

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.)

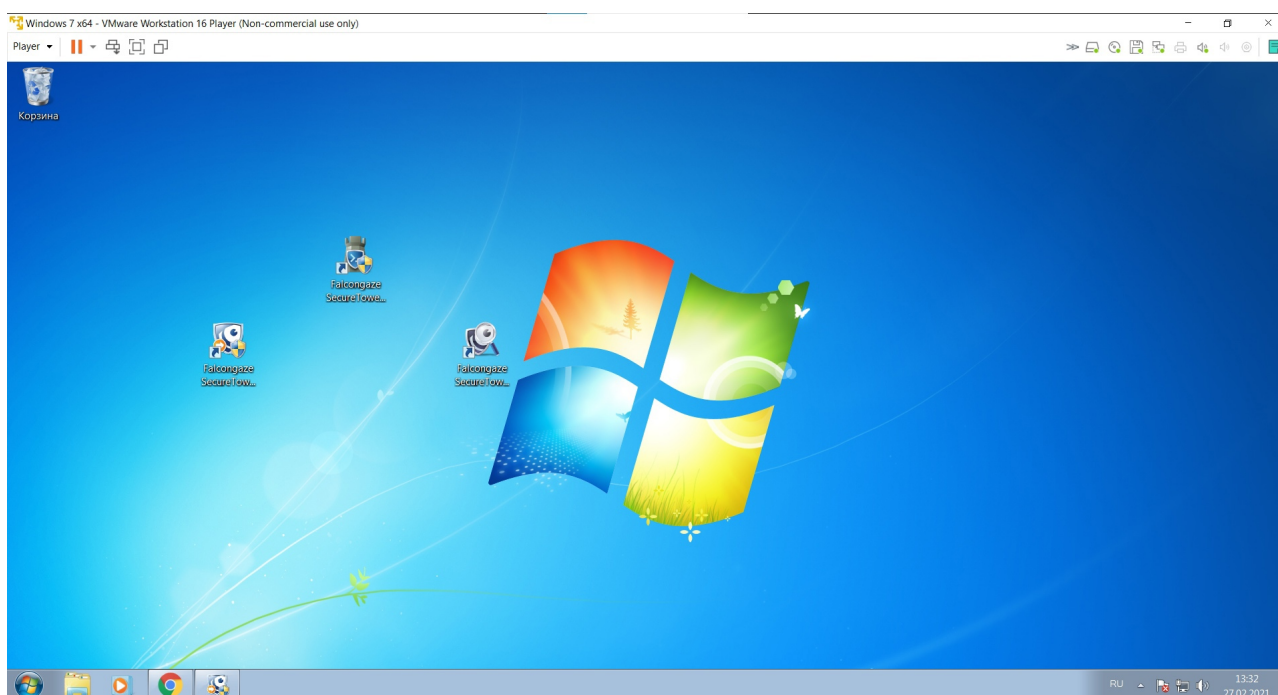
(подпись)

Санкт-Петербург

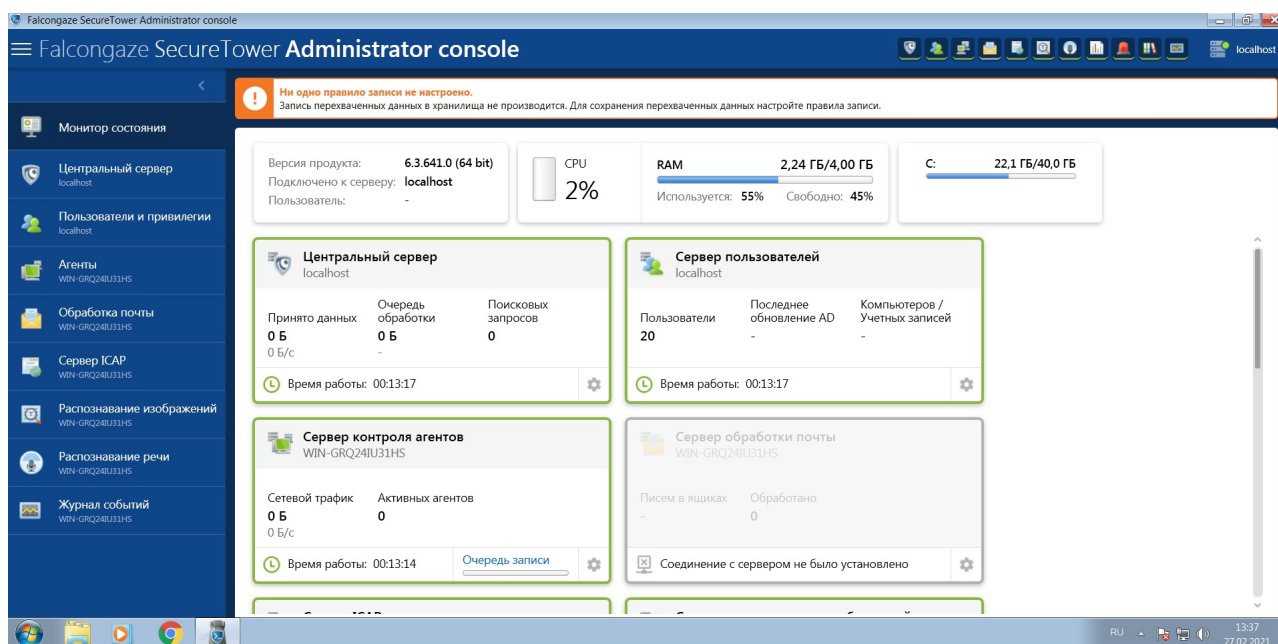
2021

**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.

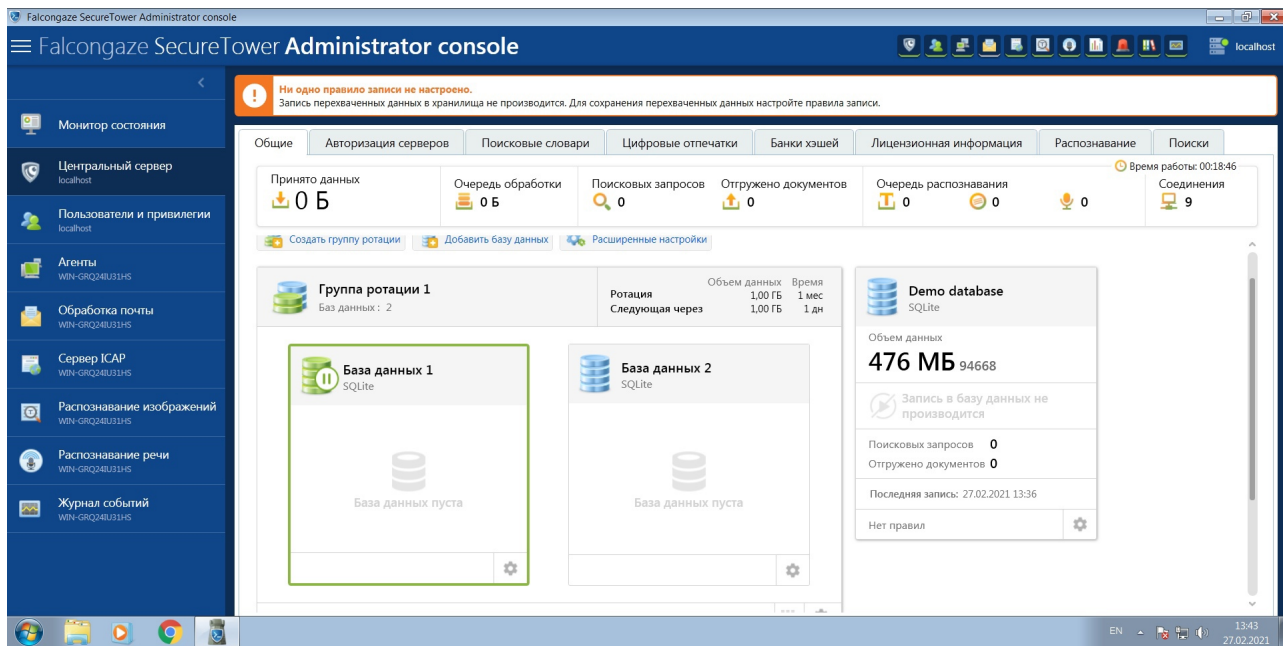
## Пункт 1



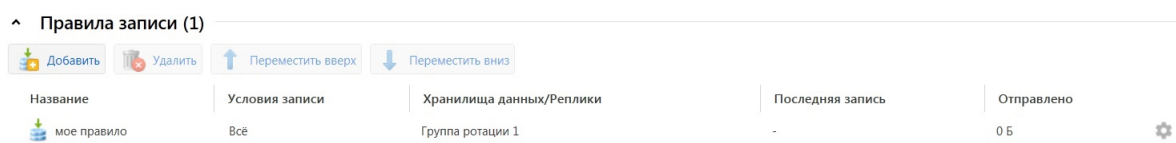
## Пункт 2





























































### Пункт 3



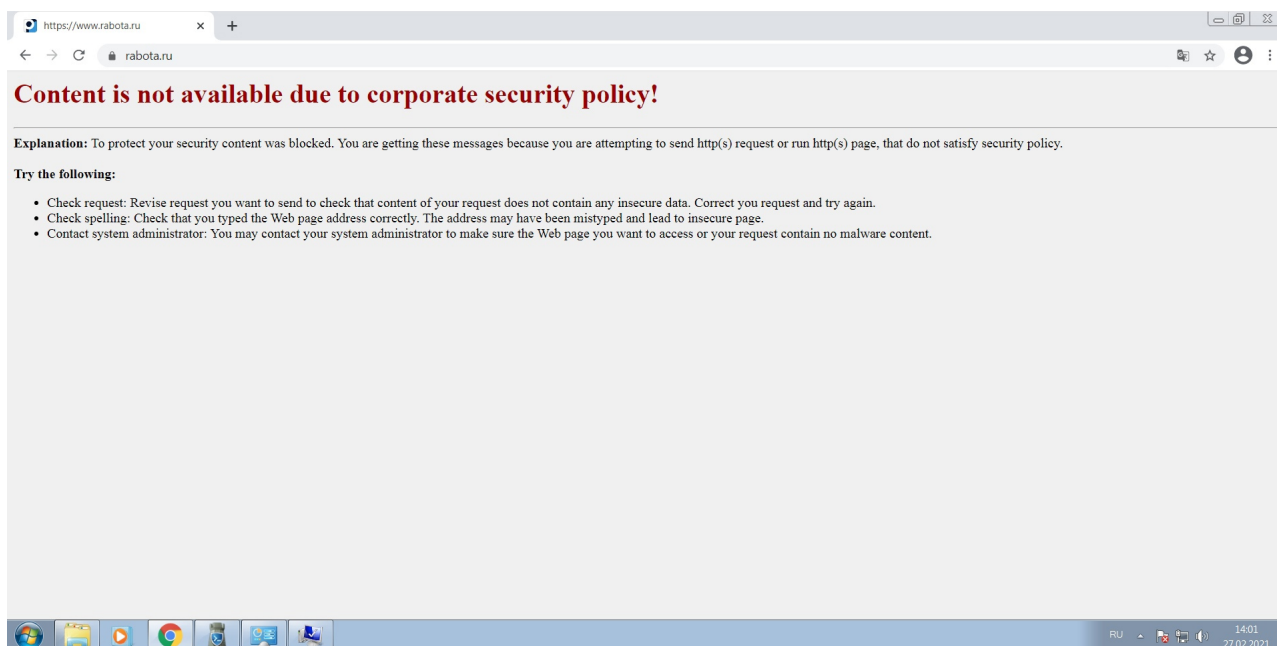
### Пункт 3.1



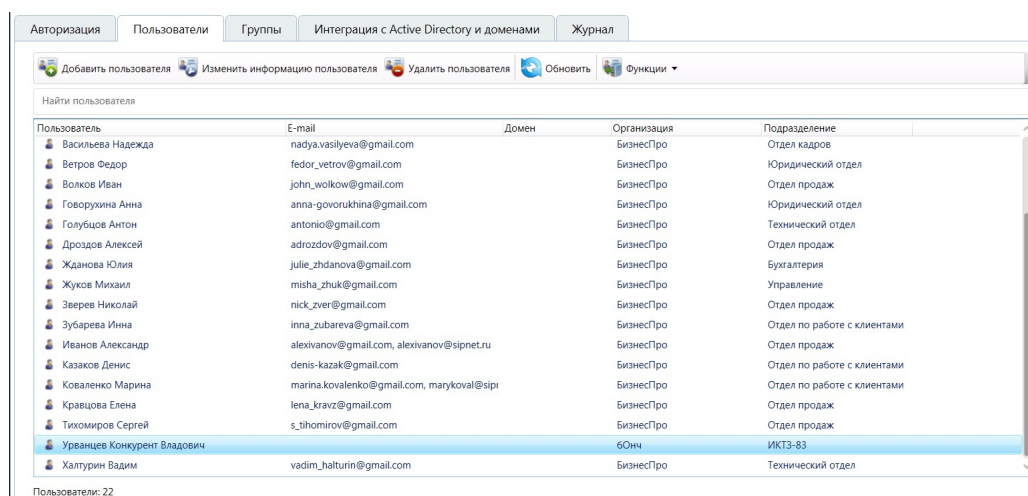
## Пункт 5

Введите имя профиля или названия объектов к которым применяется профиль		
Описание профиля	Применяется к	
 Профиль по умолчанию	По умолчанию ко всем компьютерам и пользователям	                           
 профиль аргента localhost	WIN-GRQ24IU31HS	                           

## Пункт 6



## Пункт 7



## Пункт 8

FalconGaze SecureTower Administrator console

Профили агентов (2) | Схема установки агентов (1) | Параметры агентов | Настройка сервера и хранилища

Обновить схему установки агентов | Функции | Легенда состояний | Статистика сервера

Введите имя компьютера, IP-адрес или имя пользователя

Имя компьютера	Активные пользователи	Доступ от имени	IP-адрес
Агенты под контролем сервера (1)			
WIN-GRQ24IU31HS	danma (профиль агента localhost)		192.168.80.128

Сетевая статистика сервера (начато с 27.02.2021 13:24:30)

Принято: 943 КБ (163 Б / сек)  
Отправлено: 73,5 КБ (41 Б / сек)

Протокол | Получено

- Протокол SMTP
- Протокол POP3
- Протокол HTTP (запросы, файлы) 23,4 КБ (2,77%)
- Протокол OSCAR

Легенда состояния компьютеров

состояние	Количество
Агент работает успешно	1
Компьютер не присылает данные	0
Компьютер отклонён лицензией	0
Агент устанавливается/удаляется	0
Компьютер с предупреждениями	0

Общие | Статистика компьютера WIN-GRQ24IU31HS (1) | Устройства компьютера (2)

Лог действий с компьютером | Статистика индексирования

Статистика проиндексированных файлов

Последняя проверка списка файлов: -

Состояние процесса хеширования: Разрешено

Прогресс хеширования: 3.30% 105 / 3 186

Применить изменения

RU 14:09 27.02.2021

## Пункт 8.1

FalconGaze SecureTower Administrator console

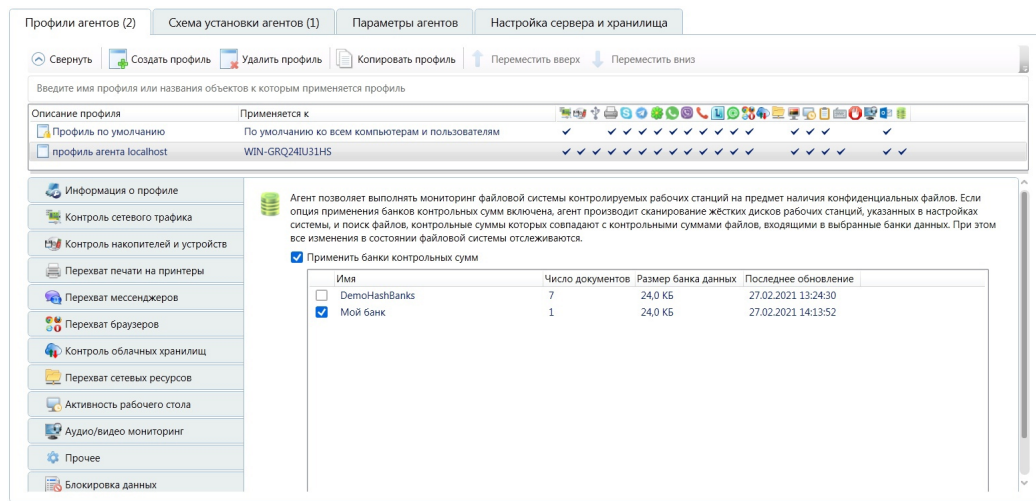
Общие | Авторизация серверов | Поисковые словари | Цифровые отпечатки | Банки хэшей | Лицензионная информация | Распознавание | Поиски

Создать банк хэшей | Удалить

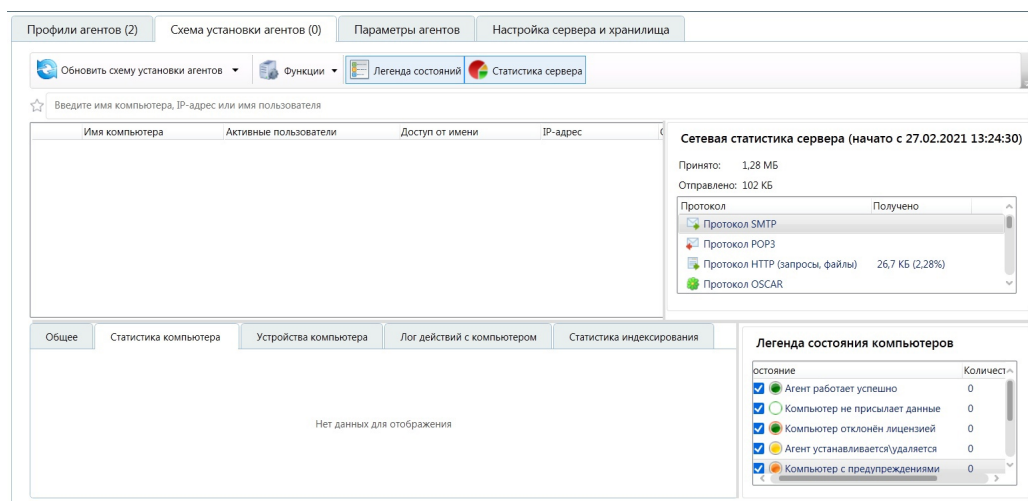
Название	Размер	Количество файлов	Дата обновления
DemoHashBanks	24,0 КБ	7	27.02.2021 13:24:30
Мой банк	24,0 КБ	1	27.02.2021 14:13:52

RU 14:14 27.02.2021

## Пункт 8.2



## Пункт 9



## Ответы на контрольные вопросы

### 1. Для чего используется Консоль администратора?

Консоль администратора используется для настройки и управления компонентами FalcoGaze.

### 2. В каких случаях при подключении к серверу указывается локальный компьютер?

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 зашифрованный (по протоколам, использующим SSL-шифрование: HTTPS, FTPS, SMTPS, POP3S, IMAP4S, SIP, протоколы мессенджеров Skype, Telegram, Viber, WhatsApp, ICQ10, Google Hangout 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 и многое другое. 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.

### **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. Суще-



ствуется 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.

**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".

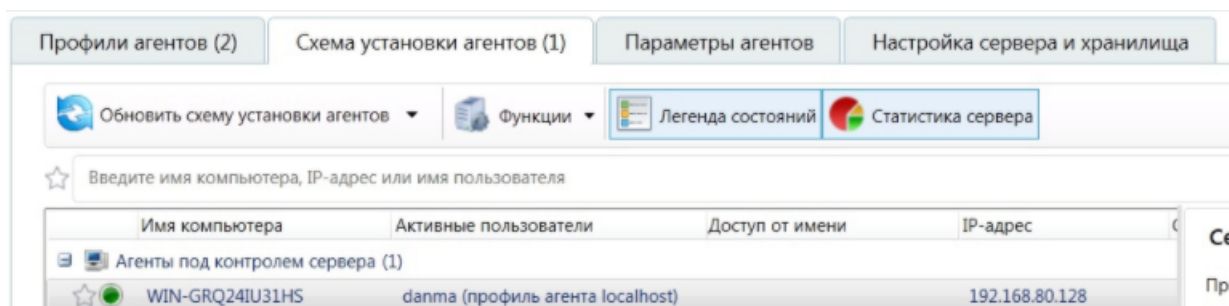
 **Защита агента**  
На этой странице можно установить режим для защиты агента на удалённом компьютере. Процесс агента может быть скрыт таким образом, что пользователь не сможет увидеть процесс агента в диспетчере задач, его файлы и папку на диске, а также службу агента в списке служб компьютера. Другая возможность для защиты процесса агента – защита от завершения процесса пользователем. Если пользователь попытается завершить процесс агента, операционная система сначала предупредит его, а потом и перезагрузится, если пользователь решит завершать процесс.

Режим защиты: ☐ Скрыть агента на компьютере пользователя  
☐ Защитить процесс агента, файлы агента и данные в реестре на компьютере пользователя

 Включение скрытия агентов на компьютере пользователя может привести к предупреждениям или ошибкам со стороны антивирусов или другого программного обеспечения предназначенного для защиты рабочих станций пользователей

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

Раздел "Агенты" » "Схема установки агентов"

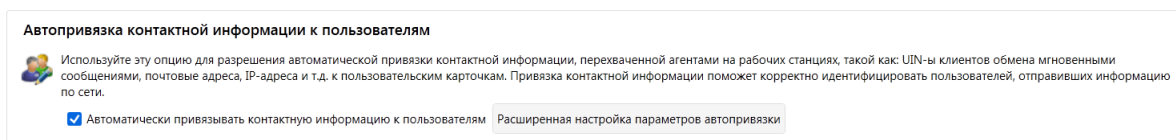


Имя компьютера	Активные пользователи	Доступ от имени	IP-адрес
<b>Агенты под контролем сервера (1)</b>			
WIN-GRQ24IU31HS	danma (профиль агента localhost)		192.168.80.128



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

Для отождествления перехваченной информации с конкретным 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. 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 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.