

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 №2**  
**МОНИТОРИНГ СЕТЕВОЙ И КОМПЬЮТЕРНОЙ АКТИВНОСТИ**  
**ПОЛЬЗОВАТЕЛЕЙ. Ч.2**

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)

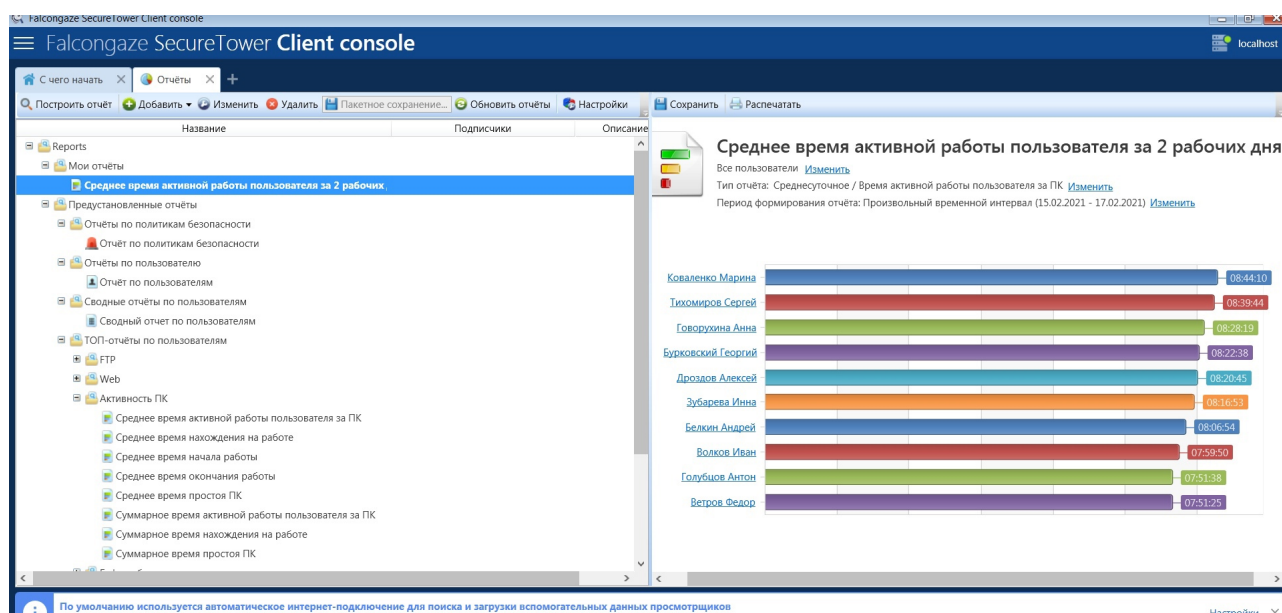
Санкт-Петербург

2021

## Цель лабораторной работы:

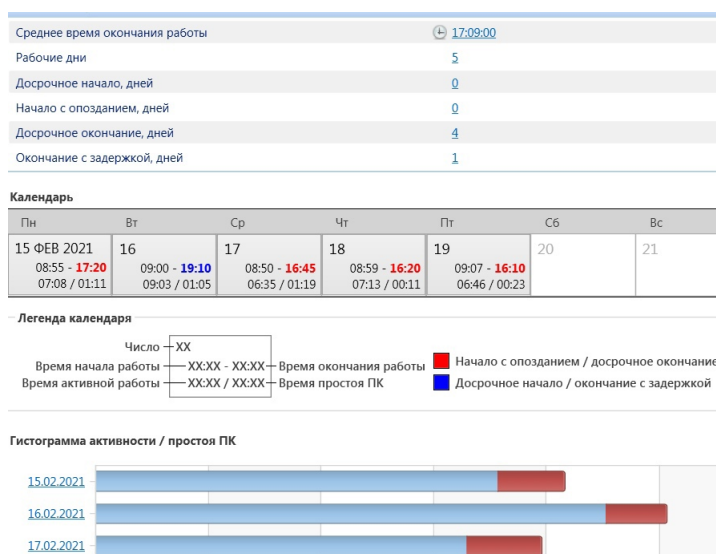
Научиться работе с Клиентской консолью Falcongaze SecureTower для проведения расследований и предупреждения инцидентов информационной безопасности организации, освоить инструмент создания статистических отчетов о компьютерной и сетевой активности пользователей. Научиться использовать инструменты системы для наблюдения за активностью пользователей в режиме реального времени и для мониторинга файловых систем.

### Пункт 2.4 - Дублирование отчета.



Дубликат "Среднее время активной работы пользователя за ПК"

### Пункт 2.8 - раздел отчета Активность пользователя за компьютером.



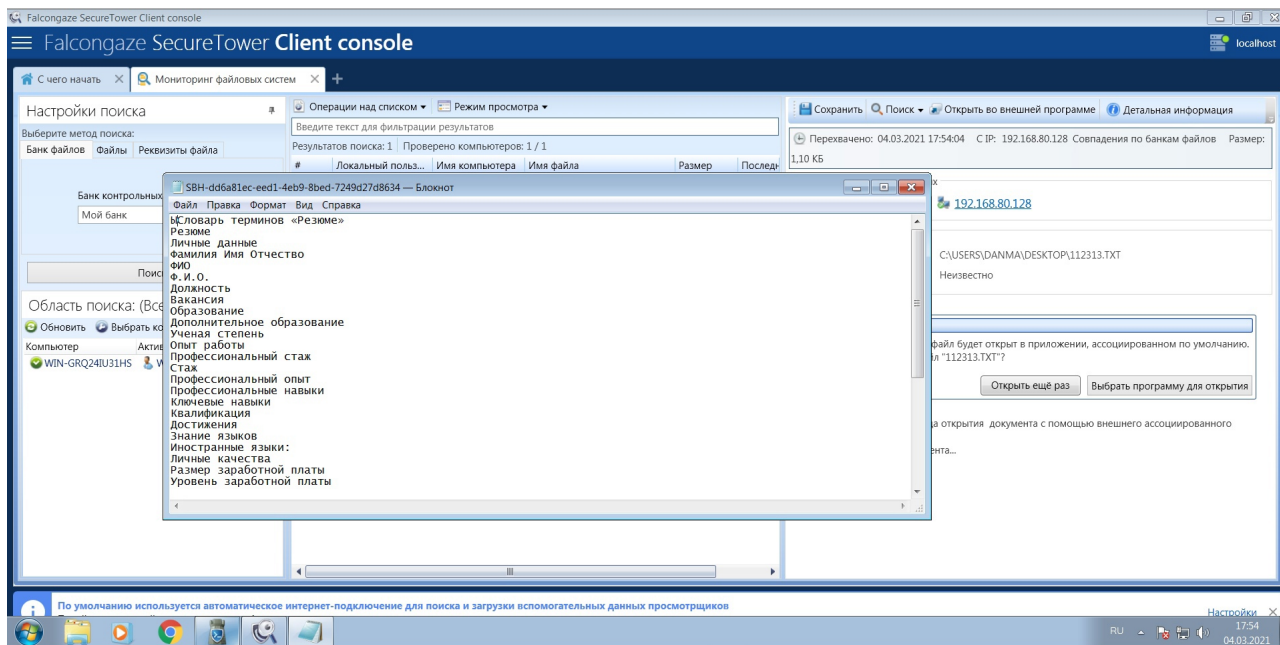
Статистика работы пользователя за ПК

## Пункт 2.9 - Сохранение отчета по пользователю Елена Кравцова.

112313	27.02.2021 14:12	Текстовый докум...	2 КБ
ResultsList	04.03.2021 17:11	Лист Microsoft Off...	55 КБ
Skype conversation - lena_kravz_2021.02.15_10.13.52	04.03.2021 17:29	Rich Text Format	414 КБ
Кравцова Елена (За всё время)	04.03.2021 17:52	Chrome HTML Do...	342 КБ

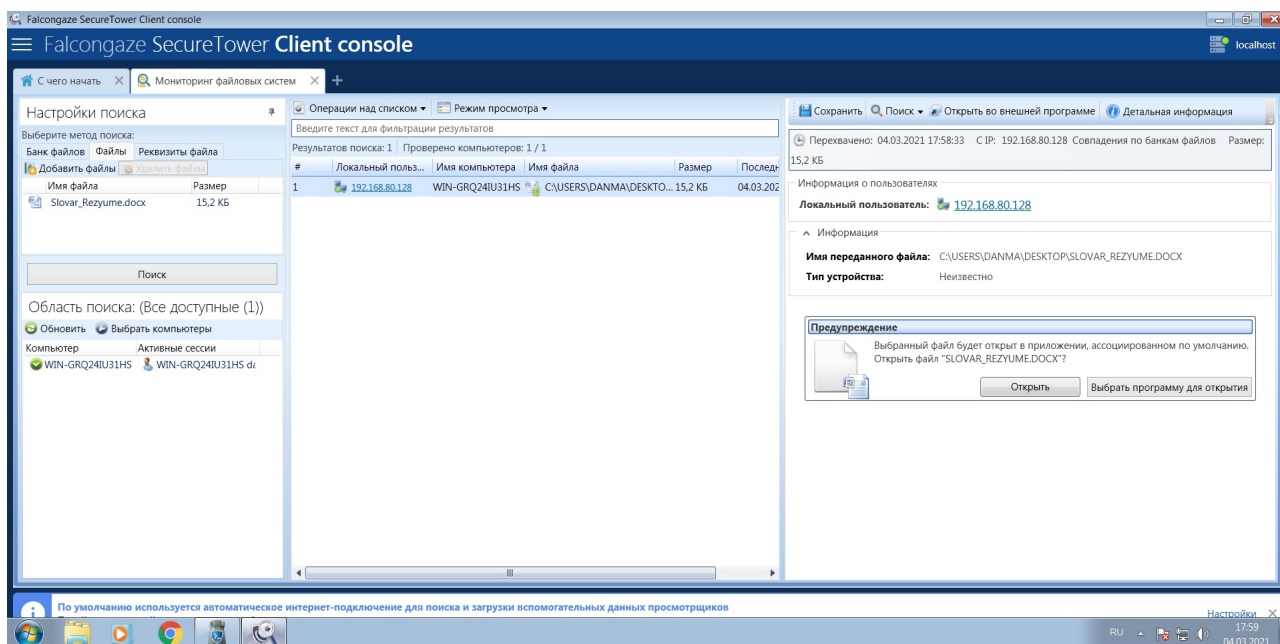
Отчет по пользователю сохранен

## Пункт 3.2 - Поиск совпадений с файлами ранее созданного банка хэшей.



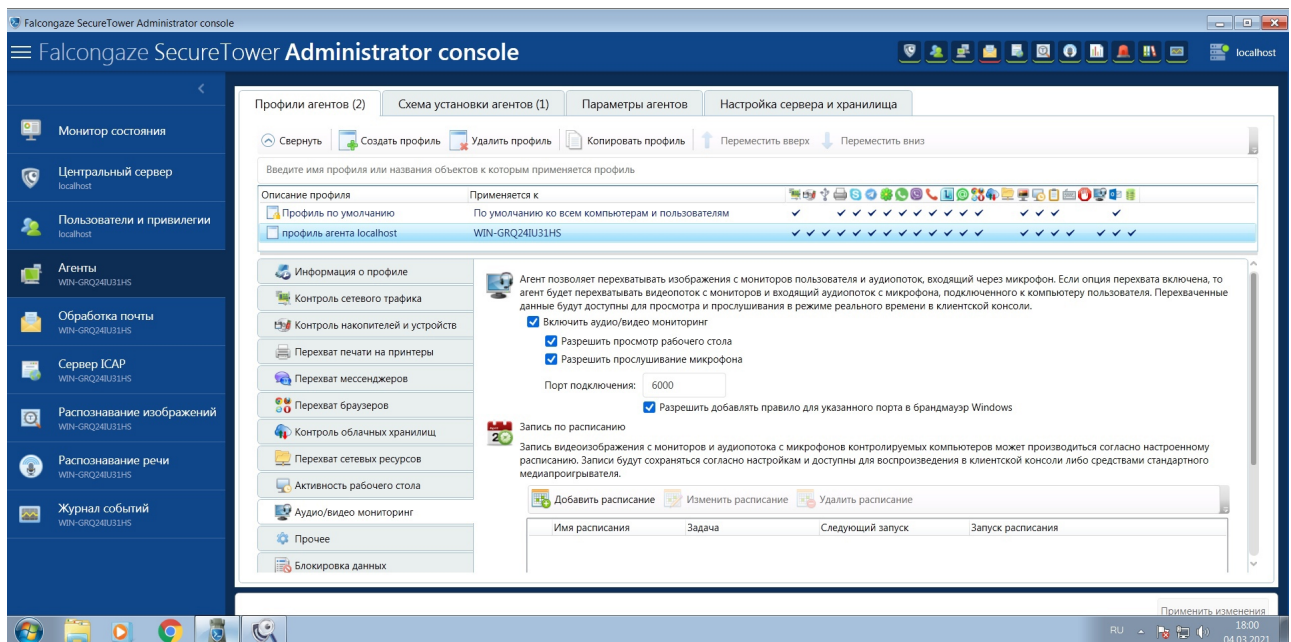
Найденный файл соответствует файлу-источнику, добавленному в банк хэшей при настройке индексирования ранее.

## Пункт 3.4 - Поиск файла в файловой системе ПК.



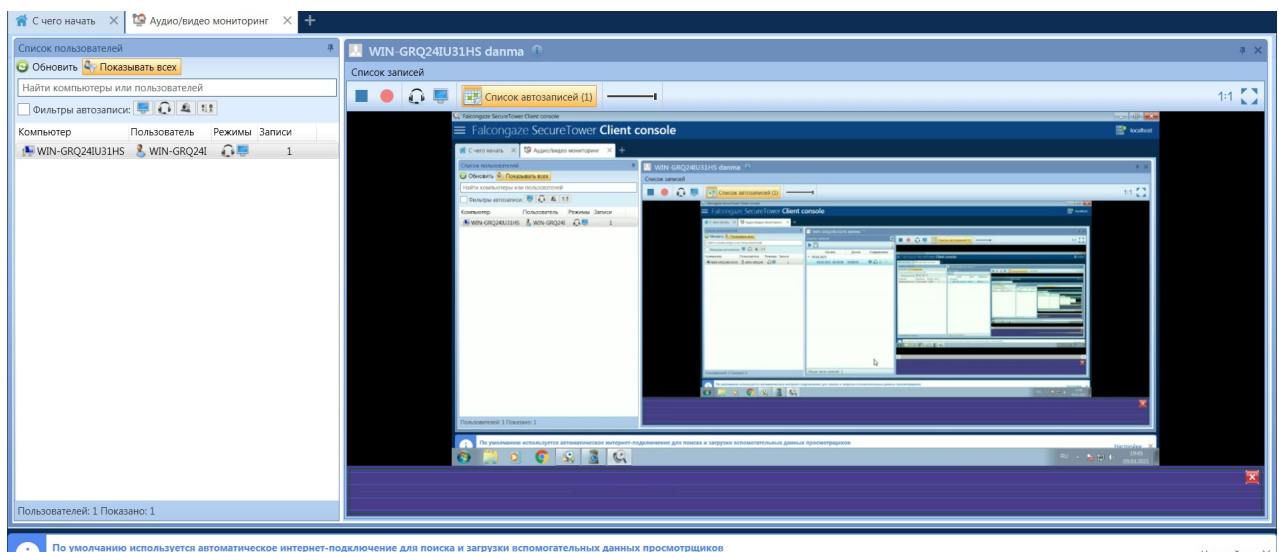
В ходе мониторинга найден файл Словарь резюме.docx, расположенный на рабочем столе в папке Student.

## Пункт 4.1 - Активация видео-аудио мониторинга.



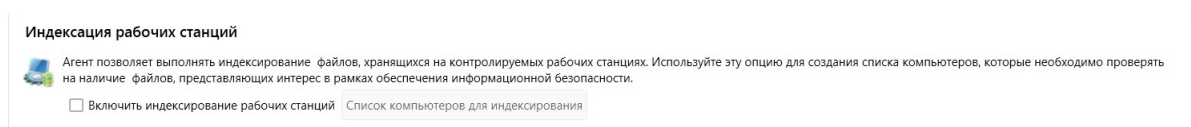
Мониторинг активирован.

## Пункт 4.8 - Изучение возможностей встроенного проигрывателя.



Воспроизводимое видео соответствуют действиям пользователя на локальном компьютере.

## Пункт 4.9 - Отключение видео-аудио мониторинга, а также индексации.



Индексация отключена

## **Выводы:**

При выполнении данной работы мы научились отслеживать действия пользователей за компьютером, например, время работы, посещаемые сайты. Также мы получили данные о работе с файловой системой и осуществили аудио/видео мониторинг рабочего ПК.

## **Ответы на контрольные вопросы.**

- 1. Какой инструмент Консоли пользователя позволяет провести комплексный (и качественный и количественный) анализ статистики по выбранному направлению активности пользователя в сети?**

Инструмент "Отчёты".

- 2. Перечислите виды активности, по которым доступно построение статистических отчетов для отдельного пользователя сети организации.**

Статистика перехвата данных, активность пользователя за компьютером, активность приложений, браузер-активность, статистика политик обеспечения безопасности.

- 3. Как получить информацию о соблюдении режима рабочего дня пользователя?**

"Отчёты" -> "Отчет по пользователю" -> "Активность пользователя за компьютером".

- 4. Для чего выполняется индексирование файловых систем компьютеров?**

Для возможности поиска по файлам.

- 5. Возможно ли выполнить поиск произвольного файла в файловой системе контролируемого компьютера? Например, файла, выбранного пользователем, или с указанным именем или расширением.**

Да, возможно.

- 6. Возможно ли записать видео рабочего стола пользователя вручную?**

Да, возможно.

**7. Позволяет ли система производить автоматическую запись результатов мониторинга компьютеров пользователей?**

Да, позволяет.