

Лабораторный практикум

УСТАНОВКА И НАСТРОЙКА СЕРВЕРНЫХ КОМПОНЕНТОВ
FALCONGAZE SECURETOWER

в сети на базе рабочей группы компьютеров

Цель практического занятия: Научиться устанавливать компоненты программного комплекса на локальный компьютер, устанавливать агента на компьютер рабочей группы, настраивать перехват данных при помощи агента, настраивать работу ключевых сервисов **Falcongaze SecureTower**.

Оборудование: ПК, включенные в рабочую группу компьютеров.

Содержание практикума

Общие сведения.....	3
Порядок выполнения работы.....	6
1. Установка компонентов программного комплекса SecureTower.....	6
2. Запуск Консоли системного администратора SecureTower Admin Console.....	7
3. Настройки хранения информации.....	8
4. Установка агентов на рабочие станции.....	11
5. Конфигурация профиля работы агентов.....	15
6. Контроль работы агентов.....	19
7. Работа с базой пользователей.....	20
8. Настройка индексации рабочих станций.....	21
9. Удаление агента (для ознакомления)*.....	25
Контрольные вопросы.....	26

Рекомендации по выполнению работы

Изучите теоретическую часть лабораторного практикума, изложенную в разделе **Общие сведения**, перед выполнением практических заданий.

Выполнять задания лабораторного практикума следует строго в соответствии пунктами, как указано в разделе **Порядок выполнения работы**. Шаги и задания, помеченные «*», выполняются по указанию преподавателя.

После каждого шага или при возникновении вопросов о выполнении задания сравните результат на экране с соответствующим рисунком. Для быстрого получения помощи в работе с программой, а также получения дополнительной информации нажмите клавишу F1 либо обратитесь к преподавателю.

Чтобы проверить, насколько хорошо Вы усвоили материал, ответьте на контрольные вопросы в конце работы.

Общие сведения

Установка

Установка программного комплекса сопровождается Мастером установки. При работе Мастера установки программа предложит выбрать компоненты, которые необходимо установить на компьютер. По завершении установки компонентов продукта в меню Пуск (главное меню операционной системы Windows) и на рабочем столе появятся ярлыки для запуска двух консолей: Консоль администратора и Консоль пользователя.

В рамках данного практикума выполняется установка и настройка демо-версии программного комплекса.

Интерфейс пользователя

Консоль администратора используется для централизованной настройки работы всех компонентов системы. Консоль пользователя используется для работы с перехваченными данными (включая создание правил безопасности, просмотр активности пользователей, поиск в архиве перехваченных данных). При запуске Консоли администратора или Консоли пользователя пользователю системы будет предложено выбрать сервер для подключения. Если консоль запускается на том же компьютере, где установлены серверные компоненты системы, необходимо подключиться к локальному компьютеру (localhost).

Перехват

Система **SecureTower** может перехватывать трафик данных двумя способами: централизованно (через порт зеркалирования сетевого коммутатора), либо агентами, устанавливаемыми на рабочие станции.

Централизованный перехват имеет ряд недостатков, связанных с его организацией. Так для обеспечения централизованного перехвата требуется провести дополнительные работы по настройке механизма зеркалирования трафика и настройке работы сетевого адаптера. Помимо технических сложностей централизованно может перехватываться только трафик, передаваемый по нешифрованным протоколам. Однако, в случаях, если техническое обеспечение и квалификация сотрудников позволяют использовать централизованный перехват, он может быть использован в комбинации с перехватом агентами.

Агенты, установленные на рабочих станциях позволяют перехватывать весь трафик – как нешифрованный, так и зашифрованный (по протоколам, использующим SSL-шифрование: HTTPS, FTPS, SMTPS, POP3S, IMAP4S, SIP, протоколы мессенджеров Skype, Telegram, Viber, WhatsApp, ICQ10, Google Hangouts и Microsoft Lync). Также агенты перехватывают данные, передаваемые, на внешние устройства (USB накопители, съемные жесткие диски, карты памяти и т.д.), в облачные хранилища и локальные сетевые ресурсы, локальные и сетевые принтеры, содержимое буфера обмена, реализуют функцию кейлогера, осуществляют аудит подключения внешних устройств, аудит файловых систем компьютеров. Помимо функции перехвата агенты выполняют дополнительные функции по контролю активности сотрудников – предоставляют доступ к просмотру видео с рабочего стола и веб-камер и прослушиванию звуковых потоков с рабочей станции, снимают скриншоты с заданной периодичностью, собирают статистику по используемым приложениям и т.д. Важной функциональной особенностью агента является возможность блокирования данных, отправленных на внешние накопители, облачные хранилища и локальные сетевые ресурсы по набору параметров и расширениям файлов, а также данных, переданных по протоколам SMTP(S), HTTP(S) и MAPI.

Для использования возможности перехвата через агентов необходимо, чтобы они были установлены на все контролируемые рабочие станции. Существует три способа установки агентов:

- централизованно на выборочные компьютеры либо на все доступные компьютеры в сети (с Сервера контроля агентов SecureTower через Консоль администратора);
- через групповые политики домена;
- вручную с помощью отдельного инсталлятора, запущенного на рабочей станции, подлежащей контролю.

Стратегии установки выбираются в зависимости от количества компьютеров, которые требуется контролировать.

При установке агентов на определенные компьютеры, необходимо указать имена компьютеров либо выбрать соответствующие имена из структуры Active Directory. При включении данной опции Сервер контроля агентов будет осуществлять проверку наличия и состояния агентов только на **указанных** станциях и будет в автоматическом режиме производить установку агентов на соответствующий компьютер в случае отсутствия, сбоя или принудительного отключения агентов пользователем конечной станции.

Установка агентов на всех доступных компьютерах производится, если необходимо наличие агентов на всех или на большинстве рабочих станций сети. При включении данной опции, Сервер контроля агентов будет осуществлять установку агентов на первые, обнаруженные в сети компьютеры, число которых соответствует числу приобретенных лицензий на продукт. Установка, проверка наличия и состояния агентов осуществляется на **всех** обнаруженных в сети станциях, кроме указанных в списке исключений. В случае сбоя или принудительного отключения агентов пользователем какой-либо конечной станции либо обнаружения **новой** рабочей станции в сети сервер будет производить автоматическую установку агентов на соответствующей станции (при условии наличия свободных лицензий).

В рамках данного практикума выполняется процедура настройки перехвата агентом, установленным централизованно через Консоль администратора на компьютер, указанный преподавателем.

Хранение перехваченных данных

Информация, извлеченная из трафика сервисом перехвата (в случае использования централизованного перехвата данных) либо перехваченная агентами, сохраняется в базы данных, подключенные к системе. На текущий момент программа поддерживает работу с СУБД MS SQL Server, MySQL, Oracle и PostgreSQL. В комплект поставки программы также входит встраиваемая библиотека баз данных SQLite, предназначенная для работы с программой в тестовом режиме или для использования в небольшой сети при невысоких сетевых нагрузках. База данных SQLite создается в рабочей папке при установке системы и подключается к серверной части автоматически. Все данные перехвата будут сохраняться Центральным сервером в предустановленную базу данных без дополнительных настроек и вне зависимости от источника их поступления (серверного компонента, который осуществлял перехват). Для изменения настроек сохранения необходимо выполнить соответствующую конфигурацию Центрального сервера, отвечающего за сохранение данных: задать правила сохранения, добавить подключение к новой базе, настроить ротацию баз данных.

Правила сохранения позволяют описать условия, в соответствии с которыми Центральный сервер будет либо записывать перехваченные данные в указанное хранилище либо пропускать поступивший пакет.

Ротация баз данных применяется для группы баз данных и направлена на снижение размера отдельной базы и ускорение обработки поисковых запросов. Ротация представляет собой смену активной базы данных на следующую в списке сервера на основании выполнения заданных условий.

Содержимое баз данных индексируется Сервером индексирования для дальнейшей процедуры поиска по ним. Обновление индексов происходит автоматически.

Настройки перехвата

Система **SecureTower** позволяет задавать индивидуальные профили настроек работы агентов как для отдельных учетных записей пользователей, компьютеров и групп Windows Active Directory (включая домены, контейнеры и организационные единицы), так и для отдельных компьютеров, находящихся вне доменной группы Active Directory. В зависимости от выбранной стратегии установки агентов на рабочие станции, для всех компьютеров и пользователей в сети применяется Профиль по умолчанию, параметры которого могут быть изменены в соответствии с текущими рабочими задачами и восстановлены в случае необходимости. Для того чтобы применить индивидуальные настройки агента для перехвата данных отдельных компьютеров или пользователей сети, необходимо создать и сконфигурировать новый профиль настроек для выбранных объектов.

Настройка индексации рабочих станций

Индексация рабочих станций производится системой для контроля изменений файловых систем контролируемых компьютеров и обнаружение определенных файлов в индексируемых системах.

Контроль файловых систем основан на сопоставлении контрольных сумм (далее – хэши) заданных файлов с файлами, хранящимися на контролируемом компьютере. Сформировать банк хэшей документов, которые система будет автоматически отслеживать на индексируемых компьютерах, вы можете в настройках Центрального сервера на вкладке Банки хэшей Консоли администратора. Также вы можете настроить применение определенных банков для отдельных объектов контроля в профиле настроек агента.

Идентификация пользователей

Для отождествления перехваченной информации с конкретными пользователями сети программой используется система карточек пользователей. Каждому пользователю локальной сети назначена идентификационная карточка, содержащая персональную и контактную информацию пользователя (имя и фамилия, должность, адреса электронной почты, UIN для ICQ, учетные записи в коммуникационных программах, пользовательские имена в социальных сетях и т.д.). Кроме того, карточки пользователей отображают информацию о принадлежности пользователя к той или иной группе.

База пользователей формируется автоматически системой либо наполняется администратором при помощи Консоли администратора. Если сеть построена на базе Active Directory, то база пользователей создается и обновляется системой в автоматическом режиме. Система **SecureTower** позволяет произвести импорт всех пользователей из Active Directory, включая тех, чьи компьютеры не контролируются, для идентификации всех взаимосвязей контролируемых пользователей с другими сотрудниками организации. Если компьютеры сети организованы в рабочую группу, то база пользователей должна быть наполнена администратором системы вручную через Консоль администратора либо Консоль пользователя.

Группы пользователей также создаются при помощи Консоли администратора, и для каждой из них назначаются определенные пользовательские права. Группы могут создаваться по аналогии с организационной структурой предприятия и представлять собой различные его структурные подразделения. В программе существуют встроенные пользовательские группы: «Администраторы» и «Пользователи».

Карточки пользователей, присутствующие в базе на момент настройки, являются частью демоверсии системы.

Порядок выполнения работы

1. Установка компонентов программного комплекса SecureTower

Алгоритм действий

1.1 Откройте папку с комплектом поставки программного комплекса SecureTower, расположенную на рабочем столе вашего компьютера, и запустите исполняемый файл Мастера установки **FalcongazeSecureTowerNfrSetupRu.exe** и выберите язык установки в открывшемся диалоговом окне.

1.2 Ознакомьтесь с версией программного комплекса и рекомендациями по установке. Нажмите **Далее** для начала установки.

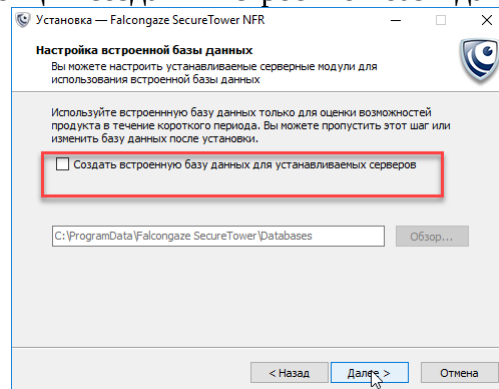


1.3 Отметьте *Я принимаю условия соглашения* и нажмите **Далее**.

1.4 Нажмите **Далее** для установки компонентов системы в папку, выбранную по умолчанию.

1.5 Нажмите **Далее** для полной установки компонентов системы.

1.6 Отмените выбор опции создания встроенной базы данных SQLite.



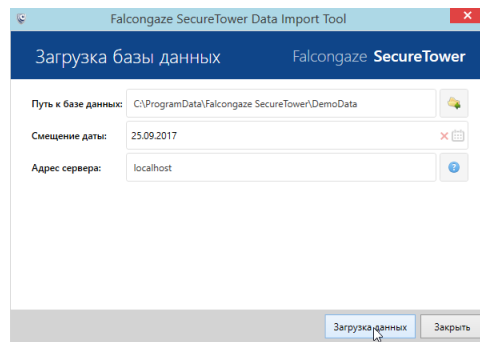
1.7 Нажмите **Далее** для размещения ярлыков в папке меню Пуск (главное меню операционной системы Windows).

1.7 Нажмите **Далее** для установки ярлыков системы на рабочий стол и обеспечения доступа к системе для всех пользователей ПК.

1.8 Нажмите **Установить**.

1.9 Дождитесь завершения установки и отмените выбор опций **Запустить Falcongaze SecureTower Client Console** и **Запустить Falcongaze SecureTower Admin Console**. Убедитесь, что отмечена опция **Запустить утилиту импорта демо-данных** и нажмите **Завершить** для завершения процесса.

1.10 В окне **Загрузка базы данных** убедитесь, что в поле **Адрес сервера** указано имя компьютера, на который производилась установка системы (localhost для локального компьютера) и нажмите **Загрузка данных**.



1.11 Не дожидаясь окончания загрузки данных на сервер, перейдите к п.2.

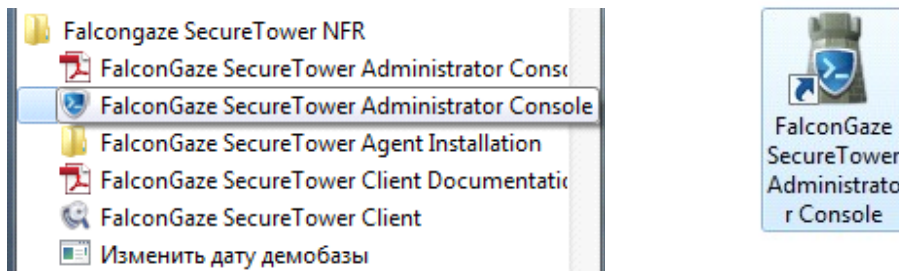
1.12 По окончании загрузки нажмите **ОК** в диалоговом окне.

Результат: папка **Falcongaze SecureTower NFR** добавлена в меню Пуск, ярлыки **Falcongaze SecureTower Client Console** и **Falcongaze SecureTower Admin Console** добавлены на рабочий стол.

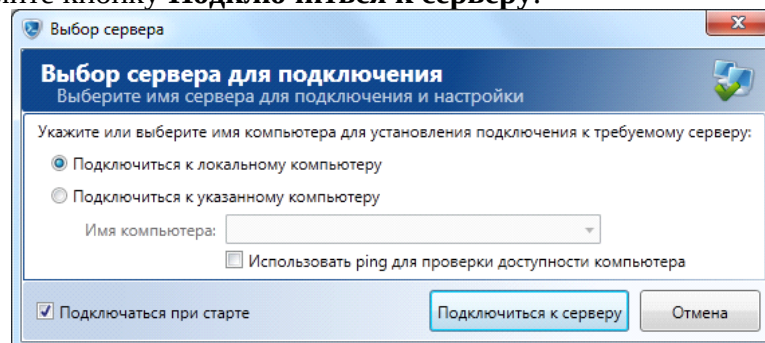
2. Запуск Консоли системного администратора SecureTower Admin Console

Алгоритм действий

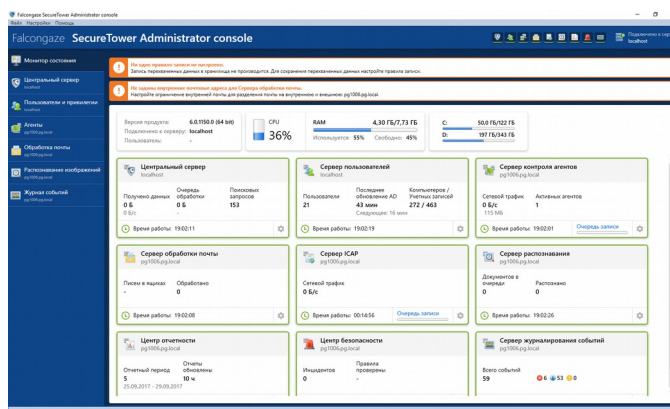
2.1 Запустите Консоль Администратора, используя ярлык консоли, размещенный в папке *Falcongaze SecureTower NFR* в меню *Пуск* либо используйте ярлык консоли на рабочем столе компьютера.



2.2 В открывшемся диалоговом окне выберите **Подключиться к локальному компьютеру** и нажмите кнопку **Подключиться к серверу**.



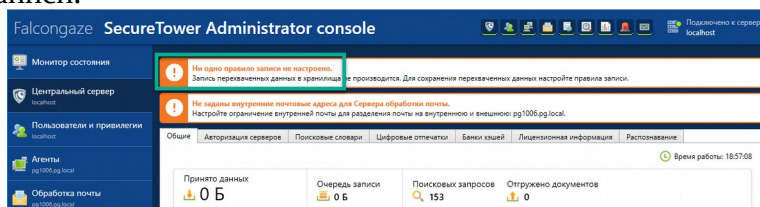
Результат: Все сервера системы установлены и работают без ошибок (зеленая рамка панели сервера).



3. Настройки хранения информации.

Получите у преподавателя реквизиты доступа к СУБД PostgreSQL.

В верхней части окна консоли отображаются два уведомления. Пройгнорируйте уведомление о настройке почтовых адресов и обратите внимание на уведомление об отсутствии правил записи.

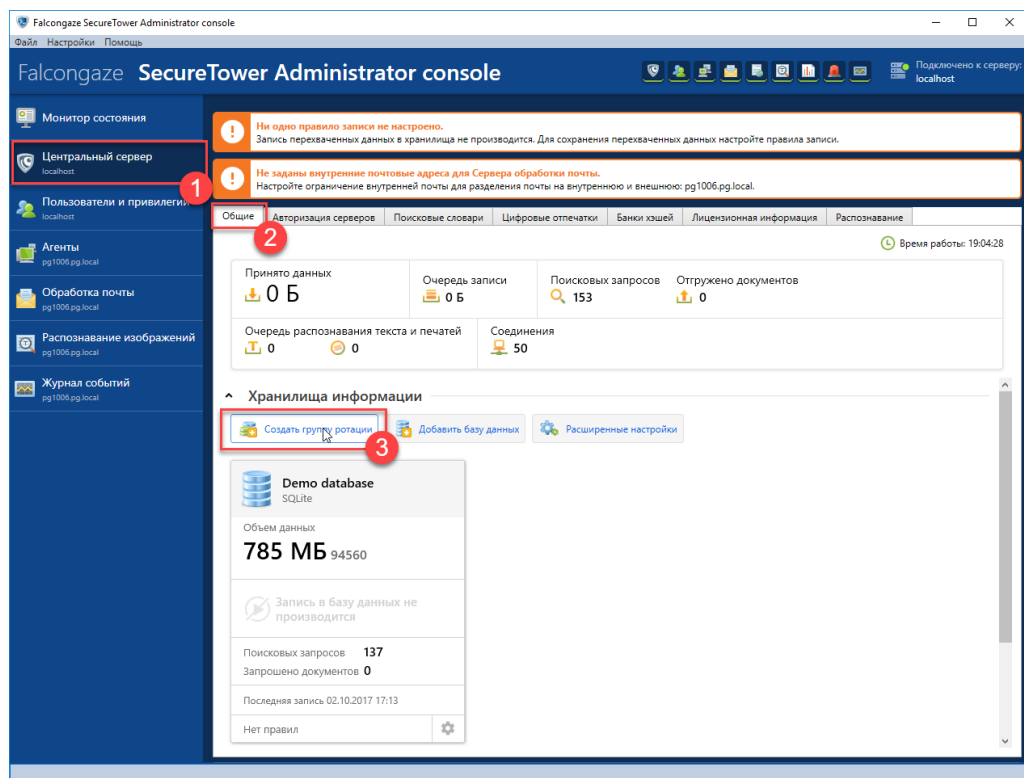


Для сохранения данных перехвата потребуется подключить хранилища данных и настроить правила записи.

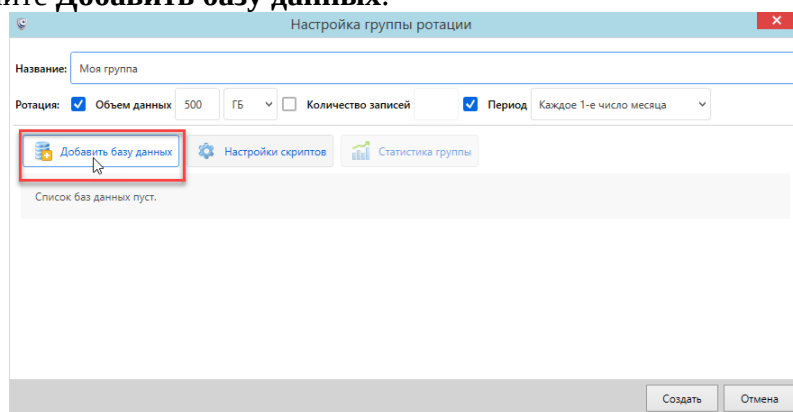
Создание группы ротации. Подключение базы данных PostgreSQL. Алгоритм действий

3.1 Выберите на боковой панели меню Консоли администратора вкладку **Центральный сервер**.

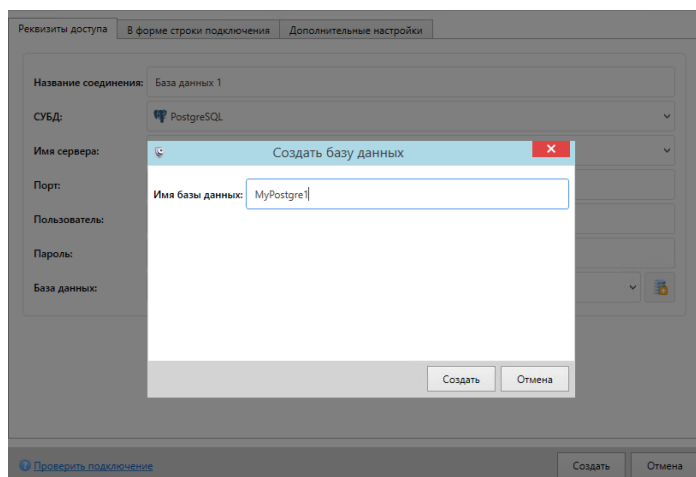
3.2 На вкладке **Общие** перейдите в раздел **Хранилища информации** и нажмите кнопку **Создать группу ротации**.



- 3.3 В окне настройки группы введите имя группы *Моя группа*.
- 3.4 Ознакомьтесь с настройками ротации в полях **Объем данных** и **Дни**.
- 3.5 Нажмите **Добавить базу данных**.

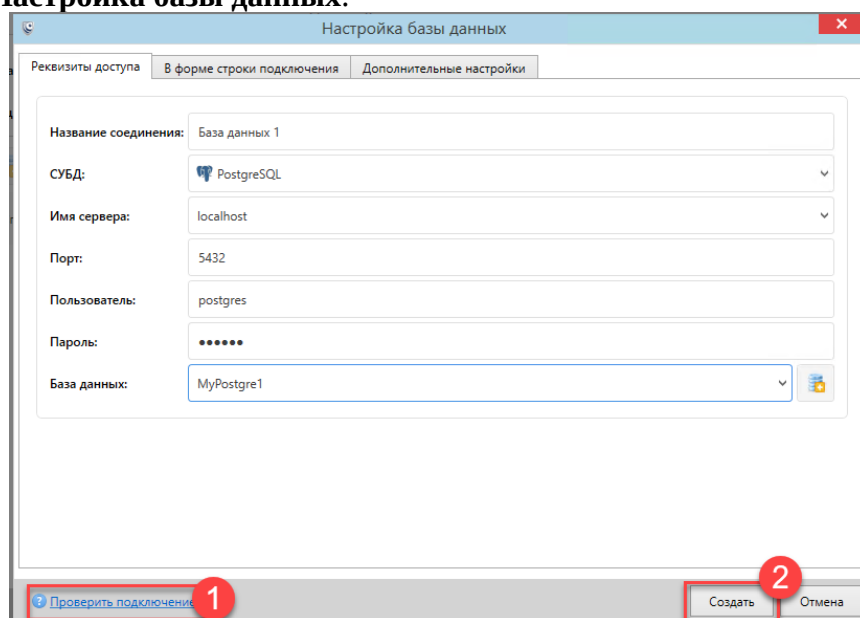


- 3.6 В окне **Настройка базы данных** на вкладке **Реквизиты доступа** в списке СУБД выберите PostgreSQL.
- 3.7 Поле **Имя сервера** оставьте без изменений (localhost) для создания базы данных на локальном компьютере.
- 3.8 Поле **Порт** (будет использоваться для подключения к базе данных) оставьте без изменений.
- 3.9 В соответствующих полях введите параметры авторизации пользователя, который имеет привилегии в СУБД для создания новых баз данных: имя пользователя и пароль для доступа к базе данных.
- 3.10 Напротив поля **База данных** нажмите кнопку **Создать базу данных**.
- 3.11 В окне **Создать базу данных** введите имя базы *MyPostgre1* и нажмите **Создать**.

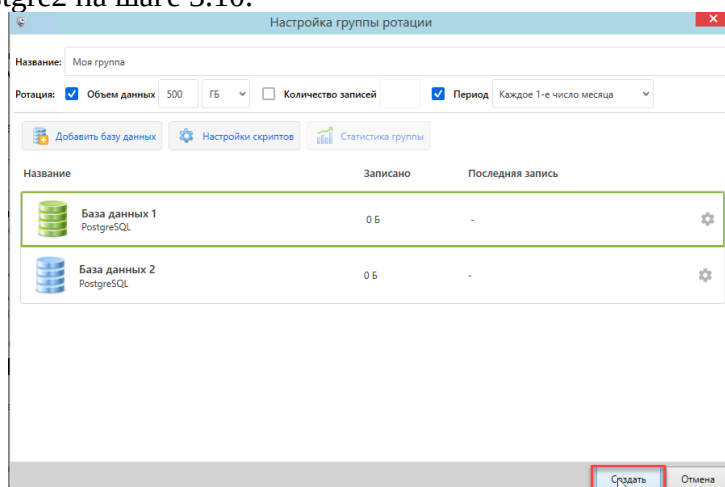


3.12 Нажмите **ОК** в окне подтверждения.

3.13 В нижнем левом углу окна **Настройка базы данных** нажмите ссылку **Проверить подключение**. После получения сообщения об успешной проверке нажмите **Создать** в окне **Настройка базы данных**.

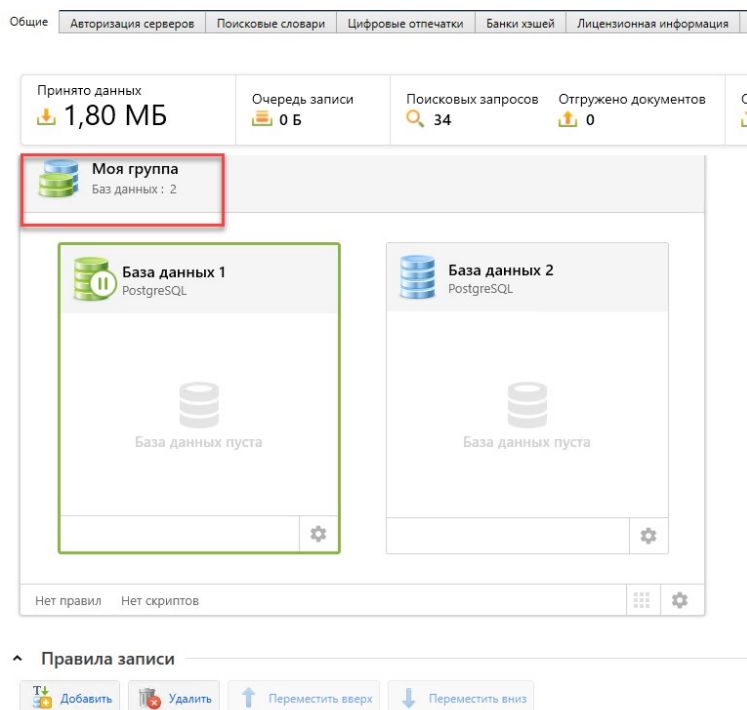


3.14 Добавьте еще одну базу в группу. Для этого повторите пп. 3.4-3.12, указав имя MyPostgre2 на шаге 3.10.



3.15 Нажмите **Создать** в окне настроек группы.

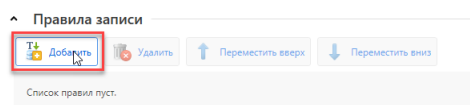
Результат: Группа ротации с именем *Моя группа* отображается в списке подключенных хранилищ раздела **Настройки хранилищ информации**.



Добавление правила записи в группу. Алгоритм действий

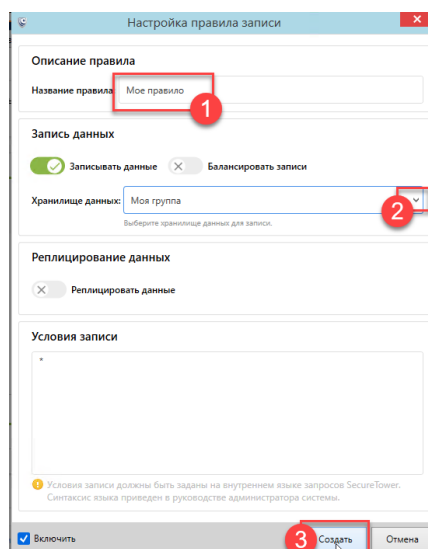
Для записи данных перехвата в новую группу необходимо создать правило записи.

3.16 Перейдите в раздел **Правила записи** и нажмите **Добавить**.



3.17 Введите имя правила *Мое правило* в поле **Название правила** в окне **Настройка правила записи**.

3.18 В списке **Хранилище данных** выберите группу **Моя группа** и нажмите **Создать**.



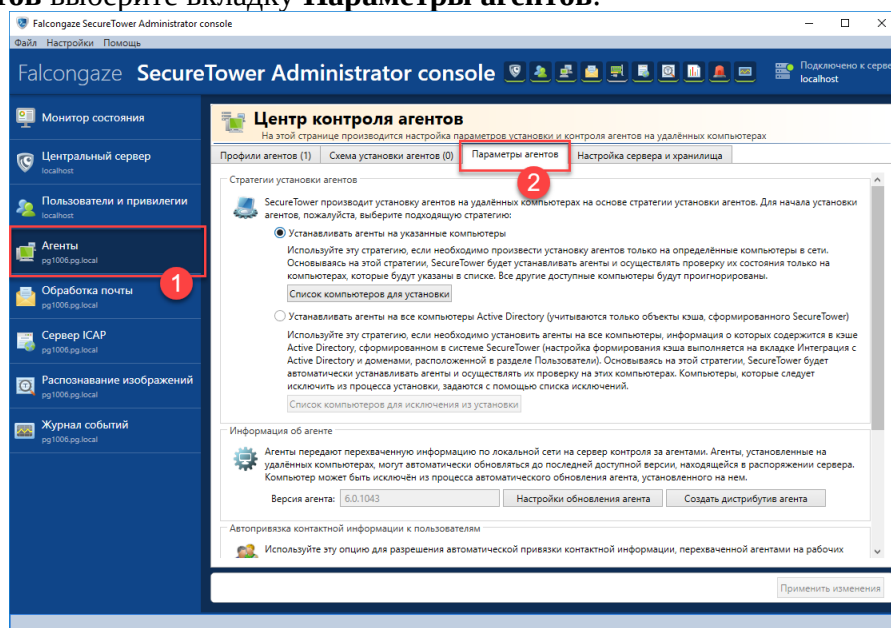
Результат: *Мое правило* добавлено в список правил записи.

4. Установка агентов на рабочие станции

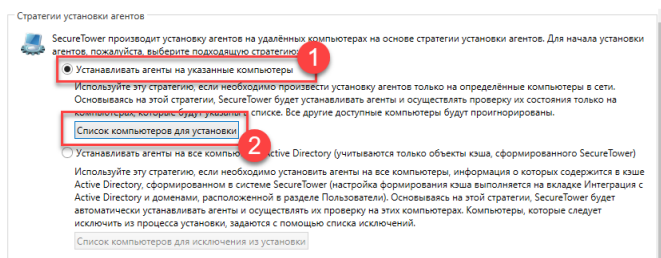
Получите у преподавателя имя компьютера из рабочей группы для установки агента и, если требуется, имя учетной записи Администратора сети для доступа к другим компьютерам рабочей группы. Используйте имя localhost при установке агента на свой компьютер.

Алгоритм действий

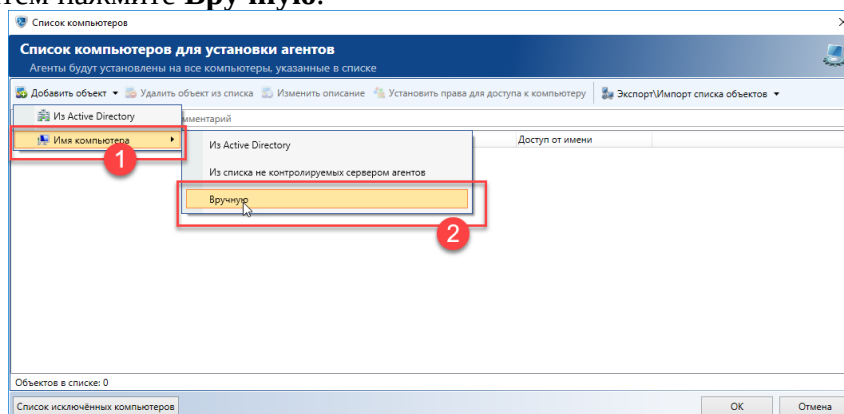
3.1 Выберите вкладку **Агенты** на боковой панели меню, затем в окне **Центр контроля агентов** выберите вкладку **Параметры агентов**.



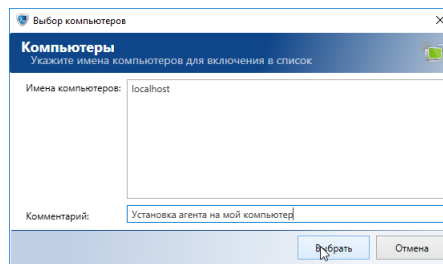
3.2 В разделе **Стратегии установки агентов** выберите опцию **Устанавливать агенты на указанные компьютеры**. Нажмите кнопку **Список компьютеров для установки**.



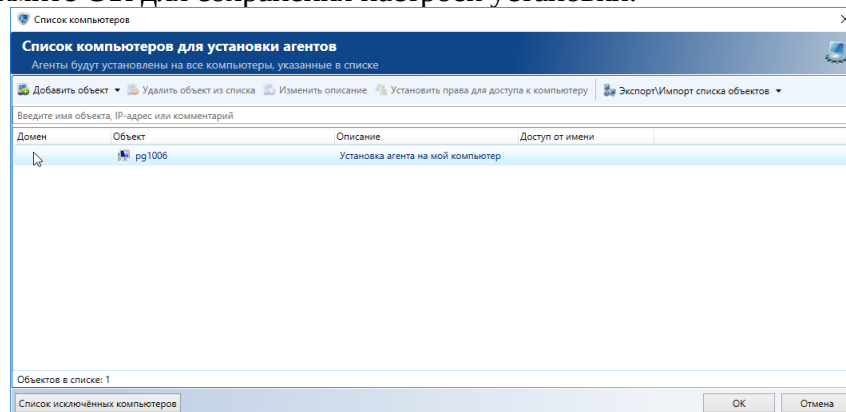
3.2.1 В окне настройки списка нажмите кнопку **Добавить объект**. Выберите **Имя компьютера** и затем нажмите **Вручную**.



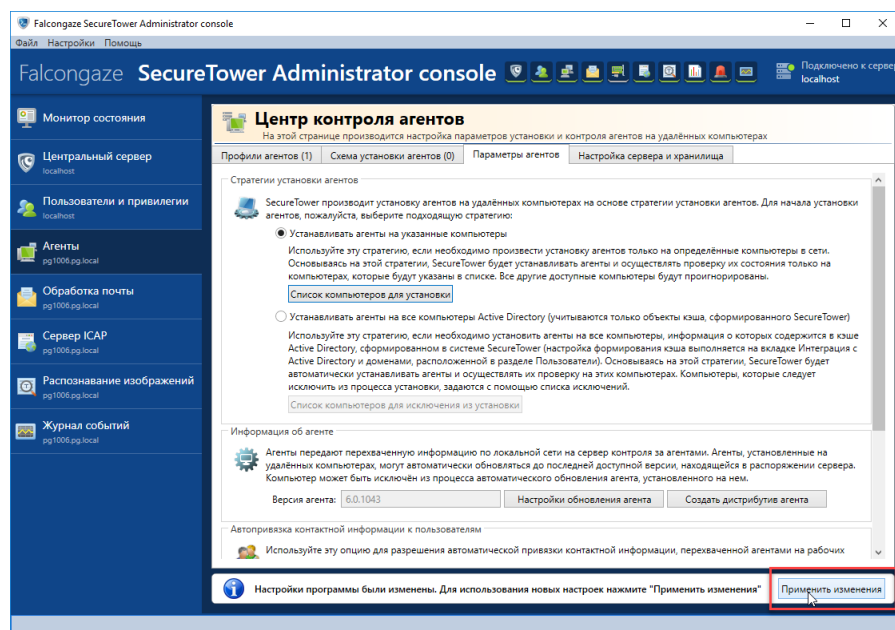
3.2.2 Введите в поле ввода **Имена компьютеров**, нажмите **Выбрать**.



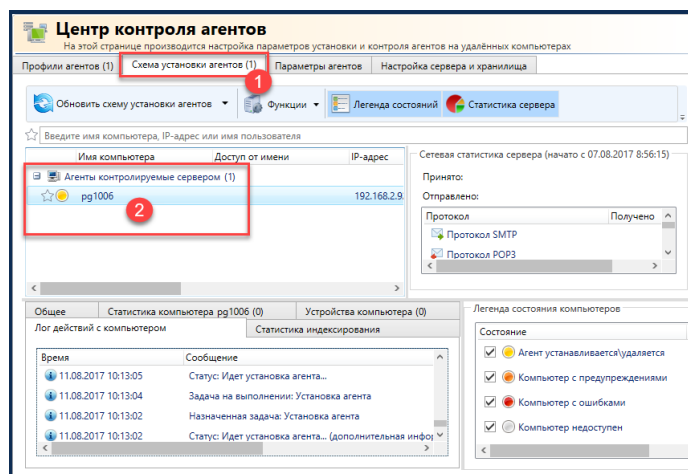
3.2.3 Нажмите **ОК** для сохранения настроек установки.



3.3 В нижнем правом углу главного окна консоли нажмите **Применить изменения**.



3.4 В окне **Центр контроля агентов** выберите вкладку **Схема установки агентов**.

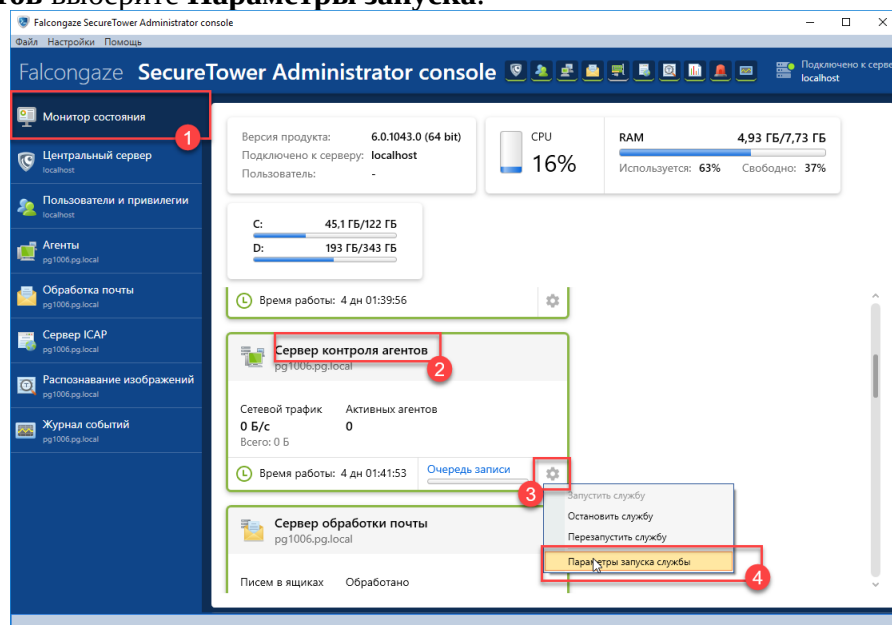


3.5 В списке компьютеров выберите имя компьютера, на котором был установлен агент на шаге 4.2. Если индикатор состояния агента желтого цвета, дождитесь завершения процесса.

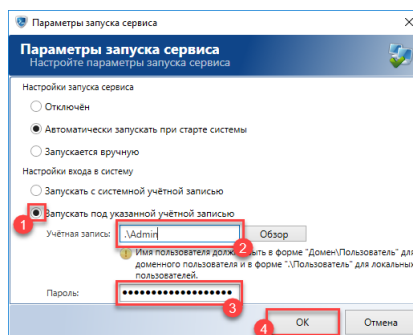
3.5.1 Если индикатор состояния агента после завершения процесса установки зеленого цвета - перейдите к шагу 5.1.

3.5.2 Если индикатор состояния агента красного цвета - перейдите к шагу 4.6 (Ситуация возникает, если сервер контроля агентов запущен от имени учетной записи, которая не имеет прав доступа к другим компьютерам рабочей группы либо не обладает правами администрирования на данном компьютере. Для установки агента необходимо запустить сервер от имени учетной записи с правами администрирования на всех компьютерах рабочей группы).

3.6 Перейдите в раздел **Монитор состояния** и в меню **Настройки сервера контроля агентов** выберите **Параметры запуска**.

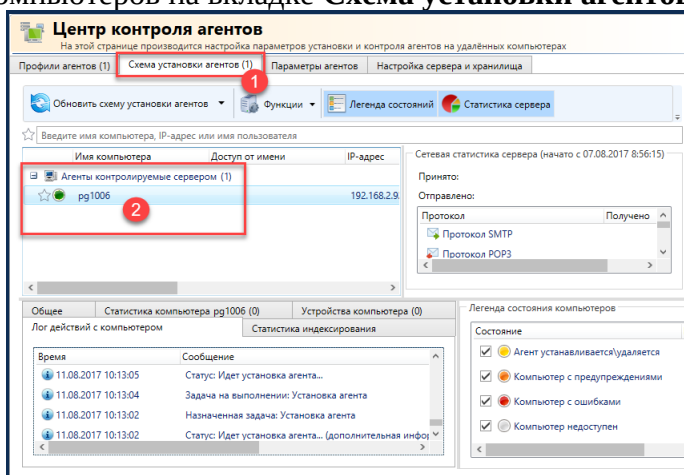


3.7 Выберите **Запускать под указанной учетной записью** в разделе **Настройки входа в систему**. Укажите имя и пароль учетной записи Администратора, полученные у преподавателя.



3.8 Подтвердите настройки и примите предложение системы о перезапуске сервиса для сохранения настроек. Перейдите к шагу 5.1.

Результат: Сетевое имя компьютера, который был указан для установки агента, отобразится в списке компьютеров на вкладке **Схема установки агентов**.

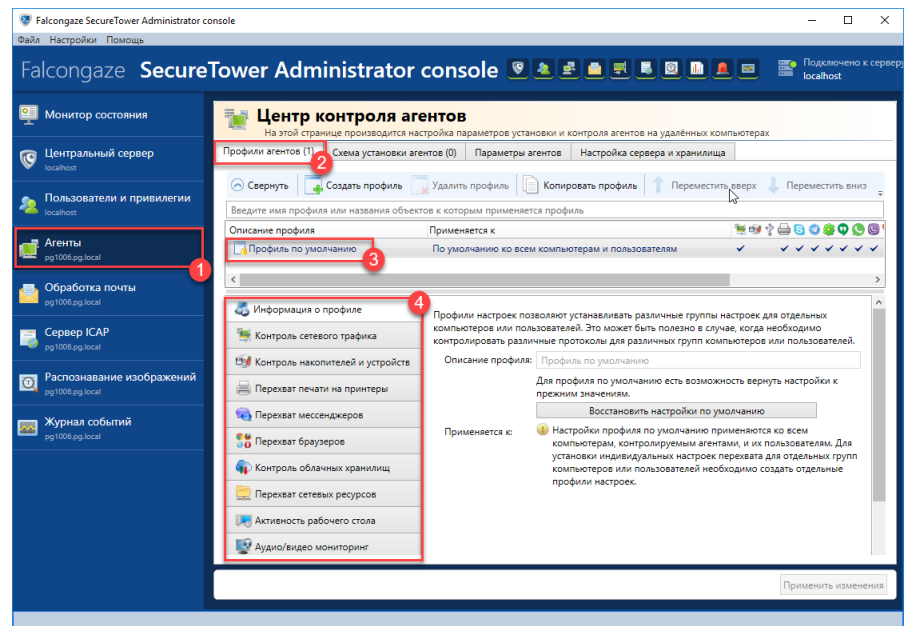


5. Конфигурация профиля работы агентов

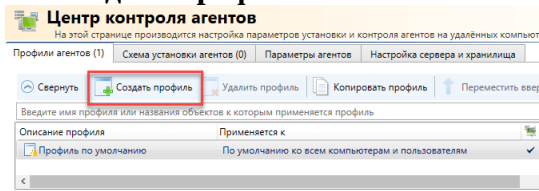
Алгоритм действий

3.9 Выберите вкладку **Агенты** на боковой панели главного окна консоли.

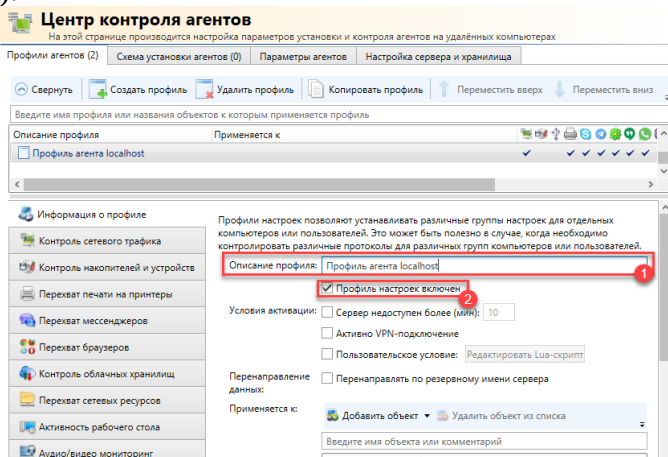
3.10 В окне **Центр контроля агентов** на вкладке **Профили агентов** изучите все настройки **Профиля по умолчанию**, переключаясь между вкладками доступных настроек в нижней части окна.



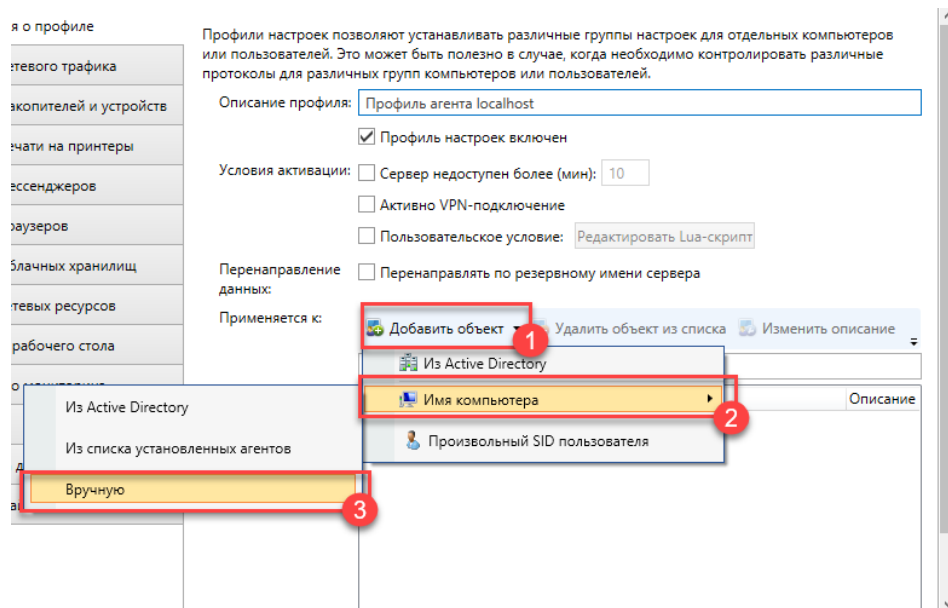
3.11 Создайте новый профиль для агента, установленного на локальном компьютере. Для этого нажмите **Создать профиль** на панели команд окна вкладки.



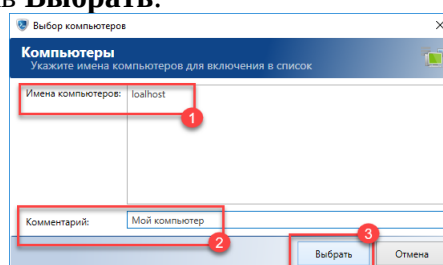
3.12 Введите имя нового профиля, например, «Профиль агента localhost» в поле **Описание профиля**. Убедитесь, что профиль настроек включен (отмечена соответствующая опция).



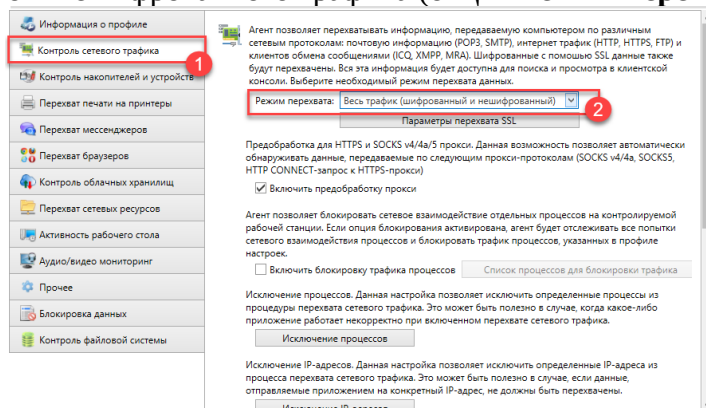
3.13 Примените новый профиль к компьютеру. Для этого нажмите кнопку **Добавить объект** и выберите опцию **Имя компьютера**, и далее нажмите **Вручную**.



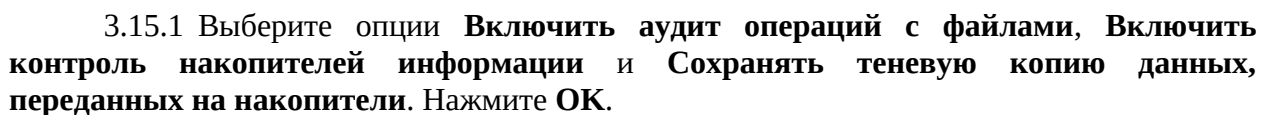
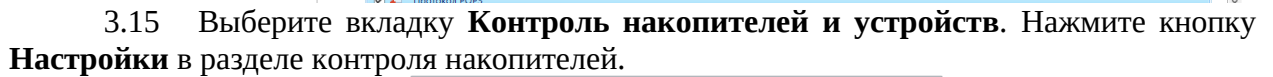
Укажите имя компьютера и комментарий по желанию в диалоговом окне и подтвердите выбор, нажав **Выбрать**.



3.14 Выберите вкладку **Контроль сетевого трафика**. Убедитесь, что включен перехват шифрованного и нешифрованного трафика (опция **Режим перехвата**).



3.14.1 Для того чтобы подробно изучить все доступные настройки протоколов, в списке **Протоколы, доступные для перехвата на клиентском компьютере** поочередно выберите каждый из протоколов и нажмите **Расширенные настройки протокола**. Изучите настройки.



Настройка контроля устройств

Настройка контроля устройств

Настроить параметры контроля и задать исключения из общих настроек

Если опция контроля включена, агент будет предоставлять информацию о всех подключенных устройствах и выполнять контроль доступа к подключенным устройствам с учетом заданных настроек исключений. Информация о подключенных устройствах будет доступна для просмотра на сервере консоли администратора.

☒ Включить контроль устройств 1

Некоторые устройства могут быть запрещены к использованию. Агент будет блокировать доступ указанным устройствам.

☒ Настроить контроль устройств не применяемых к внешним накопителям информации.

Активация опций контроля накопителей осуществляется в окне "Настройка контроля устройств" текущейкладки.

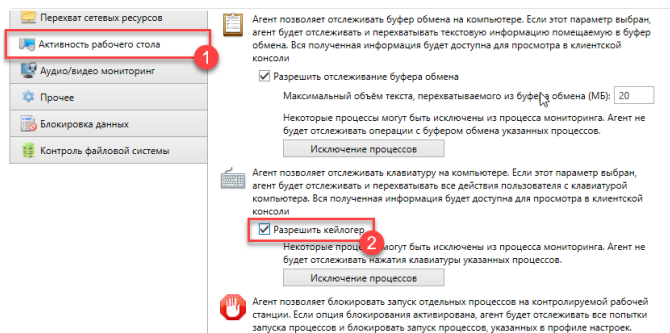
Исключения доступа

Если опция аудита включена, агент будет выполнять аудит подключенных устройств к рабочей станции. Информация о подключении будет доступна для просмотра клиентской консоли.

☒ Включить использование устройств 2

OK Отмена

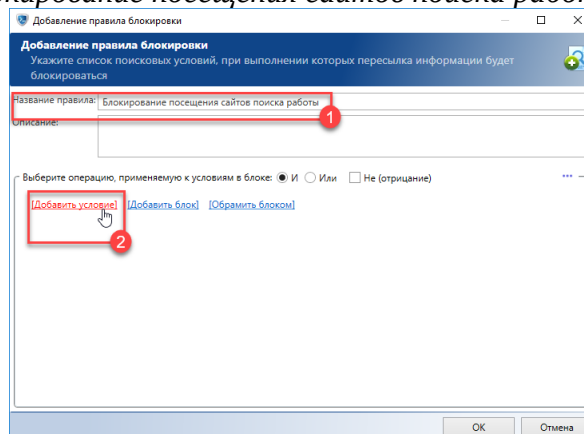
18



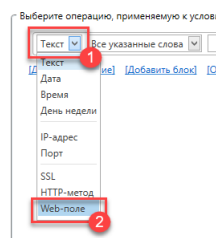
3.18 Выберите вкладку **Блокировка данных**.

3.18.1 В окне настройки блокирования нажмите кнопку **Добавить** и выберите в меню пункт **Правило блокирования HTTP**.

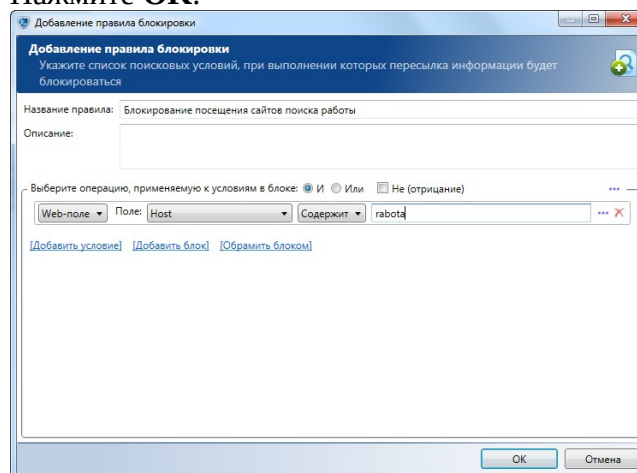
3.18.2 В окне добавления правила блокирования введите в поле **Название правила** имя правила «*Блокирование посещения сайтов поиска работы*».



3.18.3 Нажмите **Добавить условие** и выберите из списка условий, доступного при нажатии на кнопку **Текст**, условие **Web-поле**.

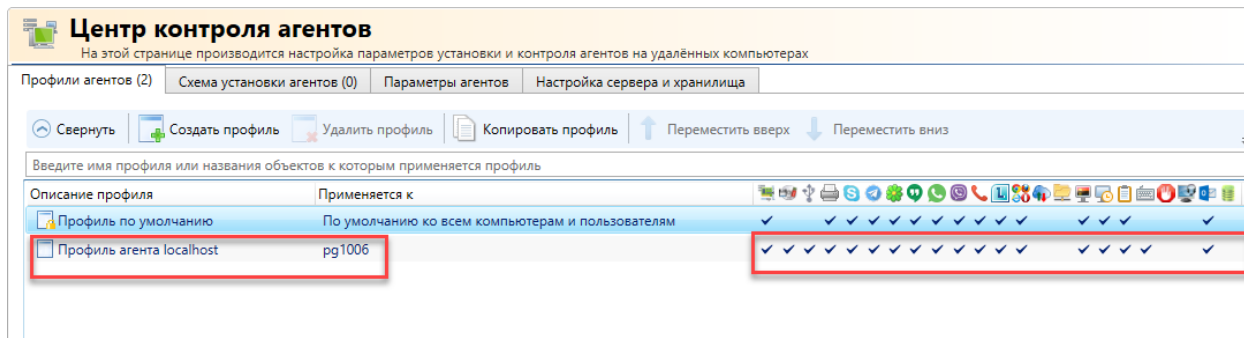


3.18.4 В списке значений веб-поля выберите **Host**. Выберите условие **Содержит** и введите значение **rabota**. Нажмите **ОК**.



3.19 Ознакомьтесь с прочими настройками агента и нажмите **Применить изменения** в нижнем правом углу главного окна консоли.

Результат: В списке профилей агента отображается профиль «Профиль агента localhost». В колонке **Применяется к** отображается сетевое имя локального компьютера, а в списке настроек помимо включенных по умолчанию отмечены опции контроля устройств и накопителей информации, а также опция кейлогера.



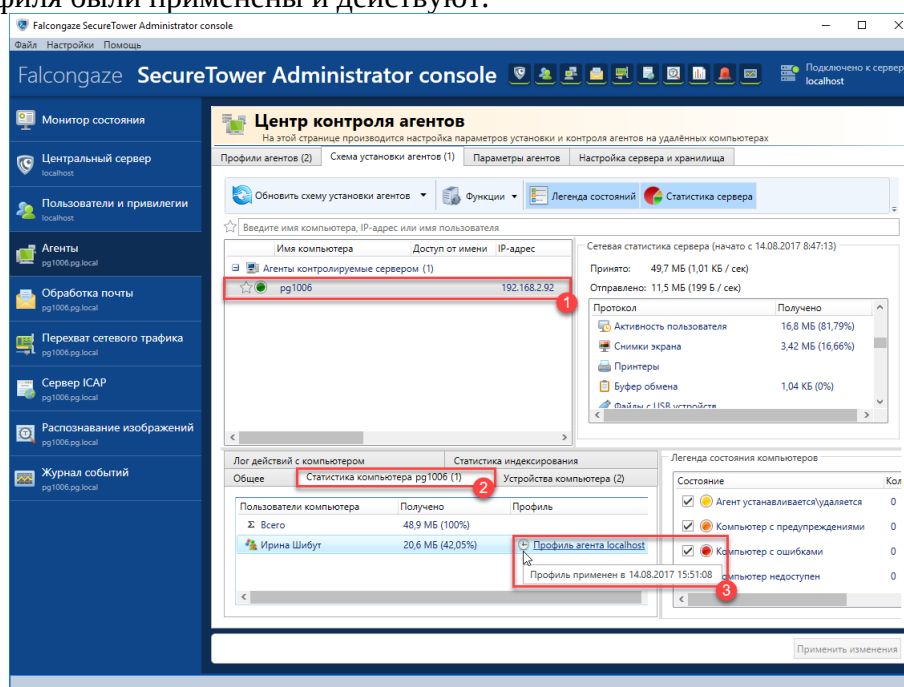
6. Контроль работы агентов

Алгоритм действий

6.1 В окне **Центр контроля агентов** выберите вкладку **Схема установки агентов**. Ознакомьтесь с представленной в окне информацией.

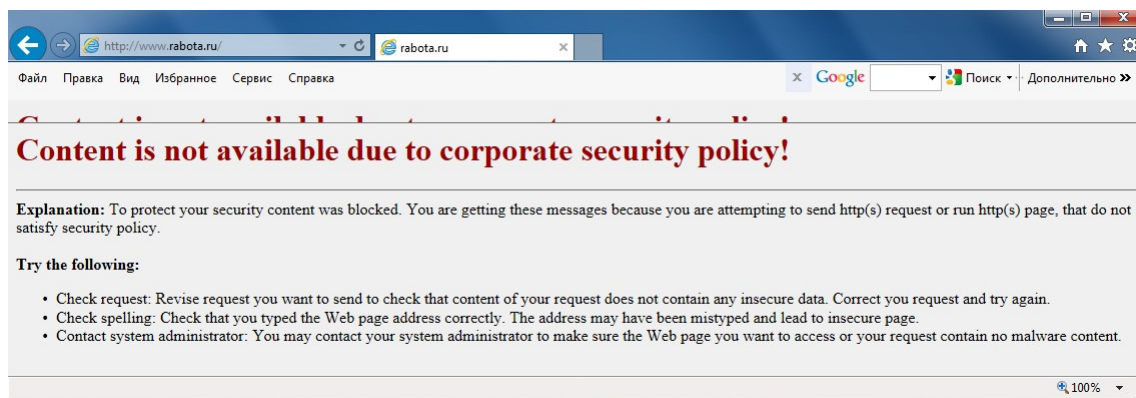
6.2 В списке компьютеров выберите имя компьютера, на котором был установлен агент на шаге 4.2.

6.3 Выберите вкладку **Статистика компьютера**, наведите указатель мыши на иконку часов рядом с именем профиля, применяемого к данному агенту. Убедитесь, что изменения профиля были применены и действуют.



Изучите прочую информацию, представленную в данном окне о подключенных устройствах, логе (журнале) действий, о статистике работы агента.

6.4 Перейдите в любой установленный на рабочей станции интернет - браузер и введите **rabota.ru** в адресную строку. Убедитесь, что доступ к сайту заблокирован.

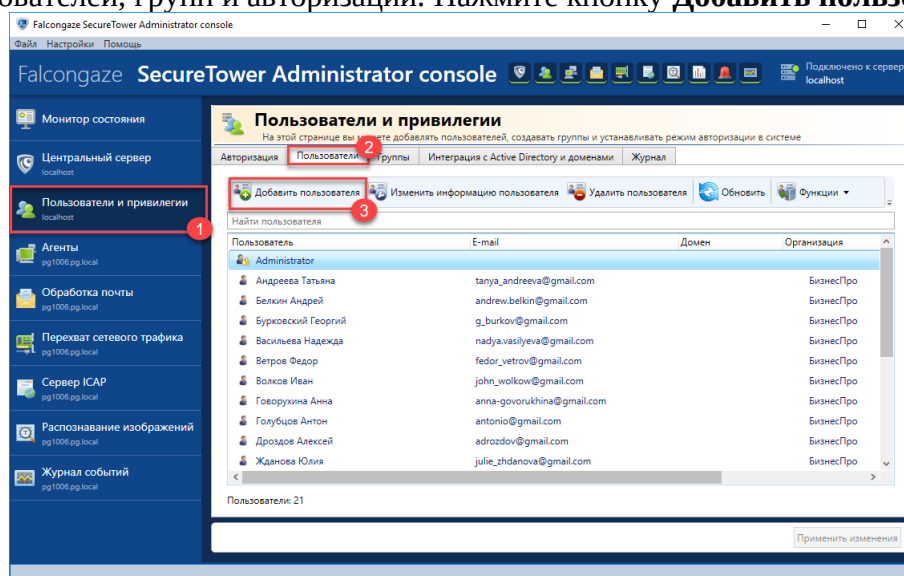


Результат: Агент присылает данные по протоколам согласно настройкам профиля.

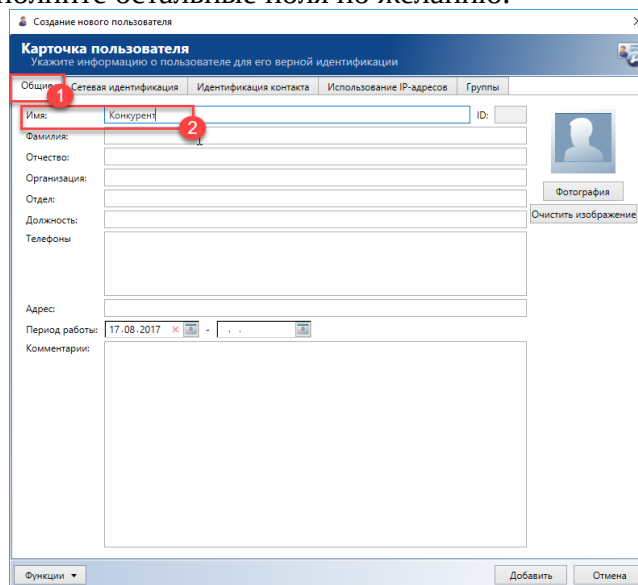
7. Работа с базой пользователей

Алгоритм действий

7.1 Выберите вкладку **Пользователи и привилегии** на боковой панели главного окна Консоли администратора. Выберите вкладку **Пользователи** в окне настроек пользователей, групп и авторизации. Нажмите кнопку **Добавить пользователя**.



7.2 В открывшемся окне **Карточка пользователя** введите в поле **Имя** «Конкурент», а также заполните остальные поля по желанию.



7.3 Нажмите **Добавить** в окне создания карточки и закройте окно. Новый пользователь будет добавлен в базу системы, но не будет связан с каким-либо контролируемым пользователем сети.

Казаков Денис	denis-kazak@gmail.com	БизнесПро
Коваленко Марина	marina.kovalenko@gmail.com, marykova@sipi	БизнесПро
Конкурент		
Кравцова Елена	lena.kravt@gmail.com	БизнесПро

7.4 Нажмите **Применить изменения** в нижнем правом углу главного окна консоли.

Результат: Имя пользователя отображается в списке пользователей, зарегистрированных в системе.

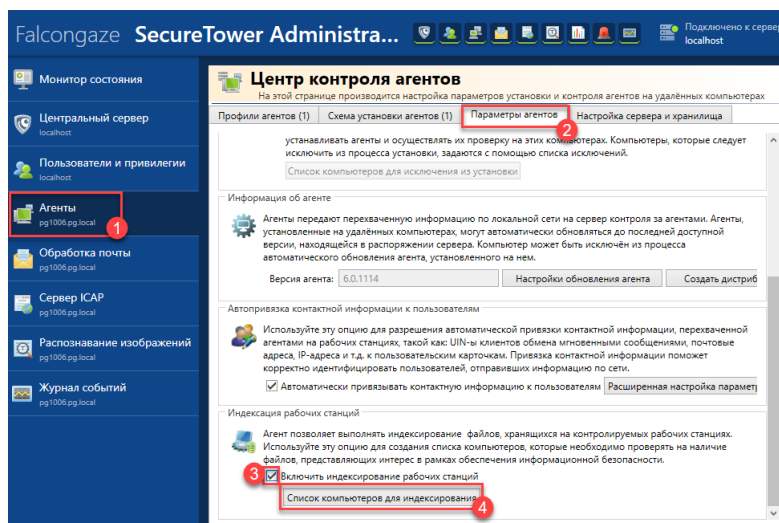
8. Настройка индексации рабочих станций

Алгоритм действий

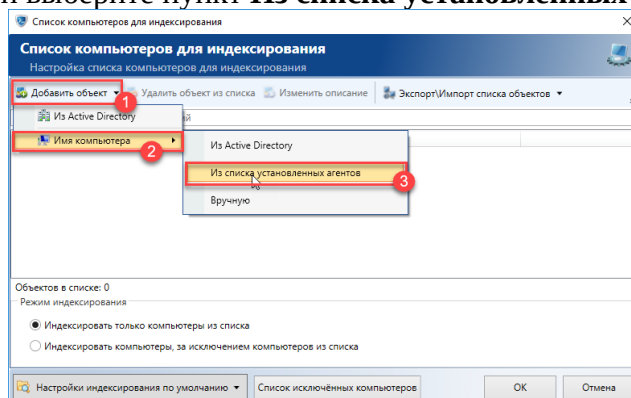
8.1 Выберите вкладку **Агенты**.

8.2 В окне Центра контроля агентов выберите вкладку **Параметры агентов**.

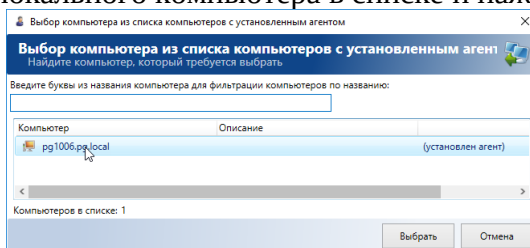
8.3 Перейдите в раздел **Индексация рабочих станций**, отметьте **Включить индексирование рабочих станций** и нажмите **Список компьютеров для индексирования**.



8.3.1 В окне настройки индексирования нажмите **Добавить объект**, выберите пункт **Имя компьютера** и выберите пункт **Из списка установленных агентов**.



8.3.2 Выберите имя локального компьютера в списке и нажмите **Выбрать**.



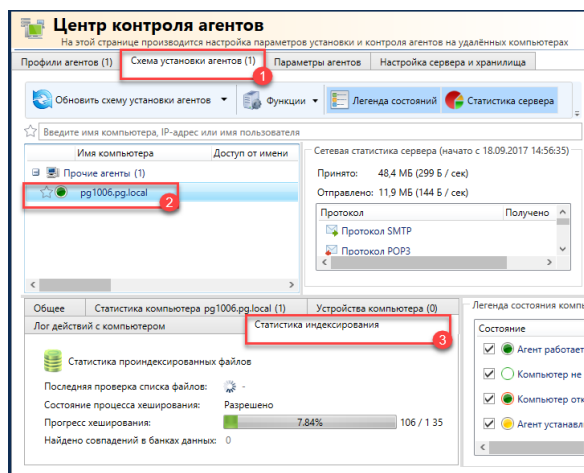
8.3.3 Нажмите **ОК** в окне настройки индексации.

8.3.4 Нажмите **Применить изменения** в нижнем правом углу окна консоли.

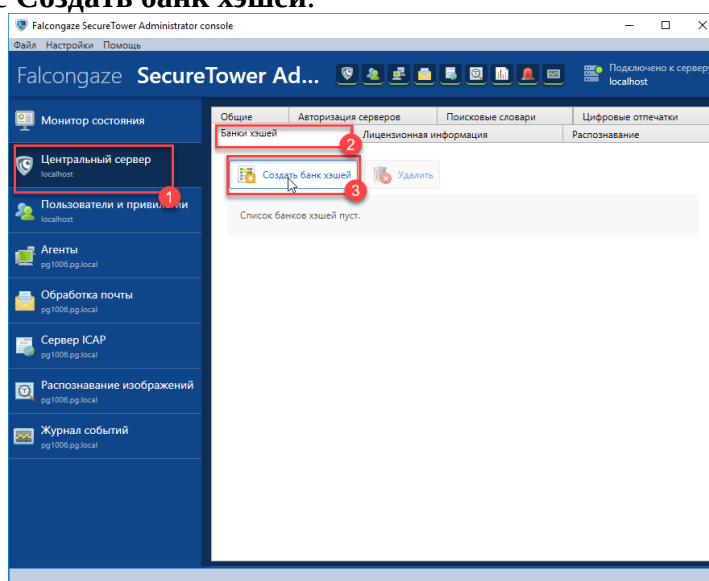
8.3.5 Перейдите на вкладку **Схема установки агентов**.

8.3.6 Выберите имя локального компьютера в списке и выберите закладку **Статистика индексирования** в зоне просмотра статистики.

Результат: Статистика индексирования отображается на соответствующей закладке.

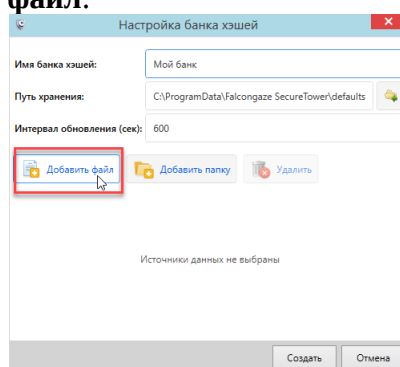


- 8.4 Перейдите на вкладку **Центральный сервер** и выберите вкладку **Банки хэшей**.
- 8.5 Нажмите **Создать банк хэшей**.

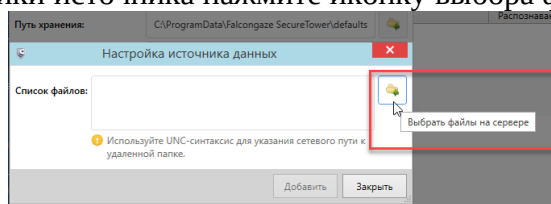


8.5.1 Задайте имя банка *Мой банк*.

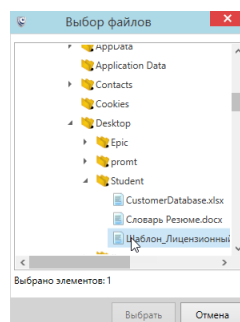
8.5.2 Нажмите **Добавить файл**.



8.5.3 В окне настройки источника нажмите иконку выбора файла на сервере.

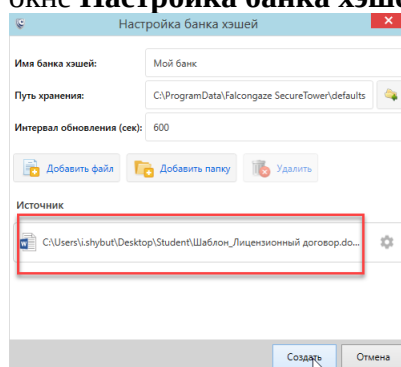


8.5.4 Выберите файл *Шаблон Лицензионный договор.docx*, расположенный на рабочем столе пользователя в папке Student (**C:\Users\Student\Desktop\Student**) и нажмите **Выбрать**.



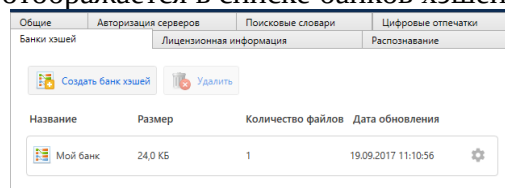
8.5.5 Нажмите **Добавить** в окне настройки источника. Запись о файле отобразится в окне настройки банка.

8.5.6 Нажмите **Создать** в окне **Настройка банка хэшей**.



8.5.7 Нажмите **ОК** в окне подтверждения действия.

Результат: Имя банка отображается в списке банков хэшей.



8.6 Для включения контроля файловых систем выберите вкладку **Агенты**.

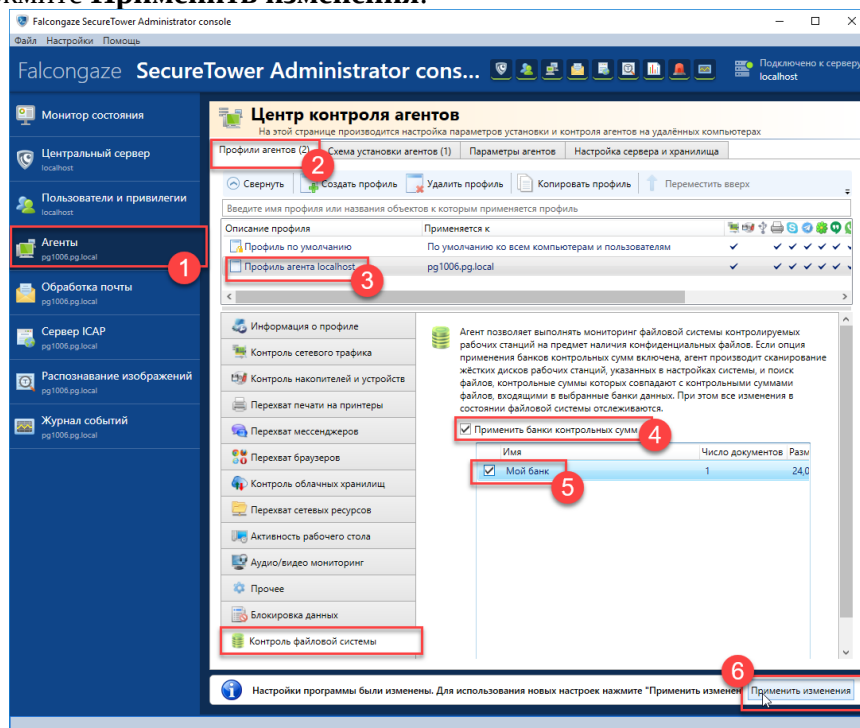
8.6.1 Перейдите на вкладку **Профили агентов**.

8.6.2 Выберите в списке профилей *Профиль агента localhost*.

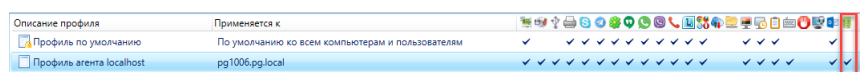
8.6.3 В зоне настроек профиля выберите закладку **Контроль файловых систем**

8.6.4 Отметьте **Применить банки контрольных сумм** и отметьте банк *Мой банк* в списке доступных.

8.6.5 Нажмите **Применить изменения**.



Результат: Индикатор контроля файловых систем установлен в профиле агента.



9. Удаление агента (для ознакомления)*

Алгоритм действий

9.1 Выберите вкладку **Агенты**.

9.2 В окне Центра контроля агентов выберите вкладку **Схема установки агентов**. Выберите имя компьютера, на котором был установлен агент в списке компьютеров, и в контекстном меню компьютера выберите команду **Удалить агента и исключить компьютер из схемы**.

9.3 Нажмите **Применить изменения** в нижнем правом углу главного окна консоли.

9.4 Дождитесь исключения агента из схемы.

9.5 Закройте окно Консоли администратора.

Контрольные вопросы

1. Для чего используется Консоль администратора?
2. В каких случаях при подключении к серверу указывается локальный компьютер?
3. Какие способы перехвата поддерживает система и в чем их отличие?
4. Для чего необходимо добавить правило записи при создании новой группы ротации/добавлении хранилища.
5. Какие способы установки агентов поддерживает система?
6. Возможно ли, используя настройки агента, запретить доступ к USB/ к сетевым ресурсам/ к принтерам?
7. Как, используя параметры профиля настроек, защитить агента от удаления?
8. Какой раздел Консоли администратора содержит информацию о работе агентов, установленных на компьютеры в сети организации?
9. Каким образом осуществляется привязка перехваченной информации к конкретным пользователям?
10. Как добавляется и обновляется информация о пользователях системы, если сеть организации построена на базе Active Directory/рабочей группы?