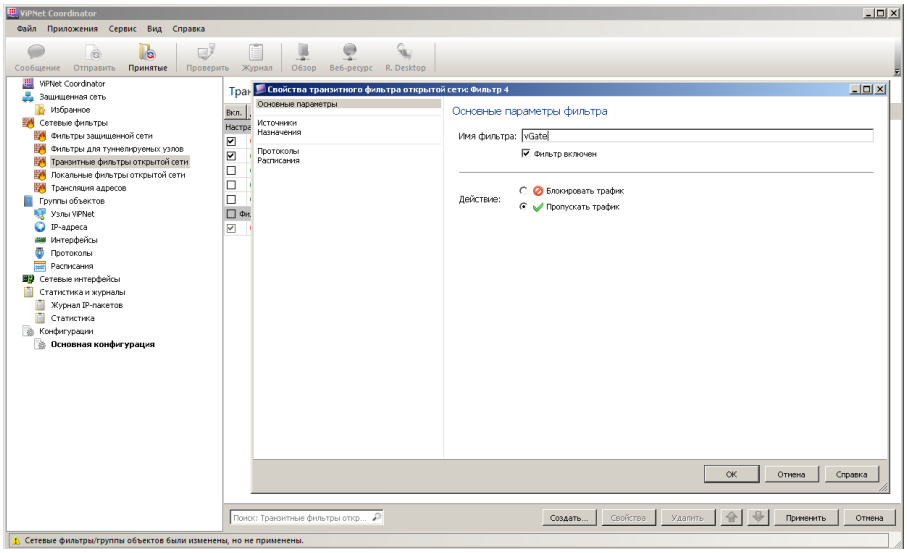
1. В меню ViPNet Coordinator выберите пункт "Группы объектов", затем "Протоколы" и создайте новую группу протоколов.



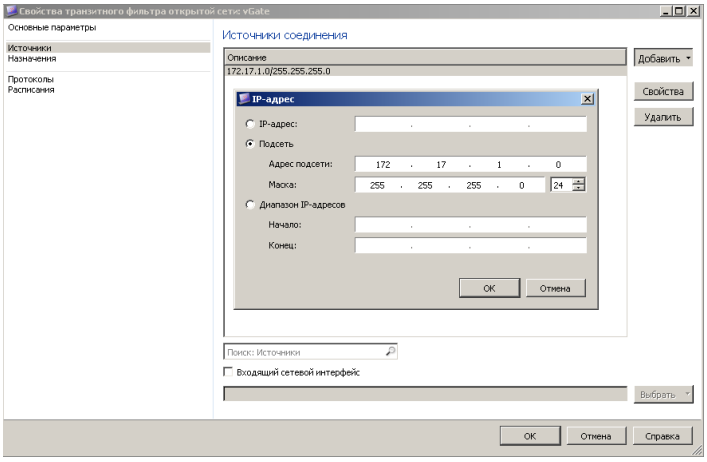
2. В окне добавления группы перейдите на вкладку "Состав", затем нажмите кнопку "Добавить" и добавьте следующие протоколы и порты Kerberos:
   - UDP 3800;
   - UDP 750;
   - UDP 88;
   - TCP 3800;
   - TCP 3801;
   - UDP 3801;
   - TCP 3808.



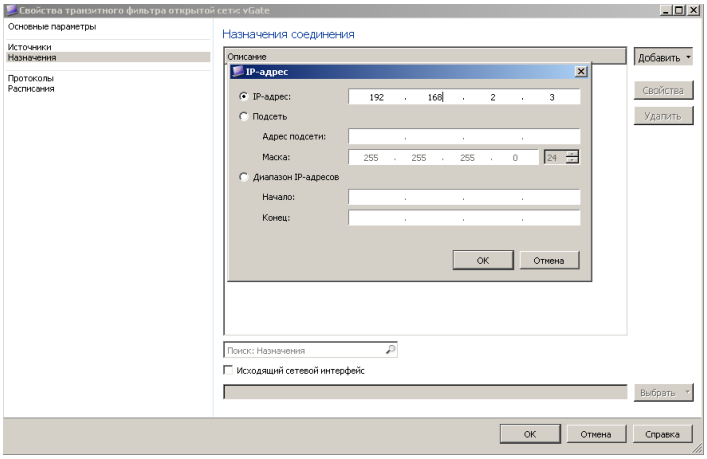
3. В меню ViPNet Coordinator выберите пункт "Сетевые фильтры", затем "Транзитные фильтры открытой сети" и создайте новый фильтр.



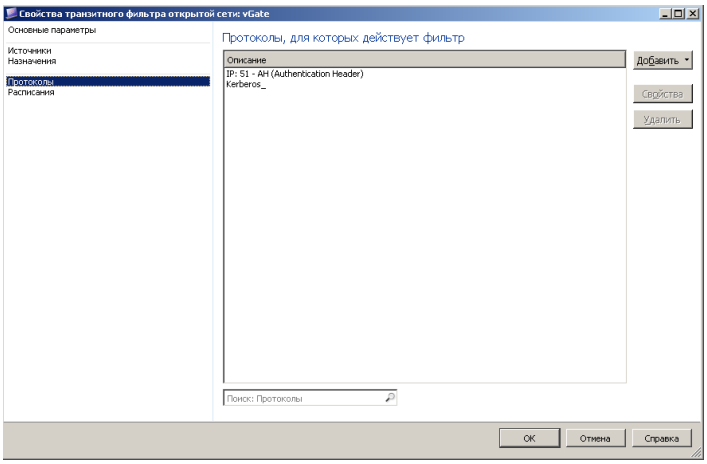
4. В окне создания фильтра перейдите на вкладку "Источники" и нажмите кнопку "Добавить", выберите "IP-адрес или группа адресов", а затем "Подсеть". Укажите адрес клиентской подсети.



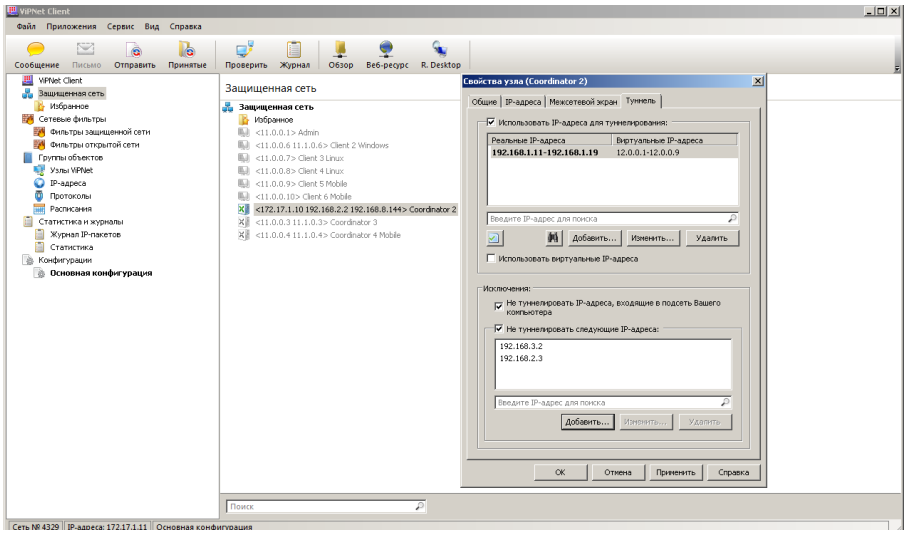
5. Перейдите на вкладку "Назначения" и нажмите кнопку "Добавить", выберите "IP-адрес или группа адресов", а затем "IP-адрес". Укажите внешний адрес сервера авторизации vGate.



6. Перейдите на вкладку "Протоколы" и нажмите кнопку "Добавить". Добавьте созданную в пп. 1, 2 группу протоколов Kerberos и IP-протокол AH, нажмите кнопку "OK".



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 TCP 5432;
- порт UDP 750;
- порт UDP 88;
- порт TCP 3802;
- порт TCP 3803.

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
80	TCP	Служба компонента защиты vGate на ESXi-сервере
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

Порт	Протокол	Назначение
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
20443	TCP	Служба vGate для контроля виртуальной инфраструктуры vSphere
30443	TCP	Служба vGate для контроля виртуальной инфраструктуры vSphere (vCSA)
40443	TCP	Порт для перенаправления Stunnel с PSC для vGate
5432	TCP	Порт для репликации PostgreSQL

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.

Документация

1.	Средство защиты информации vGate R2. Руководство администратора. Принципы функционирования	RU.88338853.501410.012 91 1-1
2.	Средство защиты информации vGate R2. Руководство администратора. Установка, настройка и эксплуатация	RU.88338853.501410.012 91 2-1
3.	Средство защиты информации vGate R2. Руководство администратора. Быстрый старт	RU.88338853.501410.012 91 3-1
4.	Средство защиты информации vGate R2. Руководство пользователя. Работа в защищенной среде	RU.88338853.501410.012 92 1