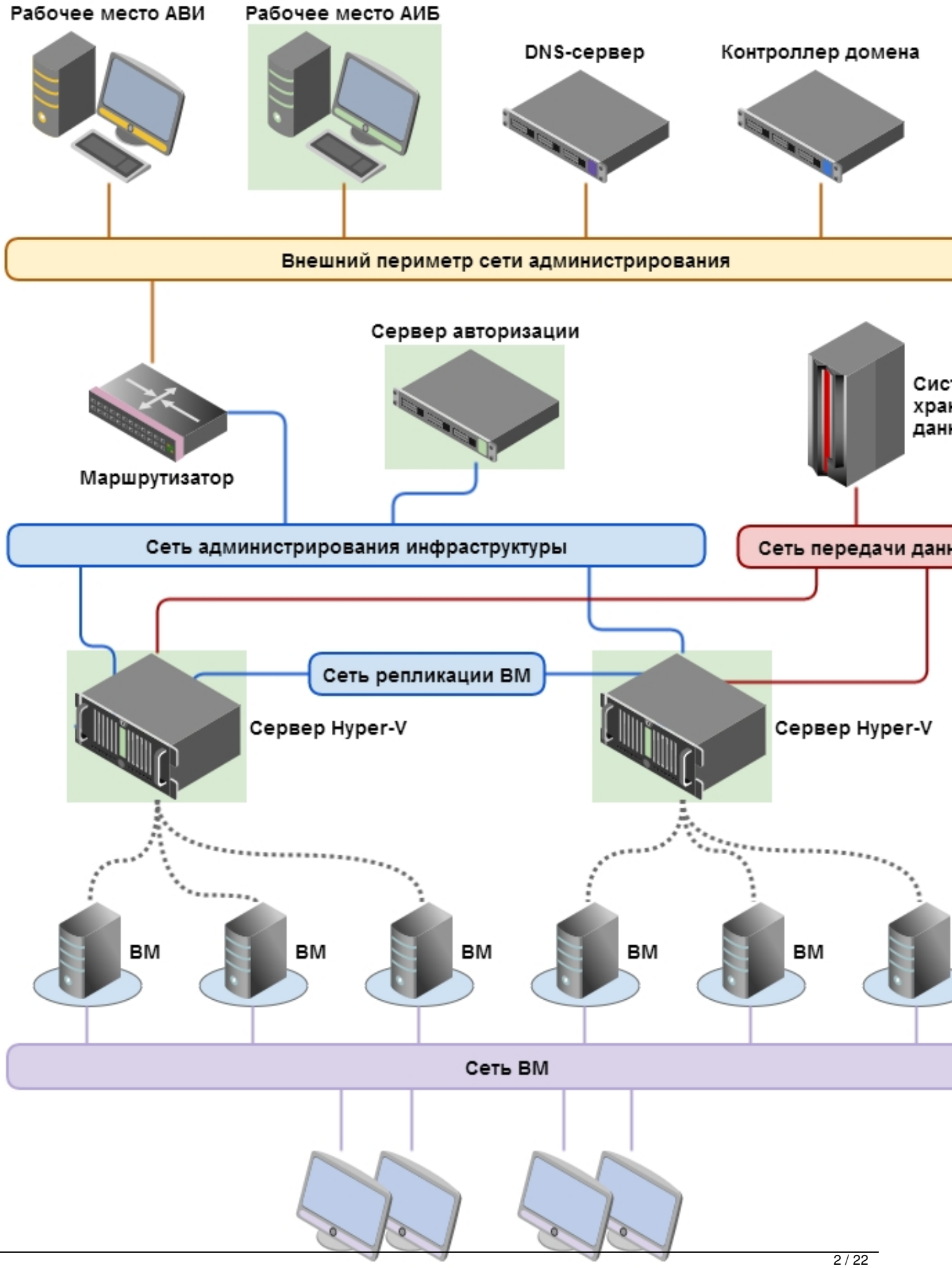
Эксплуатация решения vGate R2 for Hyper-V с точки зрения администратора

Автор: Александр Самойленко
Дата: 27/12/2014

В прошлых статьях мы рассказывали о продукте vGate R2 for Hyper-V , который позволяет проводить защищенную аутентификацию администраторов, разграничивать доступ к различным объектам инфраструктуры и проводить аудит событий безопасности. О возможностях этого продукта мы писали тут , о настройке - тут и тут , а сегодня мы поговорим о том, как выглядит повседневная эксплуатация решения со стороны администратора ИБ, который является также и администратором решения vGate.

Итак, приведем сначала референсную архитектуру vGate R2 для инфраструктуры Hyper-V, к которой можно обращаться по ходу чтения статьи:


Рабочее место АВИ
Рабочее место АИБ
DNS-сервер
Контроллер домена
Внешний периметр сети администрирования
Сервер авторизации
Маршрутизатор
Сеть администрирования инфраструктуры
Сеть репликации ВМ
Сервер Hyper-V
Сервер Hyper-V
ВМ
ВМ
ВМ
ВМ
ВМ
Сеть ВМ
Клиенты ВМ

Автор:
27.12.14 20:10 -

[redacted]

Аудит

Фильтрация событий

Типы событий
- [x] Успех
- [x] Уведомление
- [x] Предупреждение
- [x] Ошибка

Время событий: с первого 17/04/2014 5:10:44 PM
до последнего 17/04/2014 5:10:44 PM

Компьютер: *

Текст содержит: *

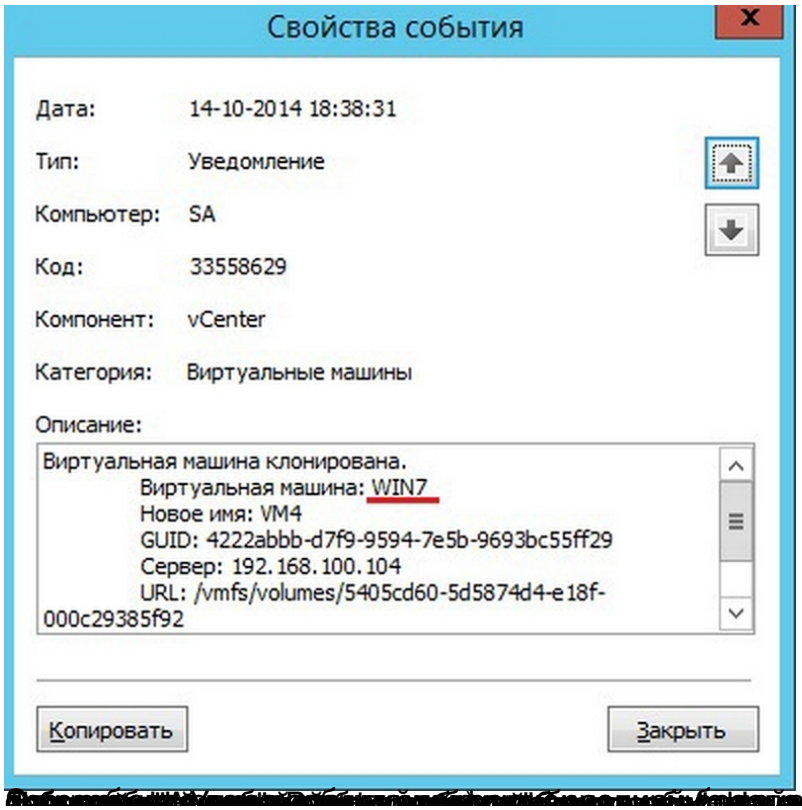
Дополнительно... Применить

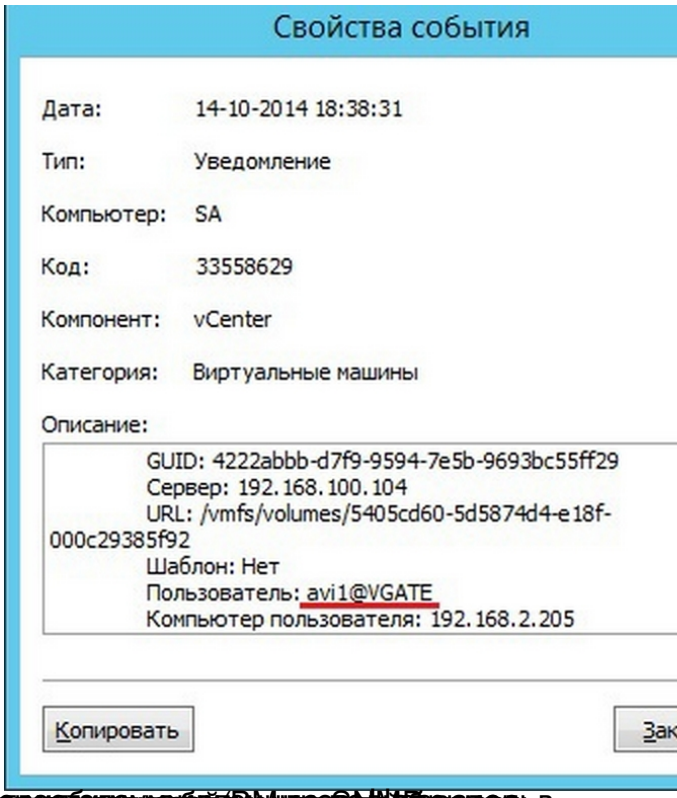
Список событий: Всего объектов: 2000

Тип	Время	Компьютер	Код события	Компонент	Категория
Предупреж...	17-04-2014 08:15:50	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:15:50	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:15:24	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:15:03	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:15:03	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:14:37	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:14:16	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:14:16	HVAUTHSERVER	16842763	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:13:50	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Предупреж...	17-04-2014 08:13:29	HVAUTHSERVER	67174413	Служба аутентификации	Управление д
Успех	17-04-2014 08:13:29	HVAUTHSERVER	16842763	Служба аутентификации	Управление д

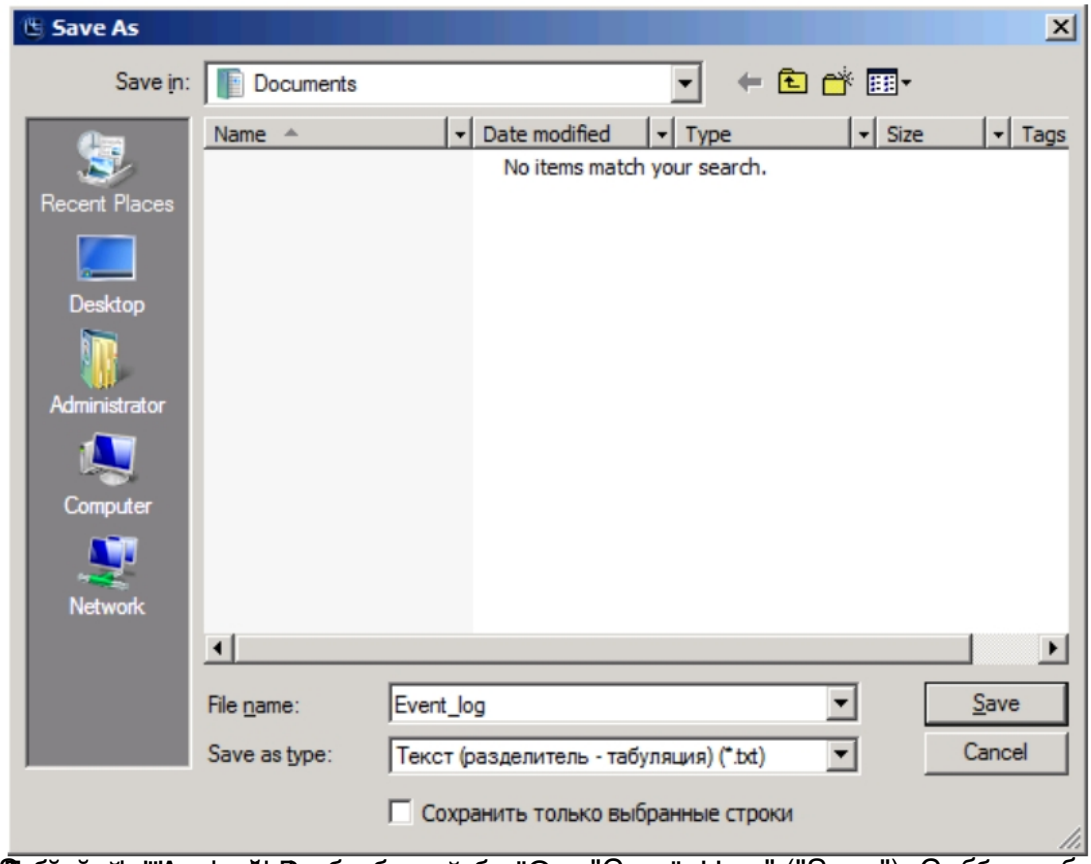
[redacted]

Автор:
27.12.14 20:10 -



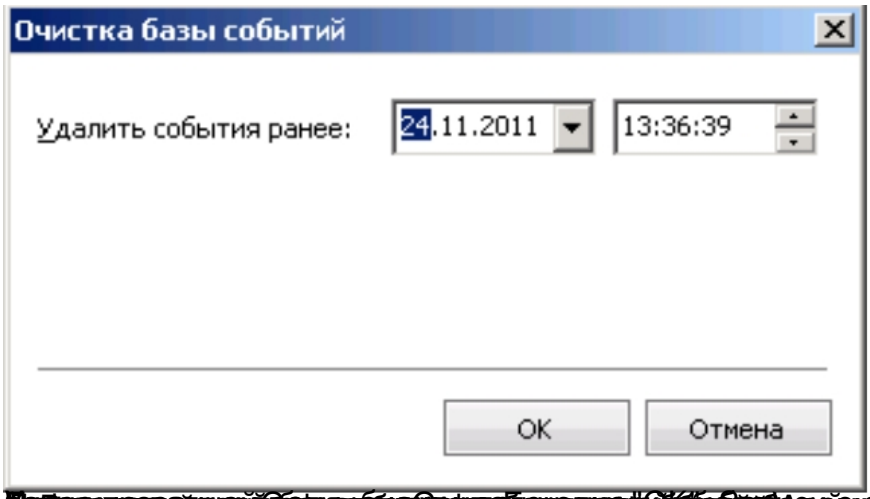


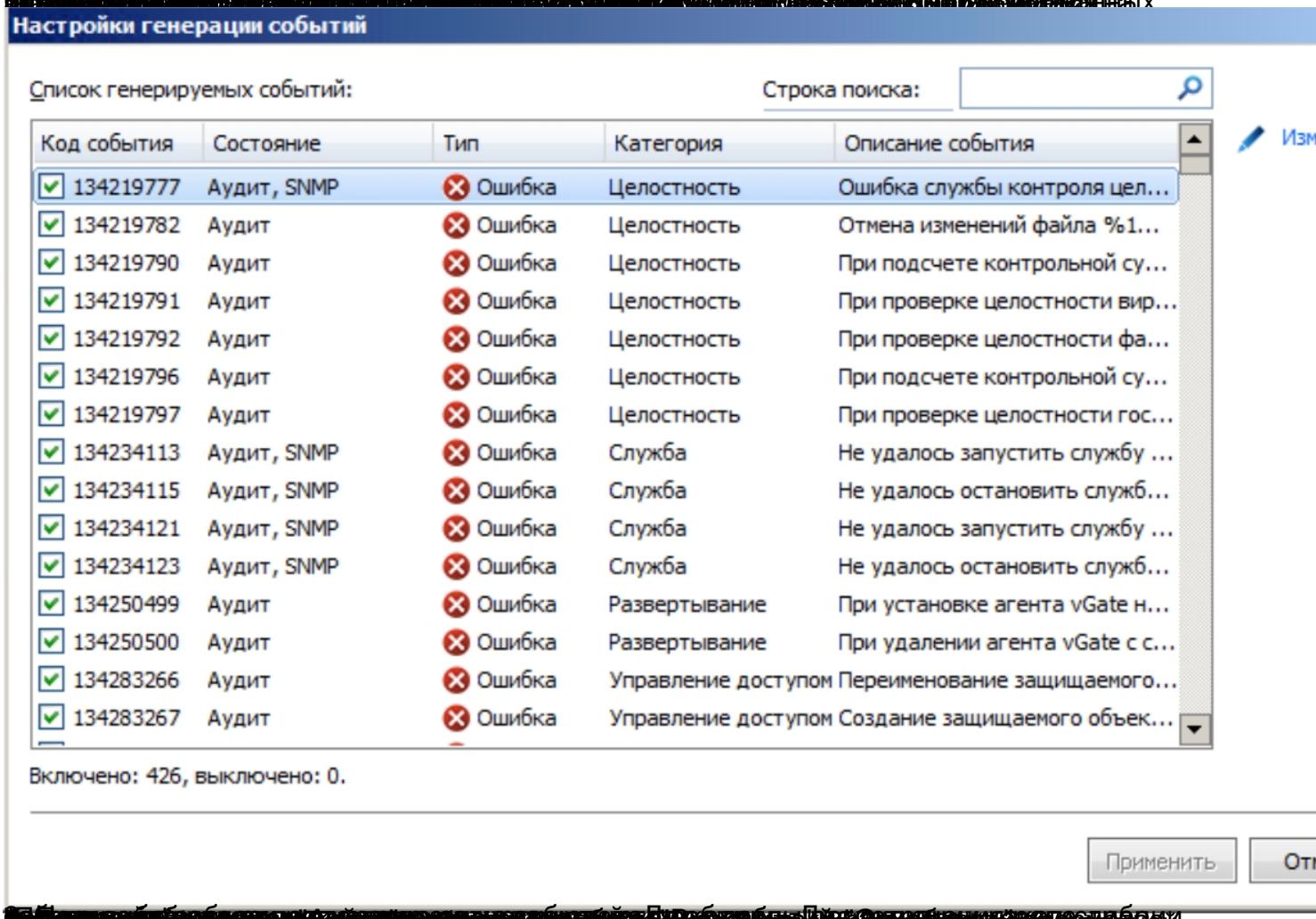
[illegible] в

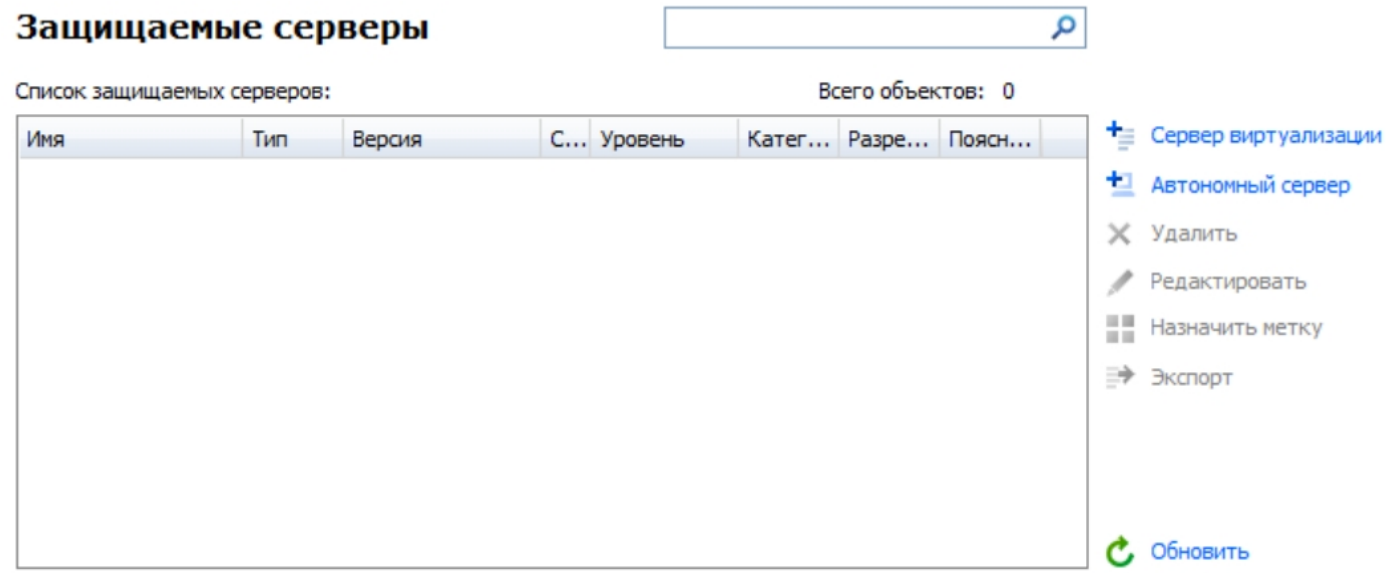


[illegible] ны в

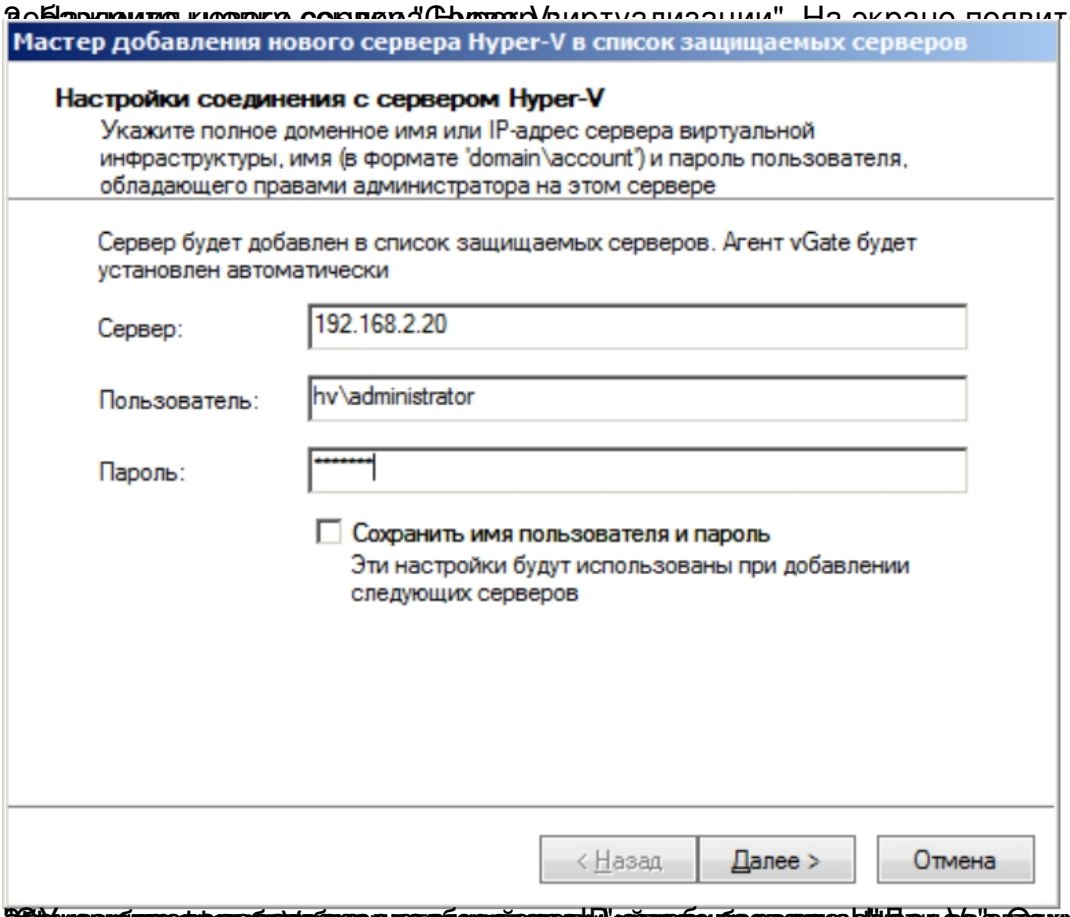
Автор:
27.12.14 20:10 -





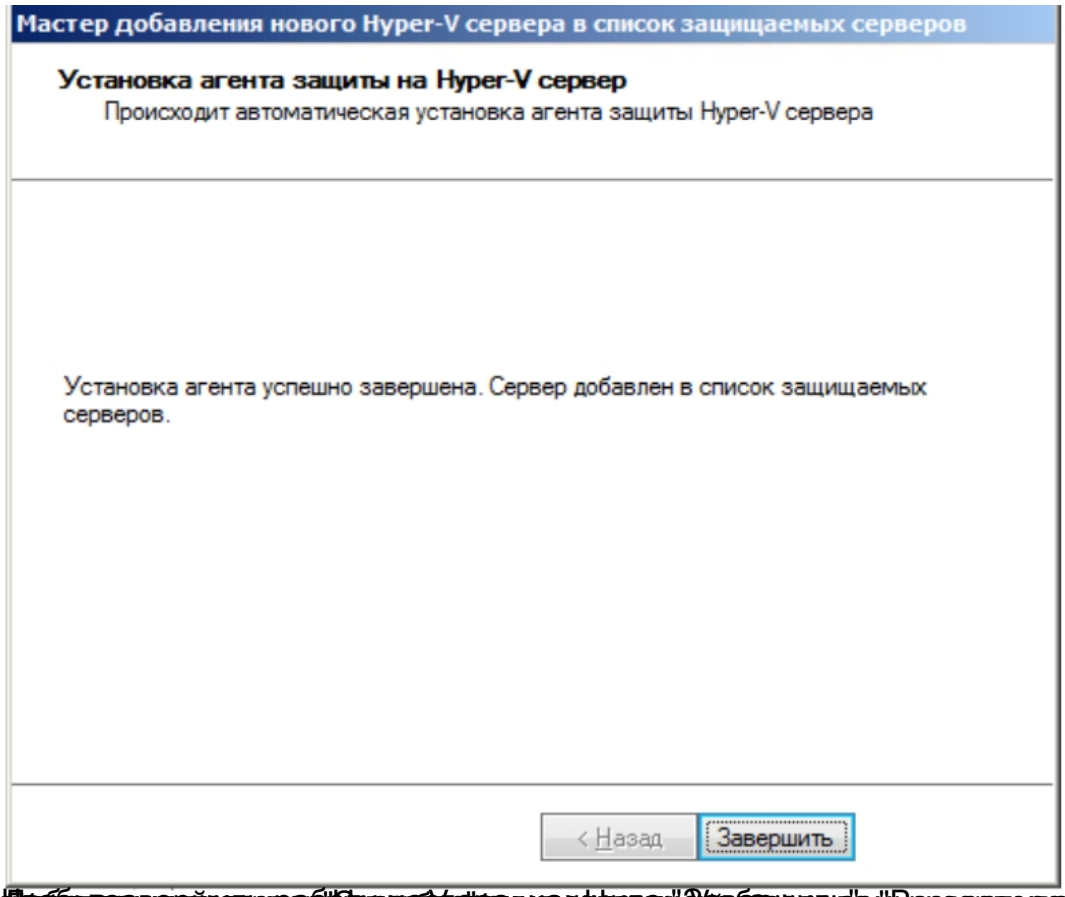


Добавим хостер сервер "Hyper-V виртуализации". На экране появится мастер

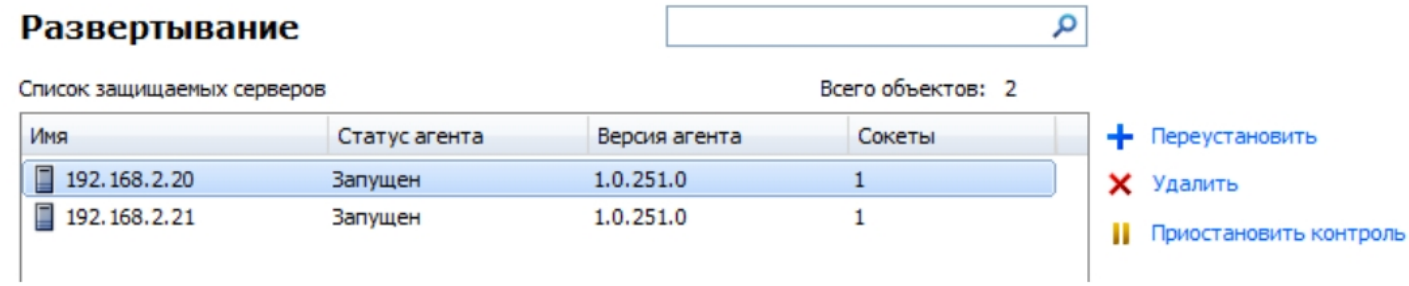


После добавления сервера в список защищаемых серверов будет доступно

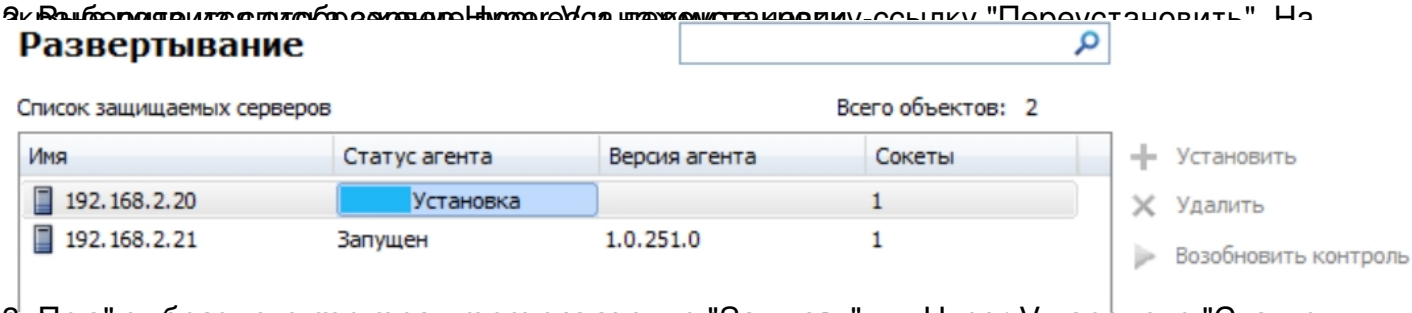
Автор:
27.12.14 20:10 -



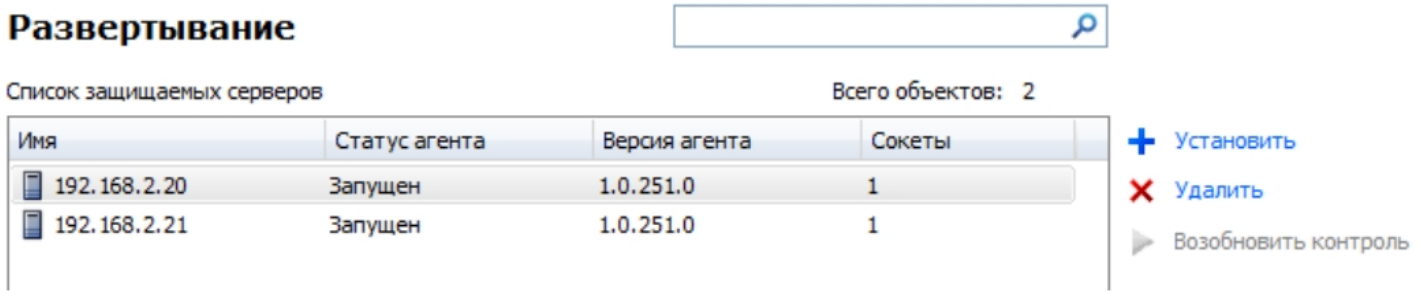
[redacted] и

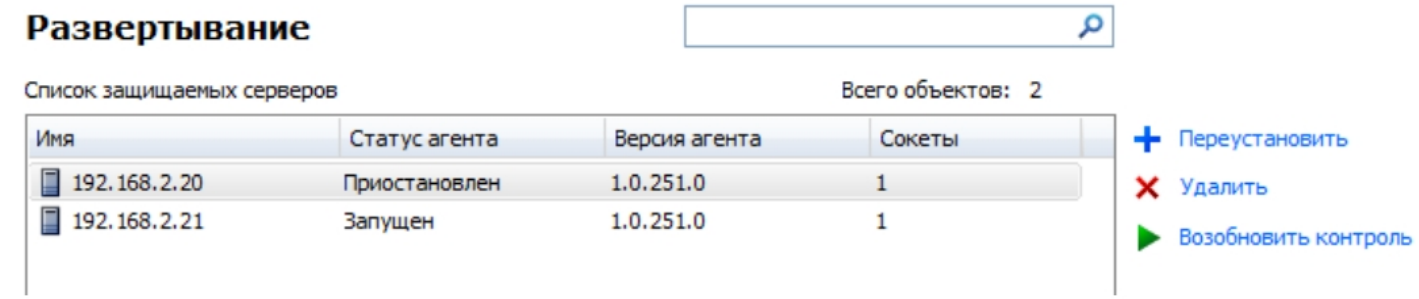


[redacted] ссылку "Переустановить". На



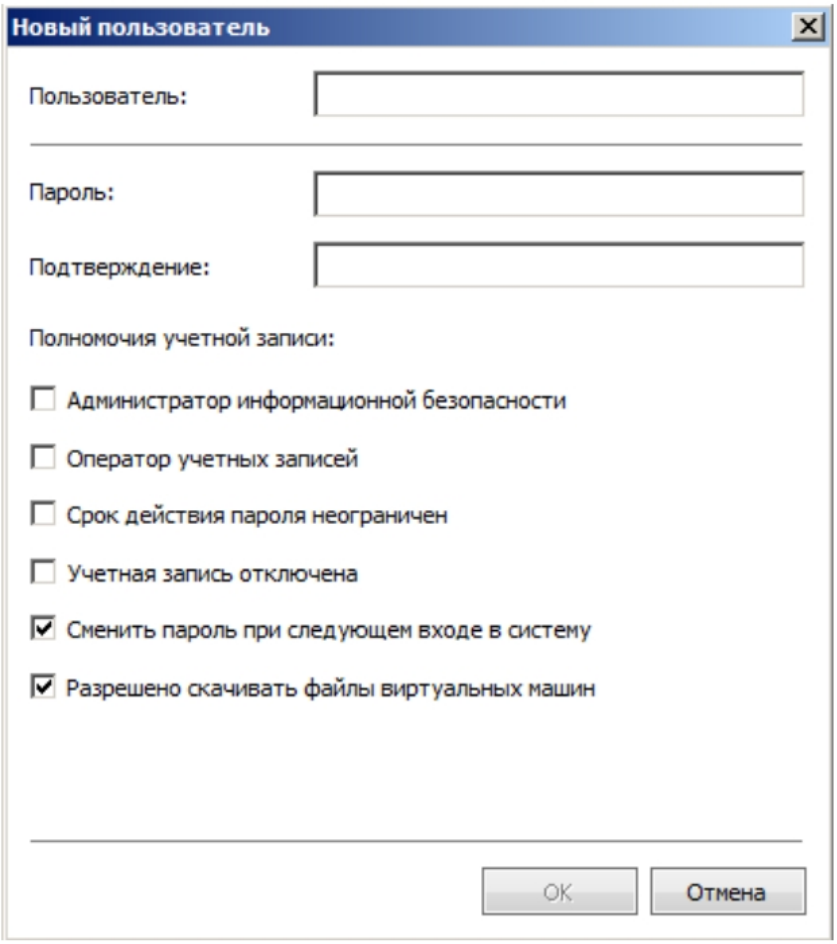
[redacted] агента защиты Hyper-V параметр "Статус


Развертывание
Список защищаемых серверов
Всего объектов: 2
Имя
Статус агента
Версия агента
Сокеты
192.168.2.20
Запущен
1.0.251.0
1
192.168.2.21
Запущен
1.0.251.0
1
Установить
Удалить
Возобновить контроль


Развертывание
Список защищаемых серверов
Всего объектов: 2
Имя
Статус агента
Версия агента
Сокеты
192.168.2.20
Приостановлен
1.0.251.0
1
192.168.2.21
Запущен
1.0.251.0
1
Переустановить
Удалить
Возобновить контроль

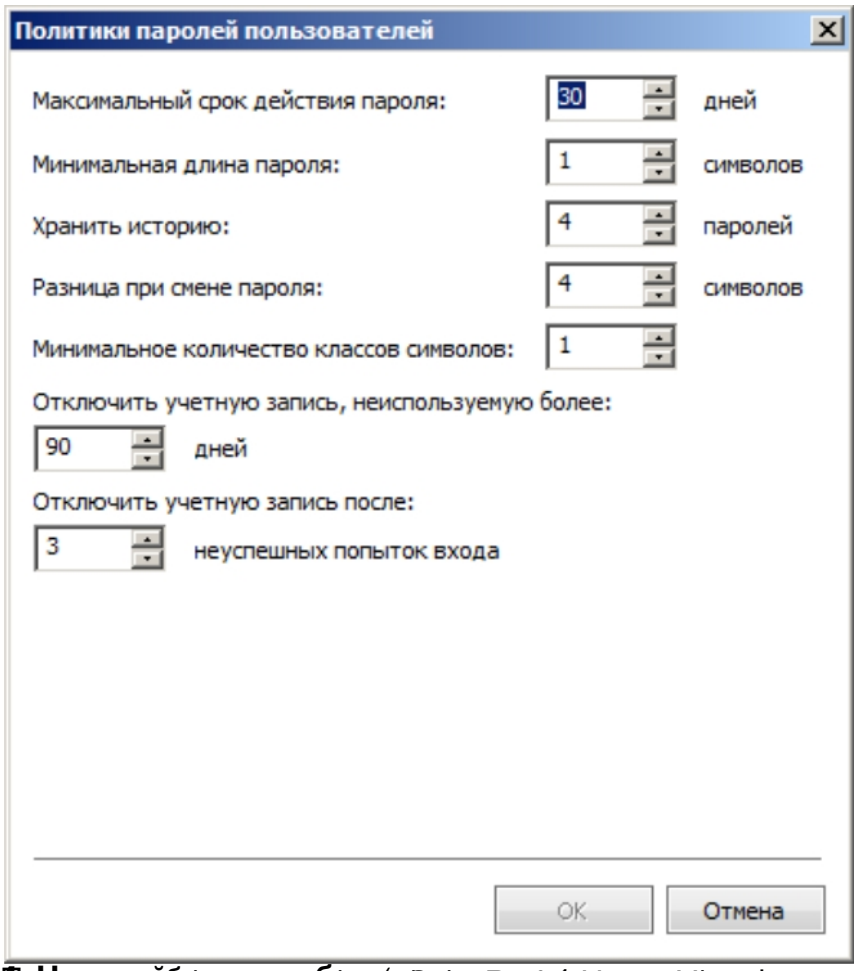
Учетные записи
Список пользователей:
Всего объектов: 3
Имя пользователя
Уровень
Категории
admin@VGATE
Неконфиденциально
u1@VGATE
Неконфиденциально
u2@VGATE
Неконфиденциально
Добавить
Создать
Удалить
Редактировать
Изменить пароль
Назначить метку
Экспорт
Политики паролей

Автор:
27.12.14 20:10 -



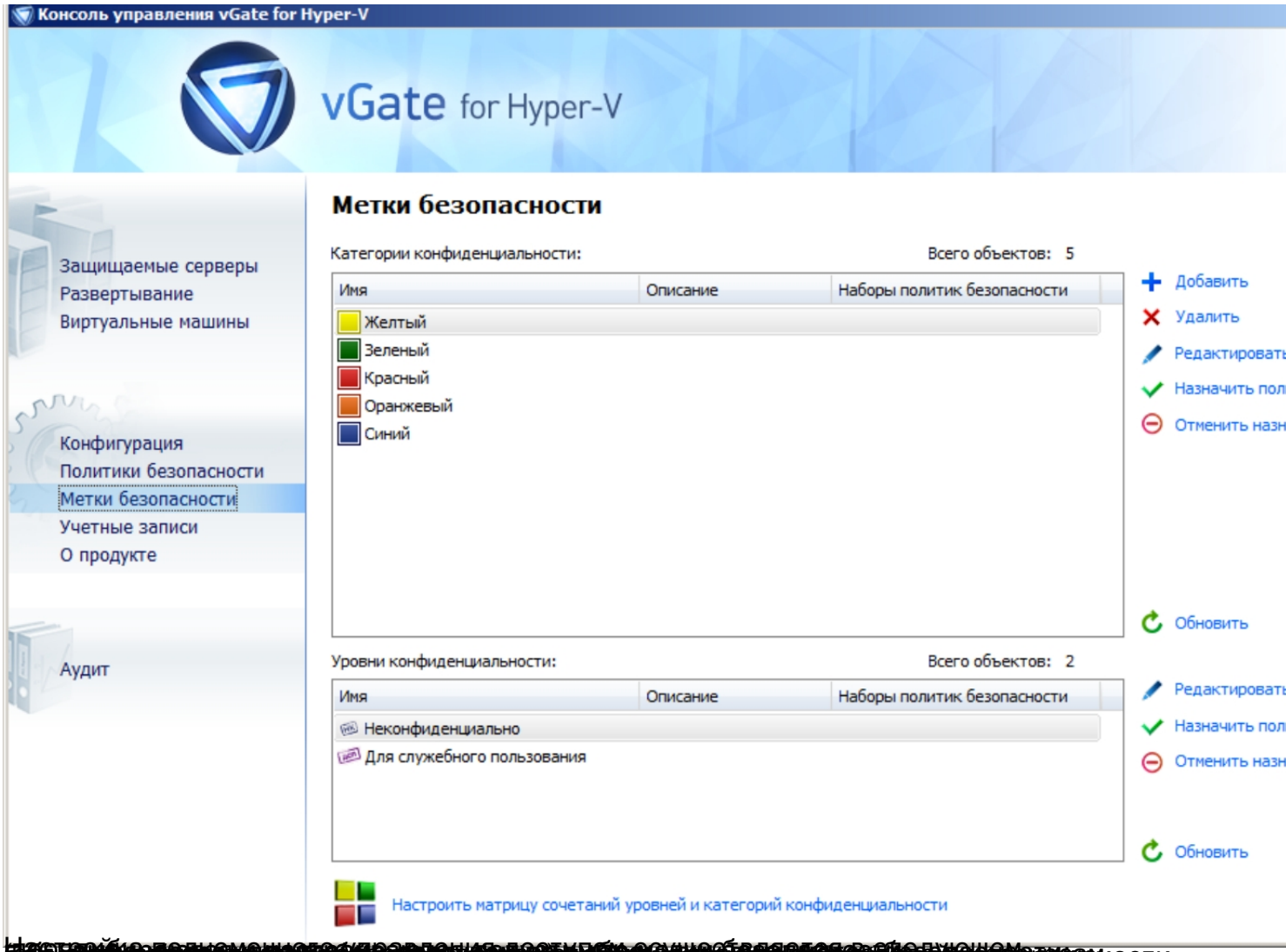
[redacted]

Автор:
27.12.14 20:10 -



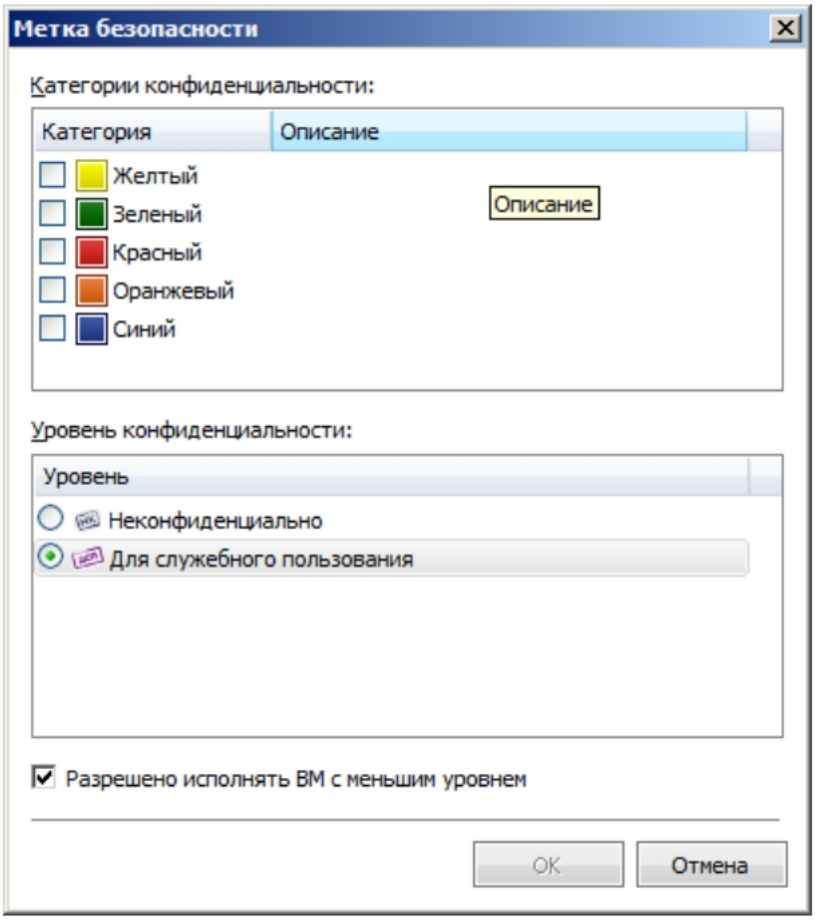
[illegible]

Автор:
27.12.14 20:10 -

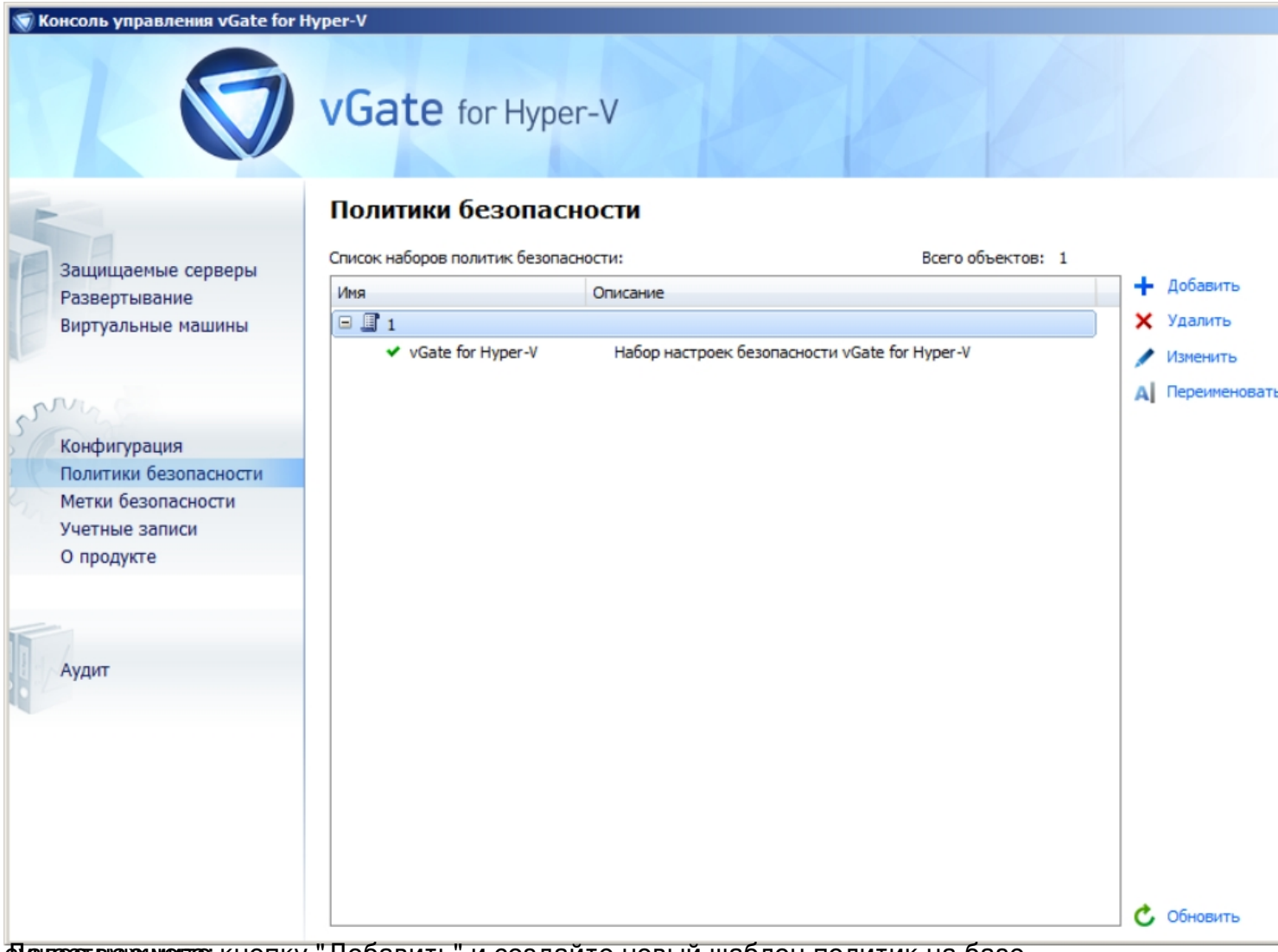


[redacted]

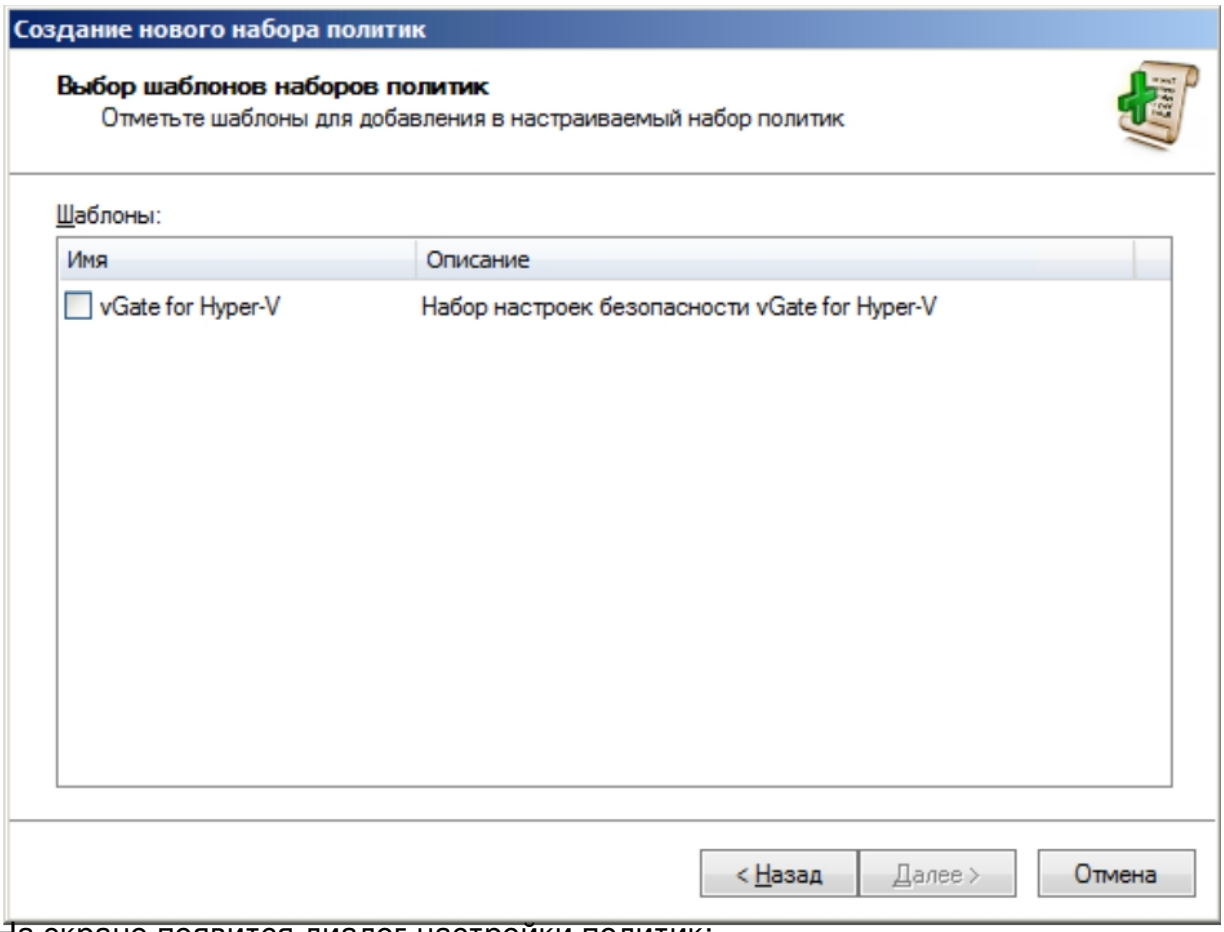
Автор:
27.12.14 20:10 -



[redacted]

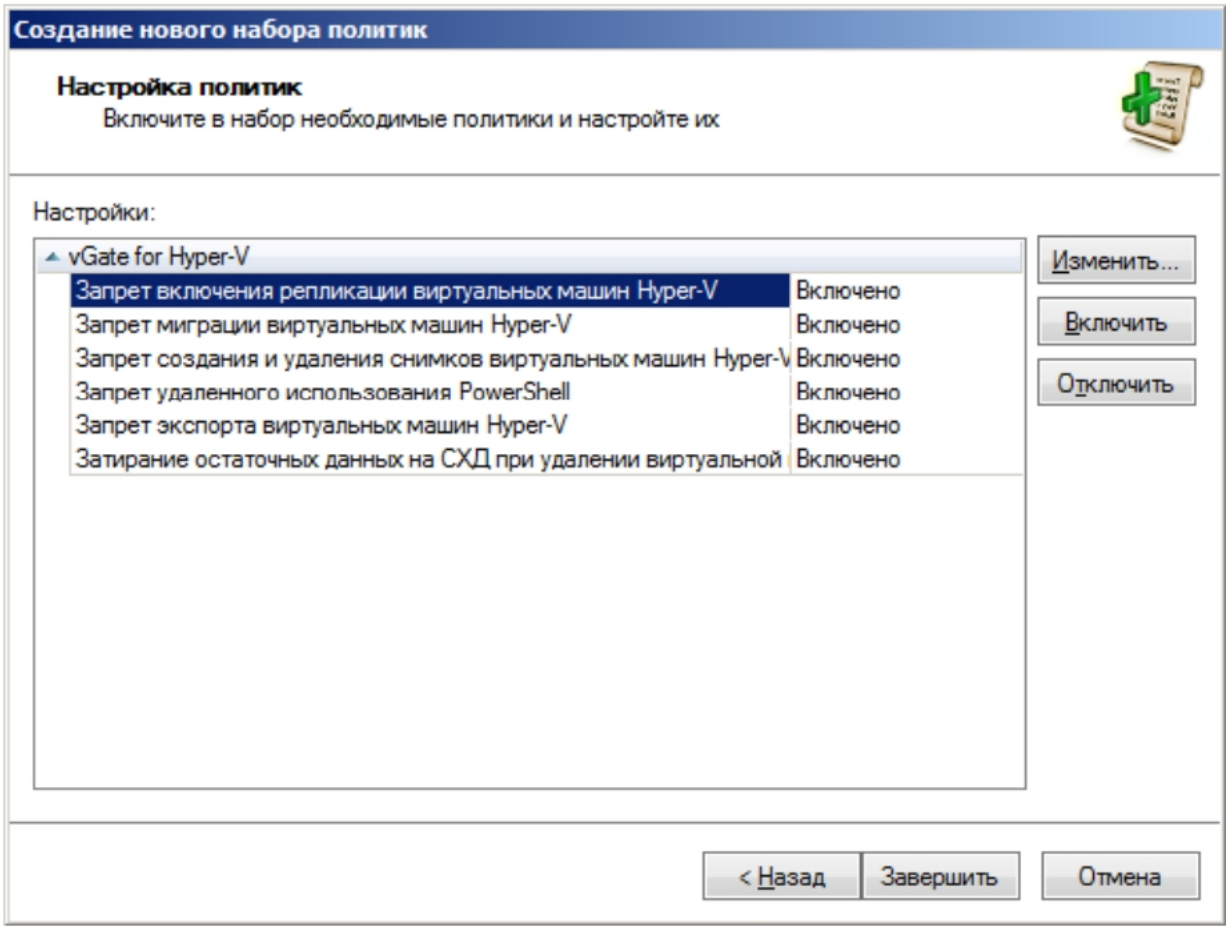


Далее нажмите кнопку "Добавить" и создайте новый шаблон политик на базе

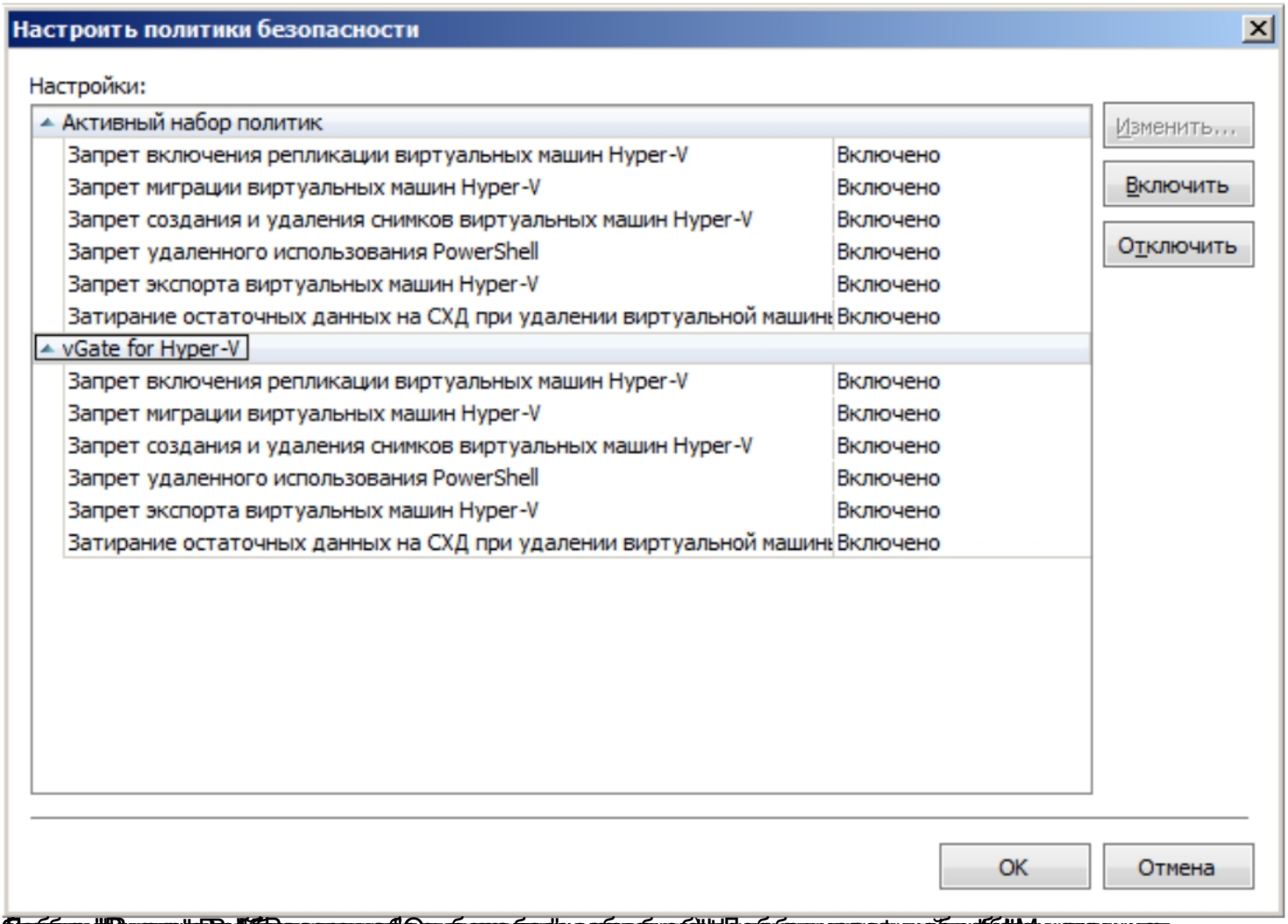


На экране появится диалог настройки политик:

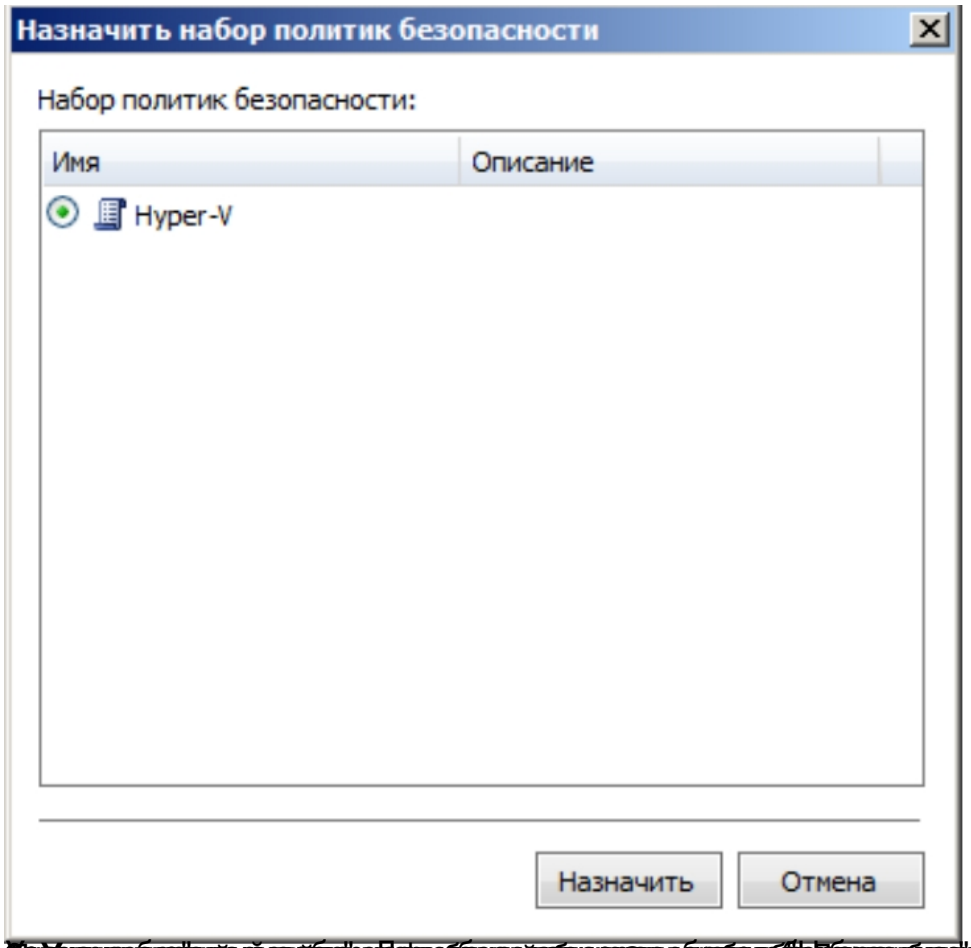
Автор:
27.12.14 20:10 -



[illegible]


Настроить политики безопасности
Настройки:
Активный набор политик
Запрет включения репликации виртуальных машин Hyper-V Включено
Запрет миграции виртуальных машин Hyper-V Включено
Запрет создания и удаления снимков виртуальных машин Hyper-V Включено
Запрет удаленного использования PowerShell Включено
Запрет экспорта виртуальных машин Hyper-V Включено
Затирание остаточных данных на СХД при удалении виртуальной машины Включено
vGate for Hyper-V
Запрет включения репликации виртуальных машин Hyper-V Включено
Запрет миграции виртуальных машин Hyper-V Включено
Запрет создания и удаления снимков виртуальных машин Hyper-V Включено
Запрет удаленного использования PowerShell Включено
Запрет экспорта виртуальных машин Hyper-V Включено
Затирание остаточных данных на СХД при удалении виртуальной машины Включено
Изменить...
Включить
Отключить
OK
Отмена

Автор:
27.12.14 20:10 -



Защищаемые серверы

Список защищаемых серверов: Всего объектов: 3

Имя	Тип	Версия	С...	Уровень	Катег...	Разре...	Поясн...
192.168.2.10	Автоно...						Сервер...
192.168.2.20	Сервер...	Windows Server 2...	1	Неконф...		Да	hvVmS...
192.168.2.21	Сервер...	Windows Server 2...	1	Неконф...		Да	hvVmS...

Сервер виртуа
Автономный се
Удалить
Редактировать
Назначить мет
Экспорт
Обновить

Правила доступа для 192.168.2.10: Всего правил: 5

Описание	Состо...	Пользоват...	Компьютер...	Прото...	Исход...	Порт н...
Доступ к вспомогатель...	Вкл	admin@VGATE	*	TCP	Любой	3908
Доступ к отчетам для ...	Вкл	admin@VGATE	*	TCP	Любой	5432
Доступ к службе управ...	Вкл	admin@VGATE	*	TCP	Любой	3802
Доступ к службе управ...	Вкл	admin@VGATE	*	TCP	Любой	3906
Статус операций по уп...	Вкл	admin@VGATE	*	TCP	Любой	3803

Создать прави
Удалить
Свойства
Выключить
Экспорт
Обновить

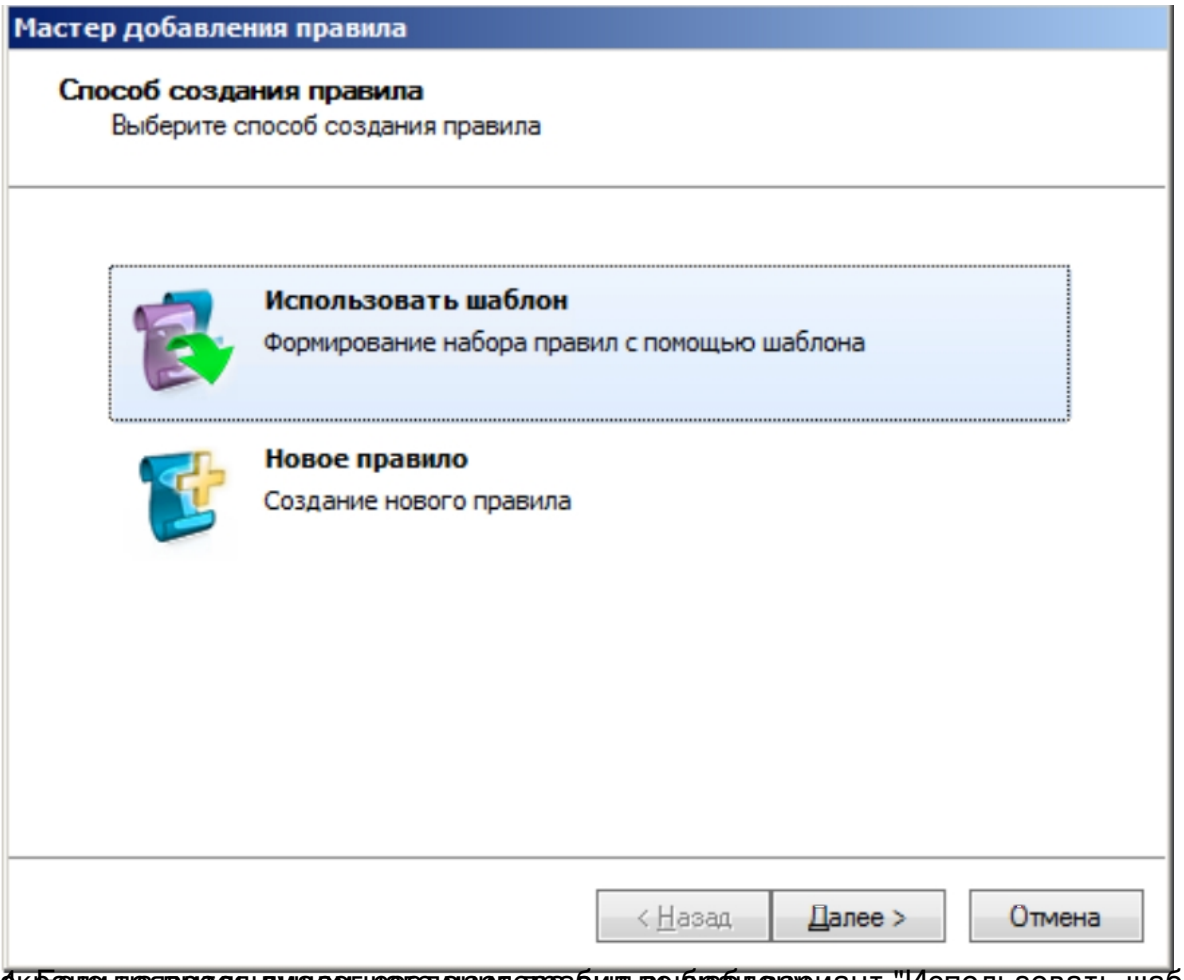
2. Выберите требуемый сервер и перейдите на вкладку "Список защищаемых серверов". В нижней

Правила доступа для 192.168.2.20: Всего правил: 3

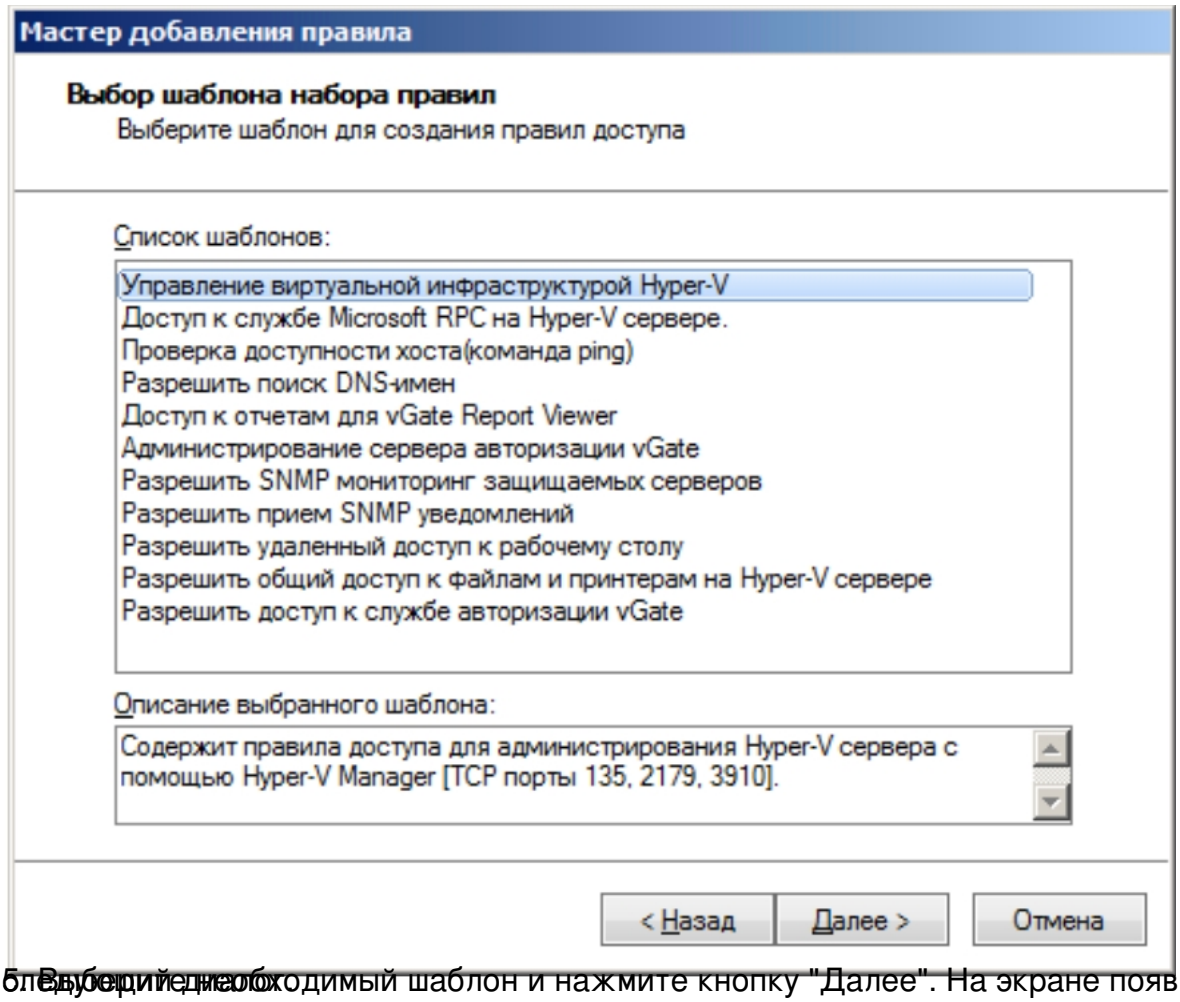
Описание	Состо...	Пользоват...	Компьютер...	Прото...	Исход...	Порт н...
Доступ к консоли вирт...	Вкл	avi@VGATE	*	TCP	Любой	2179
Доступ к службе RPC	Вкл	avi@VGATE	*	TCP	Любой	135
Доступ к службе WMI	Вкл	avi@VGATE	*	TCP	Любой	3910

Создать
Удалить
Свойств
Выключ
Экспорт

3. Для создания нового правила нажмите на кнопку-ссылку "Создать правило". На экране появится диалог создания нового правила.

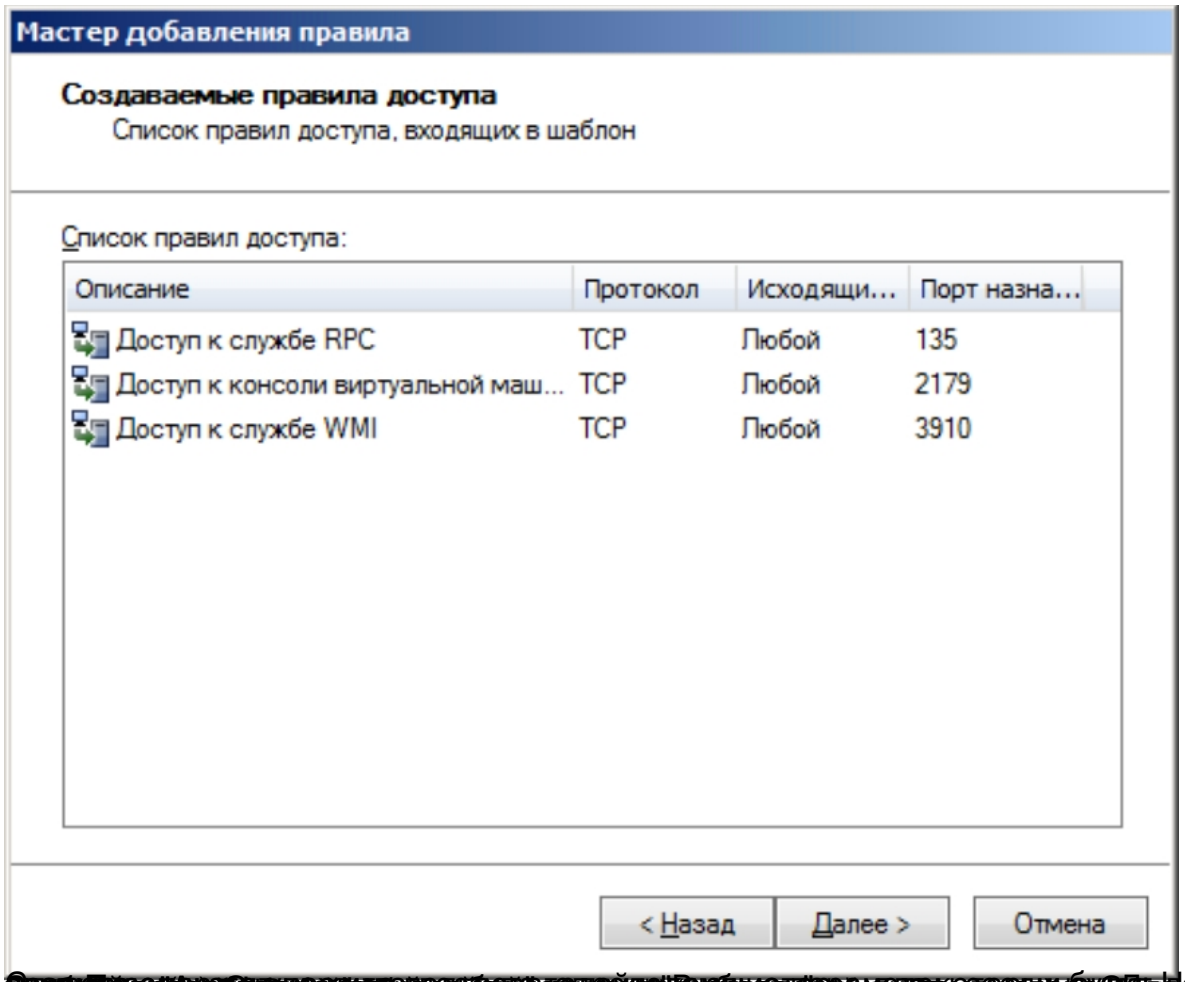


4. Далее на первом экране мастера выбираем вариант "Использовать шаблон", на экране появится диалог создания правил по шаблону.

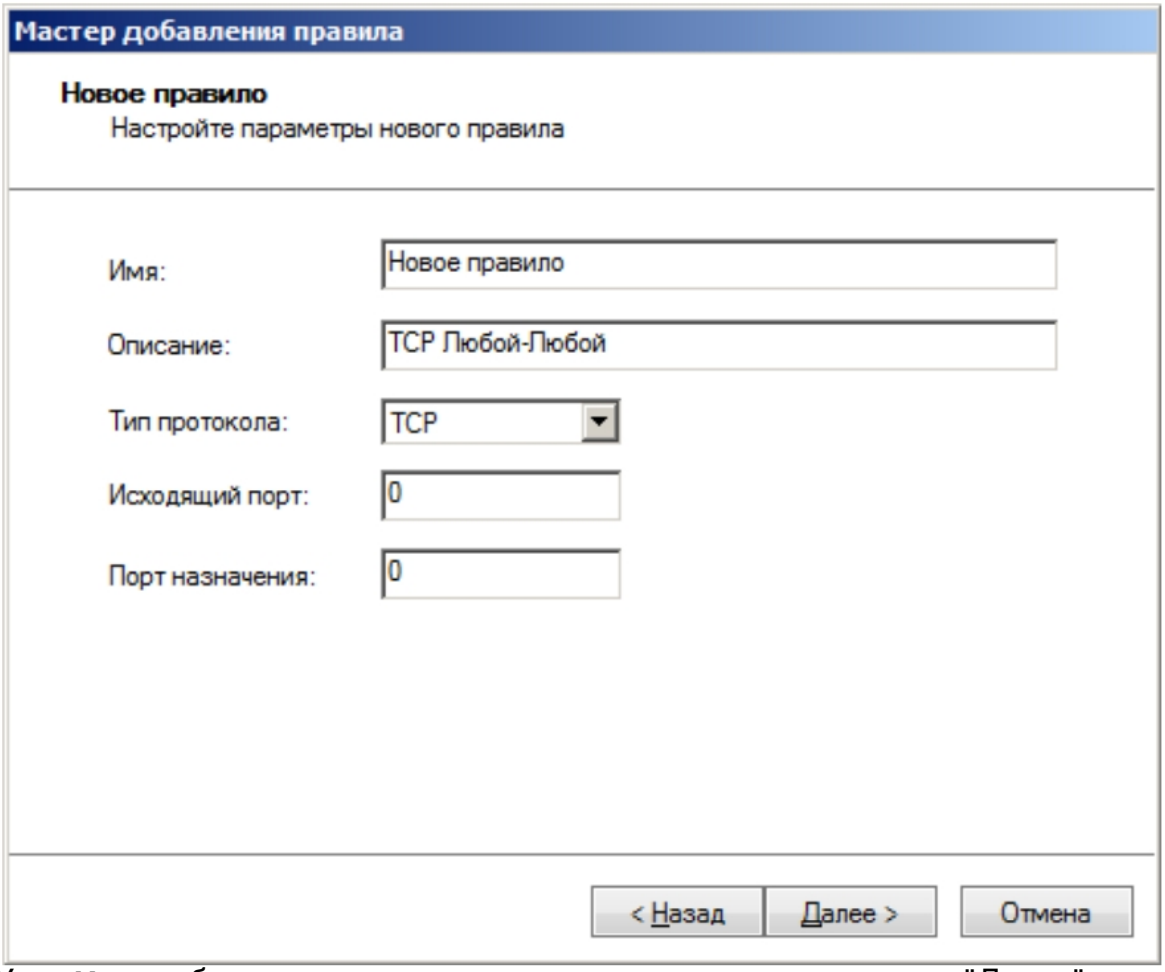


Выберите необходимый шаблон и нажмите кнопку "Далее". На экране появится следующий диалоговый блок

Автор:
27.12.14 20:10 -



Автор:
27.12.14 20:10 -



Укажите необходимые значения параметров и нажмите кнопку "Далее".