ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

Лабораторная работа №1

Выполнили студенты группы ИКТЗ-83:

Громов А.А., Миколаени М.С., Мазеин Д.С.

_____

(Ф.И.О., № группы) *(подпись)*

Проверил:

Казанцев А.А. _____

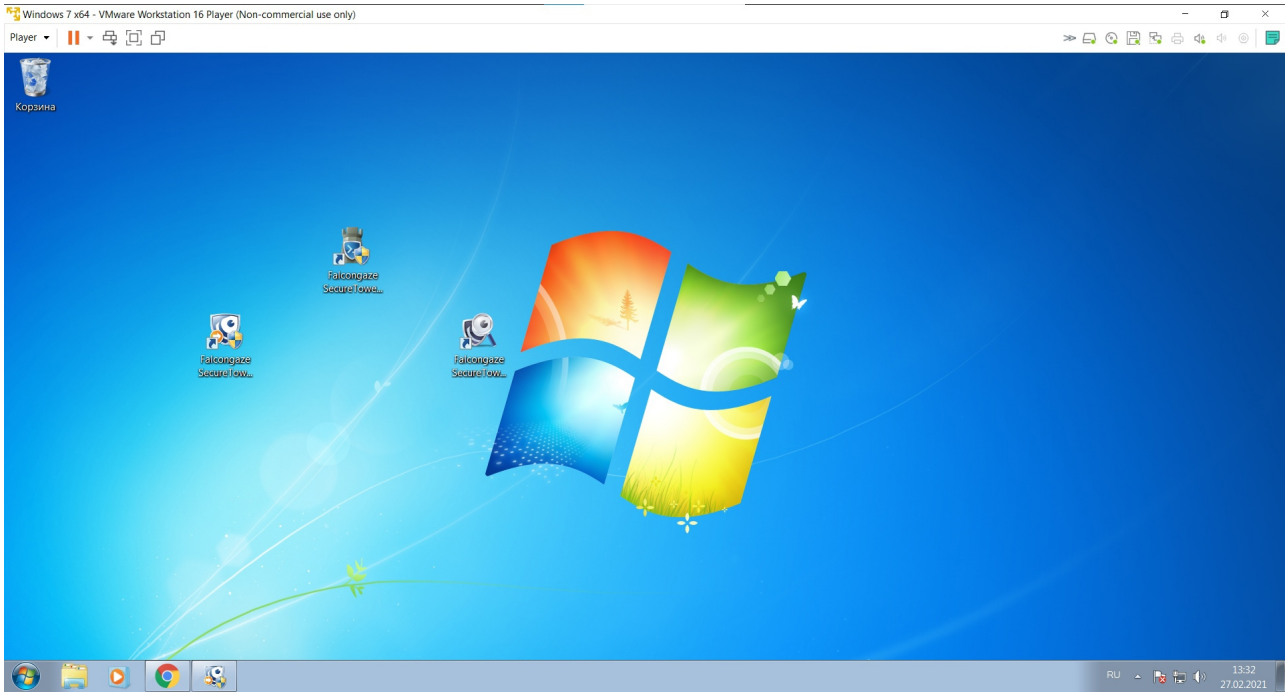
(уч. степень, уч. звание, Ф.И.О.) *(подпись)*

Санкт-Петербург

2021

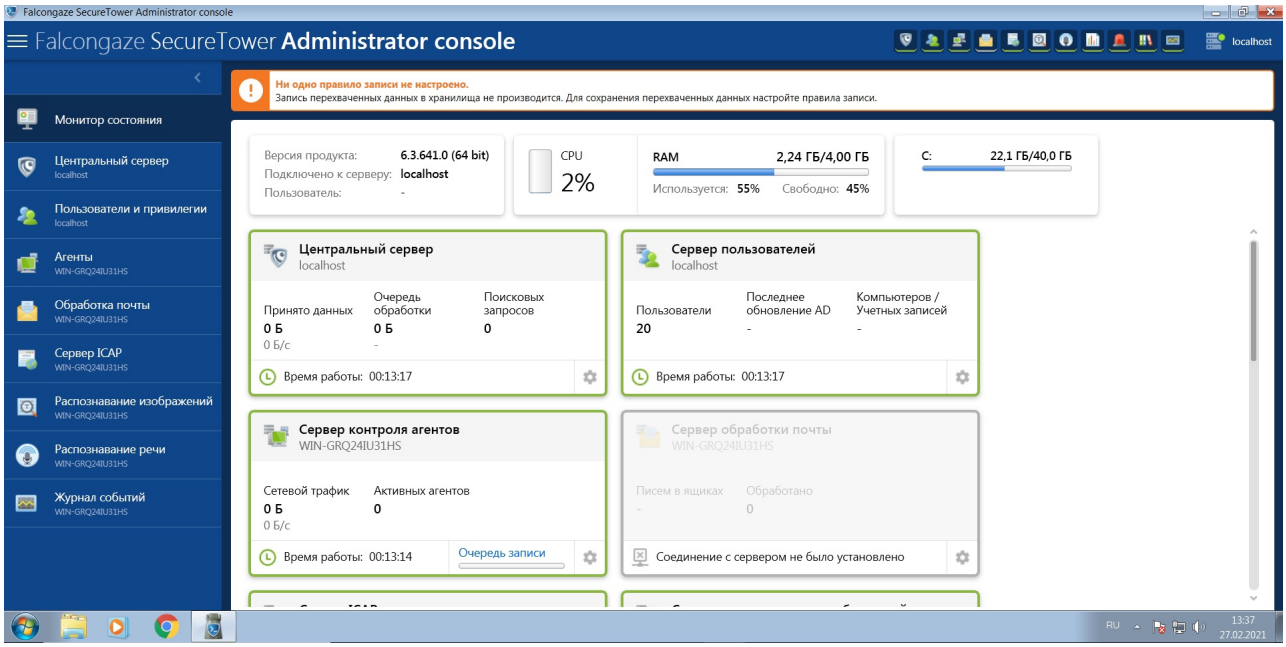
Цель лабораторной работы: Научиться устанавливать компоненты программного комплекса на локальный компьютер, устанавливать агента на компьютер рабочей группы, настраивать перехват данных при помощи агента, настраивать работу ключевых сервисов Falcongaze SecureTower.

Пункт 1 - Установка компонентов программного комплекса SecureTower.



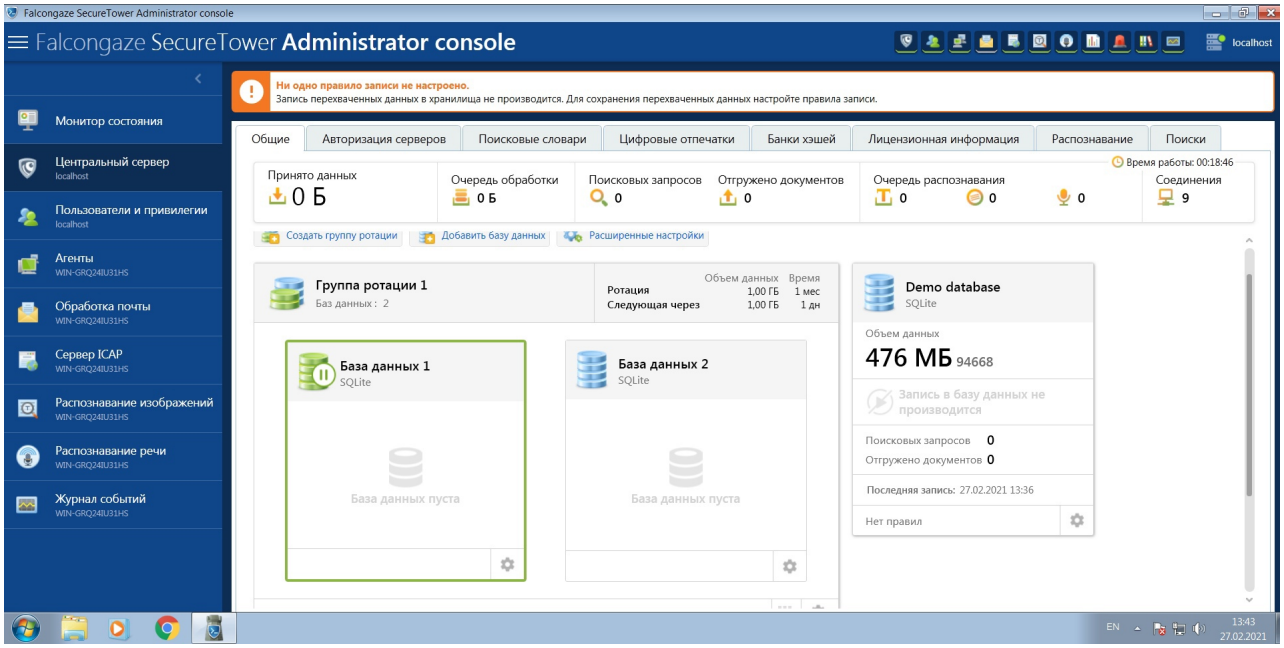
Ярлыки Falcongaze SecureTower Client ConsoleиFalcongaze SecureTower Admin Console добавлены на рабочий стол.

Пункт 2 - Запуск Консоли системного администратора SecureTower Admin Console.



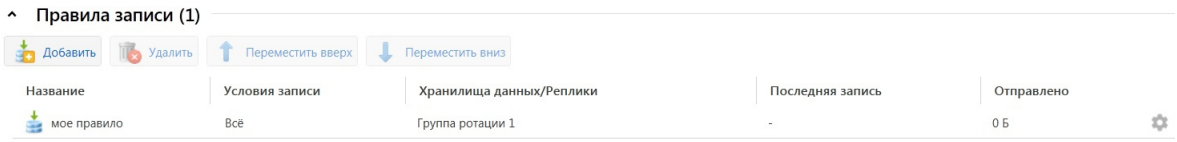
Все сервера системы установлены и работают без ошибок(кроме сервира обработки почты).

Пункт 3 - Настройки хранения информации.



Группа ротации с именем *Группа ротации 1* отображается в списке подключенных хранилищ раздела **Настройки хранилищ информации**.

Пункт 3.1 - Добавление правила записи в группу.



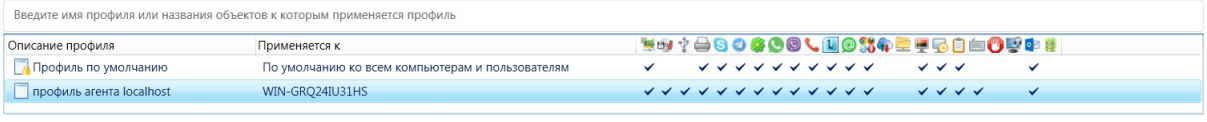
Мое правило добавлено в список правил записи.

Пункт 4 - Установка агентов на рабочие станции.

pics/4.jpg

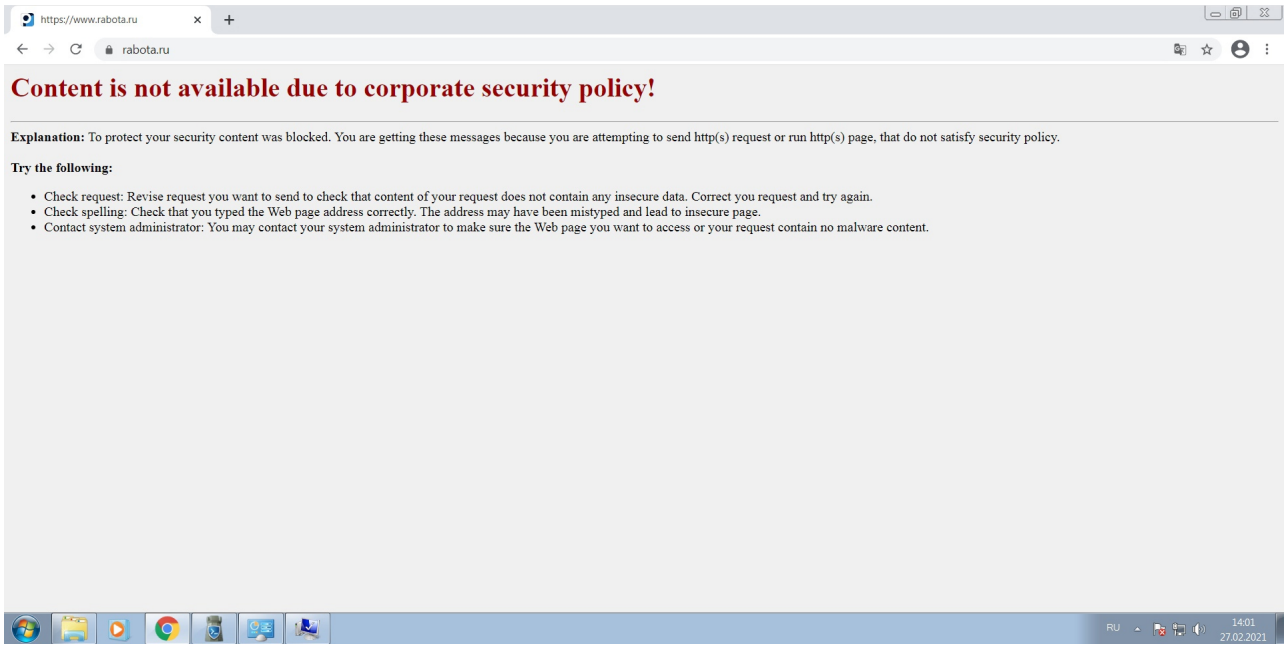
Сетевое имя компьютера, который был указан для установки агента,отобразится в списке компьютеров на вкладке **Схема установки агентов**.

Пункт 5 - Конфигурация профиля работы агентов.



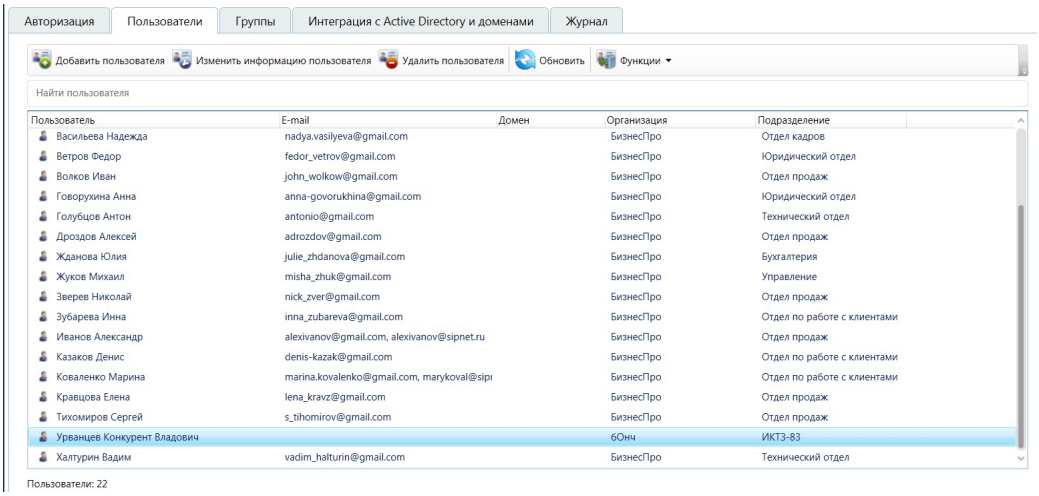
В списке профилей агента отображается профиль «Профиль агенталocalhost». В колонке Применяется к отображается сетевое имя локального компьютера, а в списке настроек помимо включенных по умолчанию отмечены опции контроляустройств и накопителей информации, а также опция кейлогера.

Пункт 6 - Контроль работы агентов.



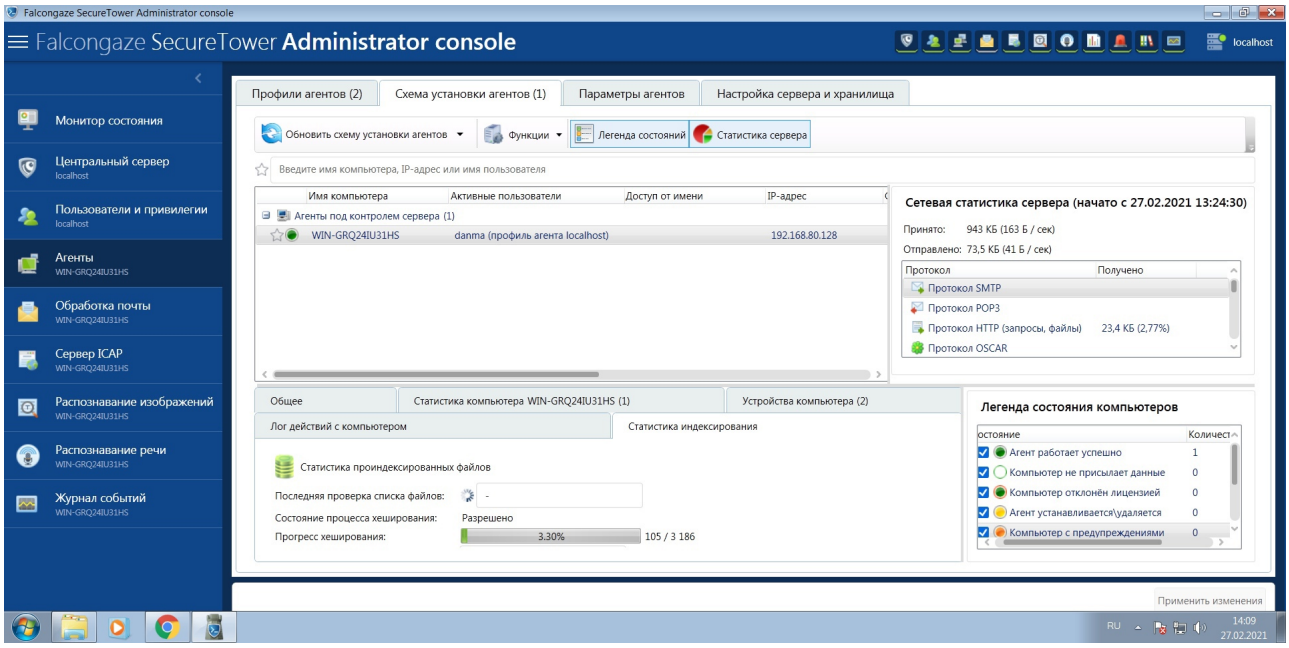
Агент присылает данные по протоколам согласно настройкам профиля.

Пункт 7 - Работа с базой пользователей.



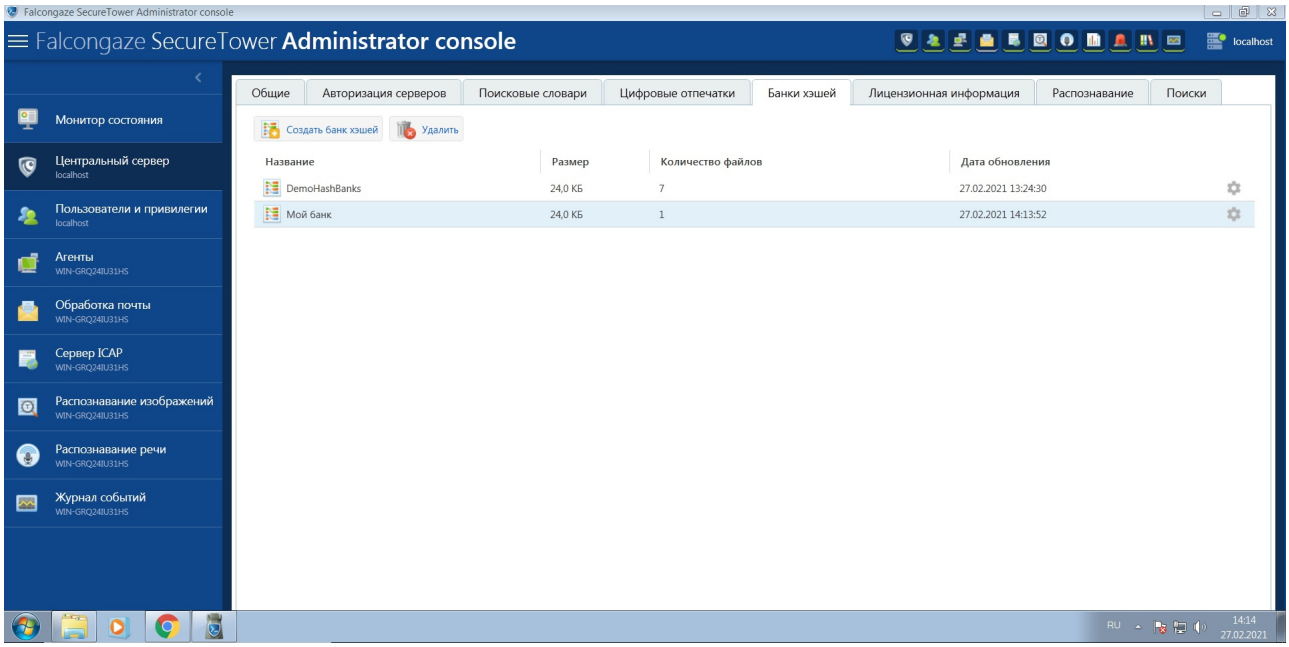
Имя пользователя отображается в списке пользователей, зарегистрированных в системе.

Пункт 8 - Настройка индексации рабочих станций.



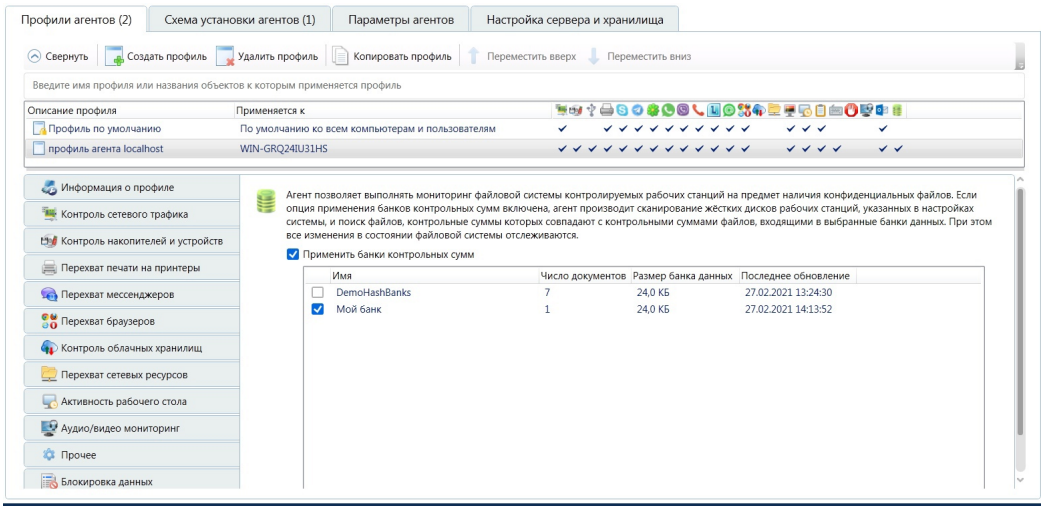
Статистика индексирования отображается на соответствующей закладке.

Пункт 8.5 - Создание банка хэшей.



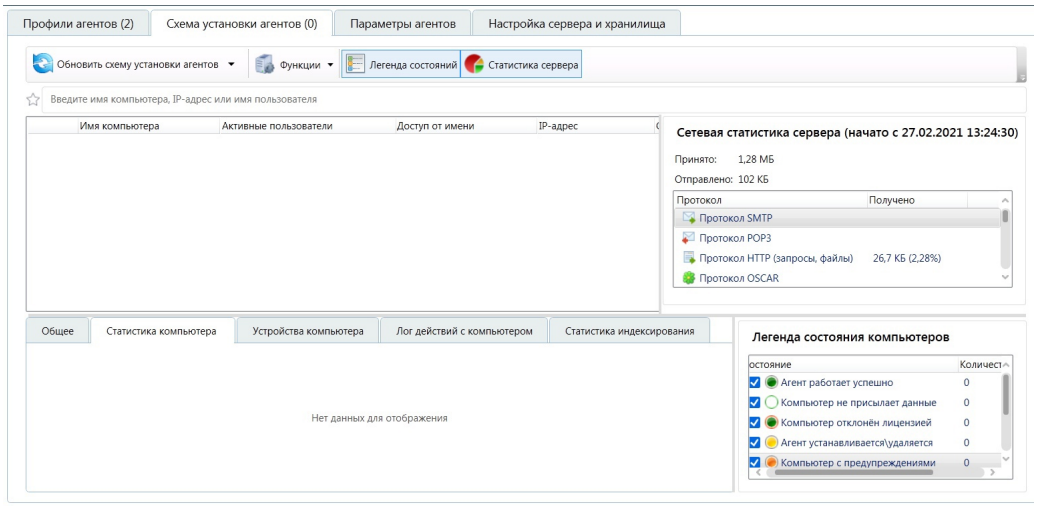
Имя банка отображается в списке банков хэшей.

Пункт 8.2 - Включение контроля файловых систем.



Индикатор контроля файловых систем установлен в профиле агента.

Пункт 9 - Удаление агента.



Удалены все агенты.

Вывод:

В ходе данной лабораторной работы мы изучили одну из DLP-систем - Falcongaze SecureTower. Данная система предназначена для контроля утечек данных. Нами была произведена установка серверной и клиентской частей данной программы. С помощью серверной части был создан и настроен агент, к которому были применены различные политики перехвата и контроля данных. Также был настроен профиль пользователя ”Конкурент”.

Ответы на контрольные вопросы

1. **Для чего используется Консоль администратора?**

   Консоль администратора используется для настройки и управления компонент Falcongaze.

2. **В каких случаях при подключении к серверу указывается локальный компьют**

   Локальный компьютер указывается в том случае, когда консоль запускается на том же компьютере, где установлены серверные компоненты системы

3. **Какие способы перехвата поддерживает система и в чем их отличие?**

   Система Falcongaze SecureTower может перехватывать трафик данных двумя способами: централизованно, либо агентами, устанавливаемыми на рабочие станции.

   Централизованный перехват имеет ряд недостатков – более трудоёмкий процесс настройки, перехватывать возможно только трафик, передаваемый по нешифрованным протоколам.

   Агенты, установленные на рабочих станциях, позволяют перехватывать весь трафик – как нешифрованный, так и шифрованный (по протоколам, использую SSL-шифрование: HTTPS, FTPS, SMTPS, POP3S, IMAP4S, SIP, протоколы мессенд 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, содержим буфера обмена, реализуют функцию кейлогера, осуществляют аудит подключения внешних устройств, аудит файловых систем компьютеров и многое другое. Важной функциональной особенностью агента является возможность блокирован 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.

4. **Для чего необходимо добавить правило записи при создании новой группы ротации/добавлении хранилища.**

Для записи данных перехвата в новую группу, репликации данных, а также задания условий записи.

5. **Какие способы установки агентов поддерживает система?**

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

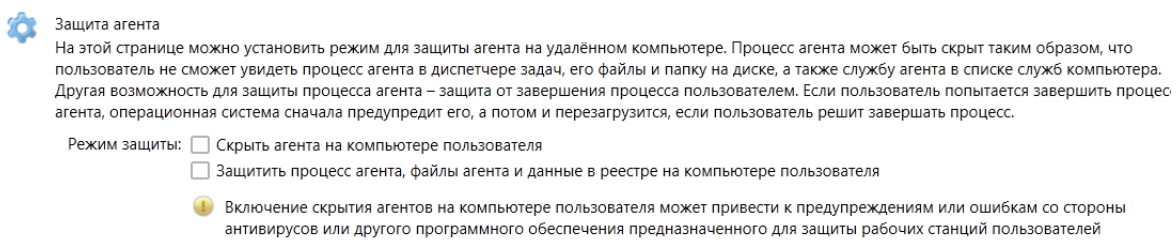
- централизованно на выборочные компьютеры либо на все доступные компьют в сети (с Сервера контроля агентов SecureTower через Консоль администратора
- через групповые политики домена;
- вручную с помощью отдельного инсталлятора, запущенного на рабочей станции, подлежащей контролю.

6. **Возможно ли, используя настройки агента, запретить доступ к USB/ к сетевым ресурсам/ к принтерам?**

Возможно заблокировать доступ ко всему перечисленному оборудованию с помощью настроек агента.

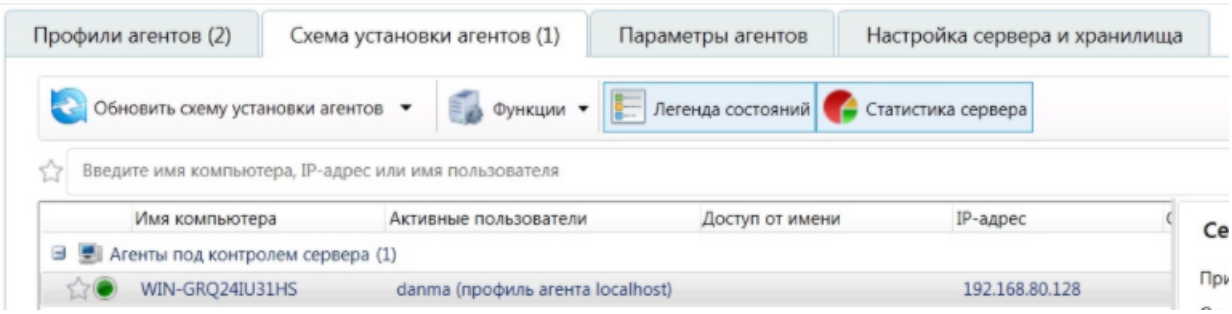
7. **Как, используя параметры профиля настроек, защитить агента от удаления?**

Во вкладке ”Агенты” » ”Параметры агентов” нужно установить флажок напротив пункта ”Включить защиту агентов от удаления”.



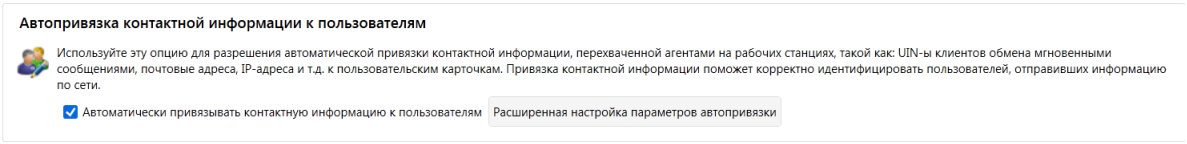
8. **Какой раздел Консоли администратора содержит информацию о работе агентов, установленных на компьютеры в сети организации?**

Раздел ”Агенты” » ”Схема установки агентов”



9. **Каким образом осуществляется привязка перехваченной информации к конкретным пользователям?**

Для отождествления перехваченной информации с конкретным пользователям сети программой используется система карточек пользователей. Каждому пользова локальной сети назначена идентификационная карточка, содержащая персональну и контактную информацию пользователя (имя и фамилия, должность, адреса электронной почты, UIN для ICQ, учетные записи в коммуникационных программа пользовательские имена в социальных сетях и т.д.). Кроме того, карточки пользовате отображают информацию о принадлежности пользователя к той или иной группе. В разделе ”Агенты” -> ”Параметры агентов” можно включить автопривязку перехваченных данных к активным пользователям.



10. **Как добавляется и обновляется информация о пользователях системы, если сеть организации построена на базе Active Directory/рабочей группы?**

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 контролиру 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.