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)*

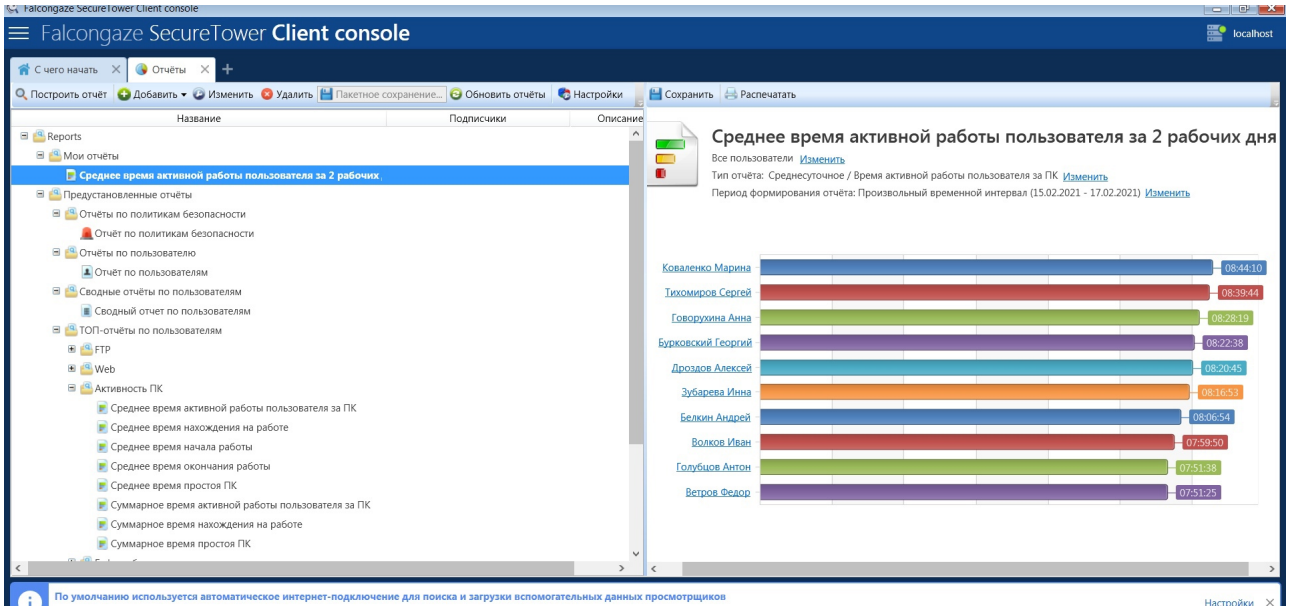
Санкт-Петербург

2021

Цель лабораторной работы:

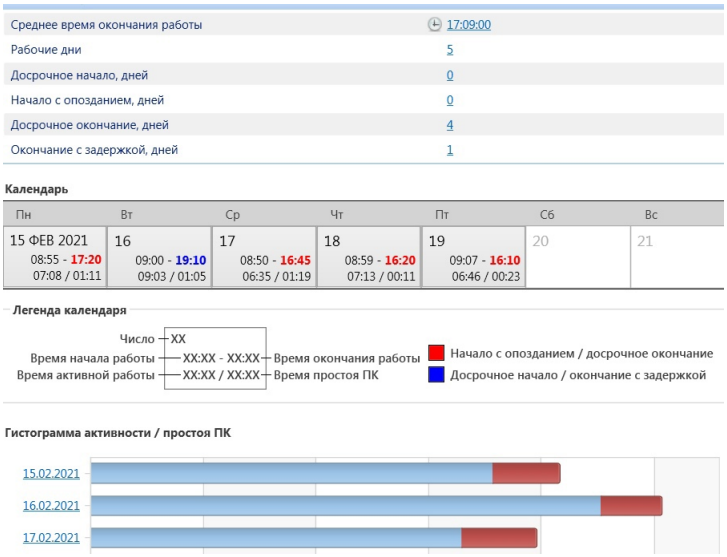
Научиться работе с Клиентской консолью Falcongaze SecureTower для проведения расследований и предупреждения инцидентов информационной безопасности организац освоить инструмент создания статистических отчетов о компьютерной и сетевой активности пользователей. Научиться использовать инструменты системы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

Пункт 2.4 - Дублирование отчета.



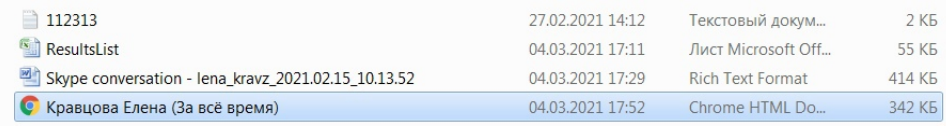
Дубликат ”Среднее время активной работы пользователя за ПК”

Пункт 2.8 - раздел отчета Активность пользователя за компьютером.



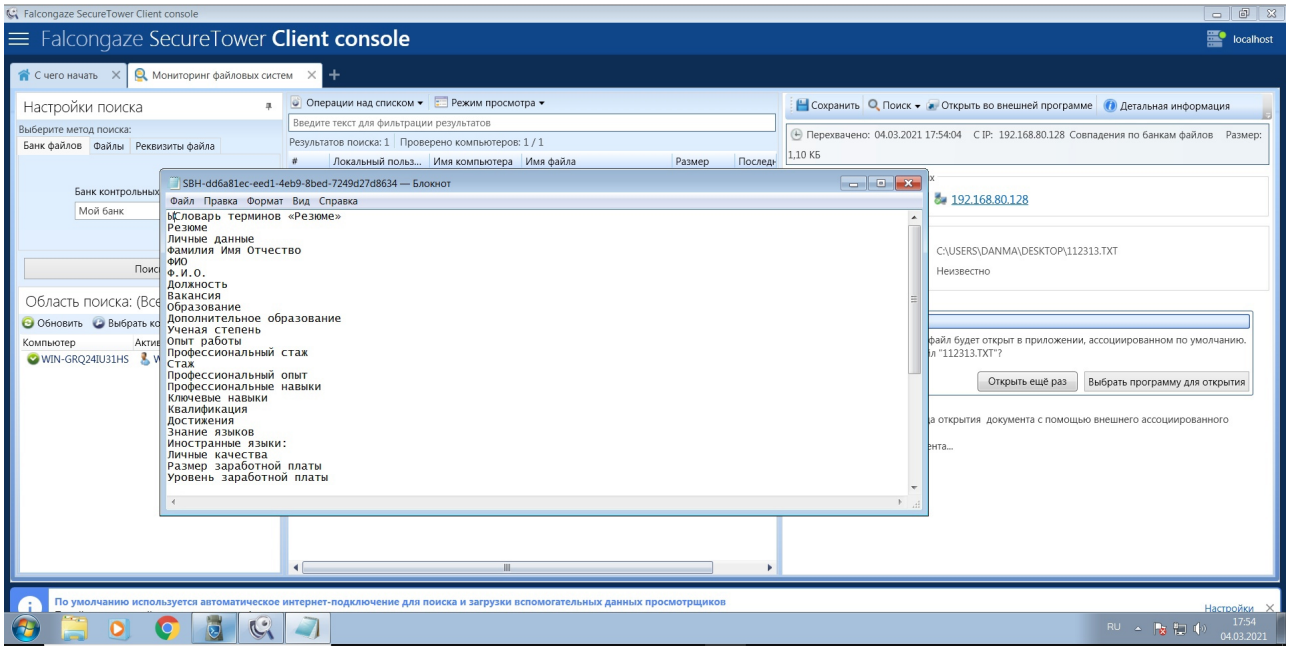
”Активность пользователя за компьютером.”

Пункт 2.9 - Сохранение отчета по пользователю Елана Кравцова.



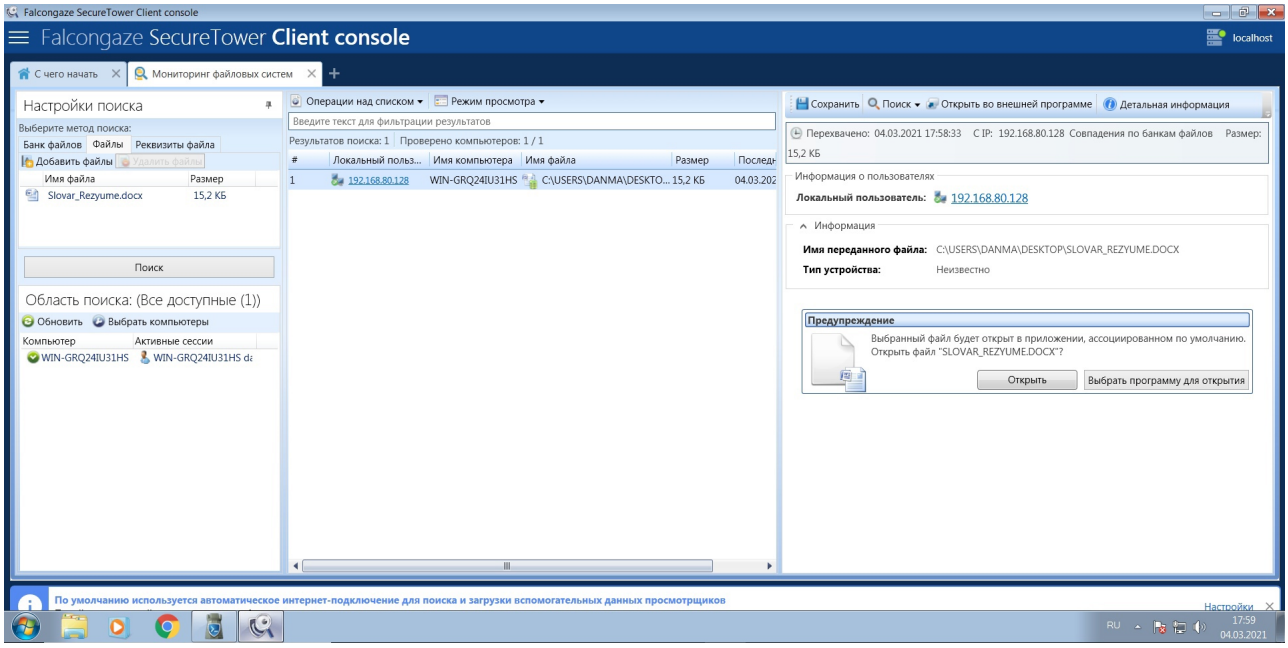
Отчет по пользователю сохранен

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



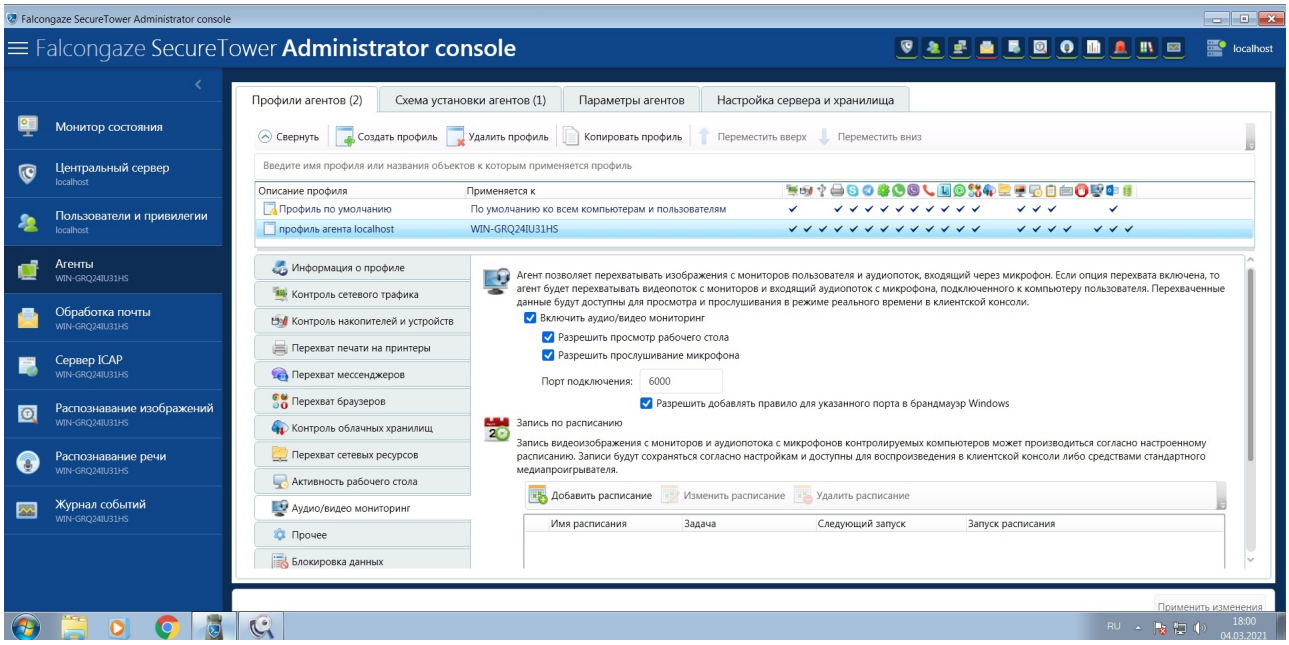
Найденный файл соответствует файлу-источнику, добавленному в банк хэшей при настройке индексирования ранее.

Пункт 3.4 - Поиск файла в файловой системе ПК.



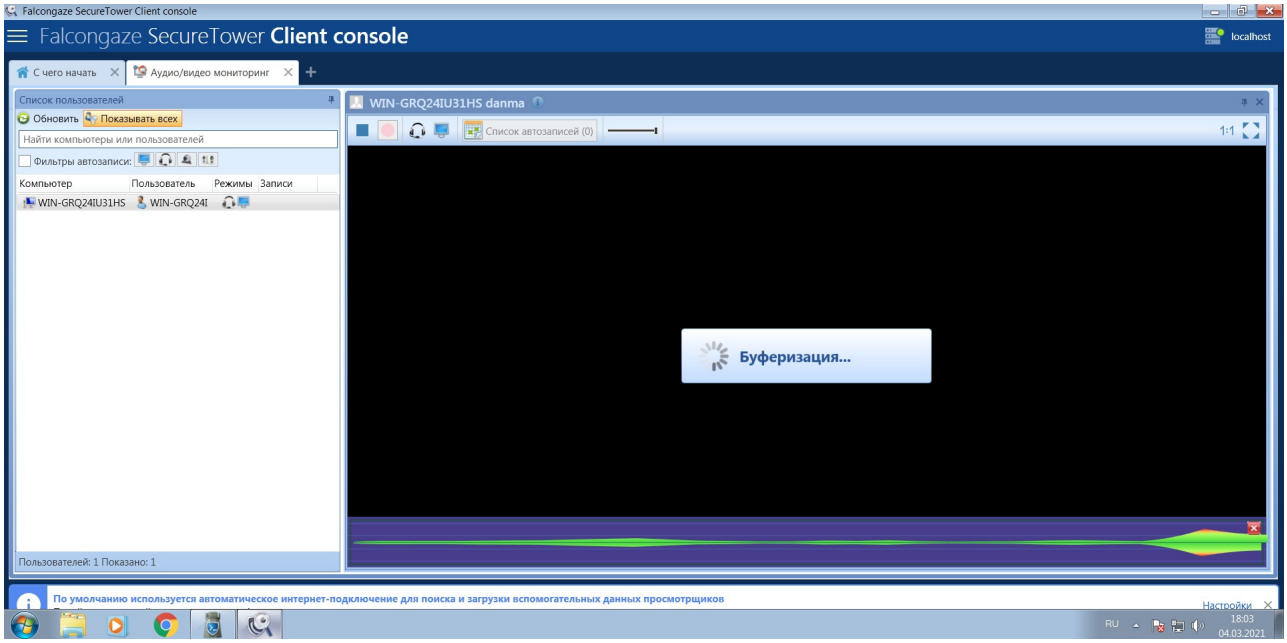
В ходе мониторинга найден файл Словарь резюме.docx, расположенный на рабочем столе в папке Student.

Пункт 4.1 - Активация видео-аудио мониторинга.



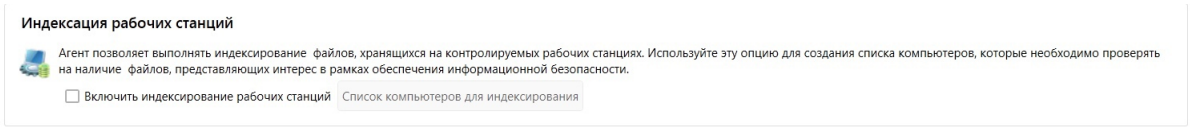
Мониторинг активирован.

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

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 статистичес отчетов для отдельного пользователя сети организации.**

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

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

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

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

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