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 №3

Назначение политик безопасности в Центре обеспечения безопасности Клиентской консоли Falcongaze SecureTower

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)*

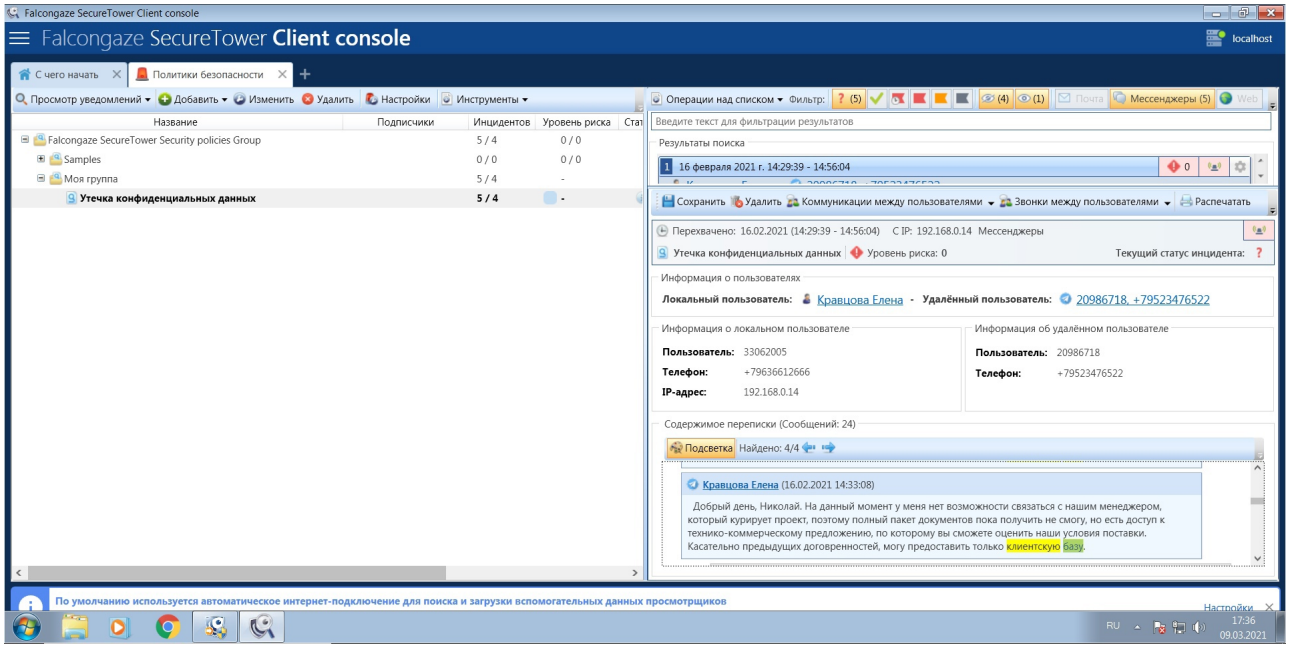
Санкт-Петербург

2021

Цель лабораторной работы:

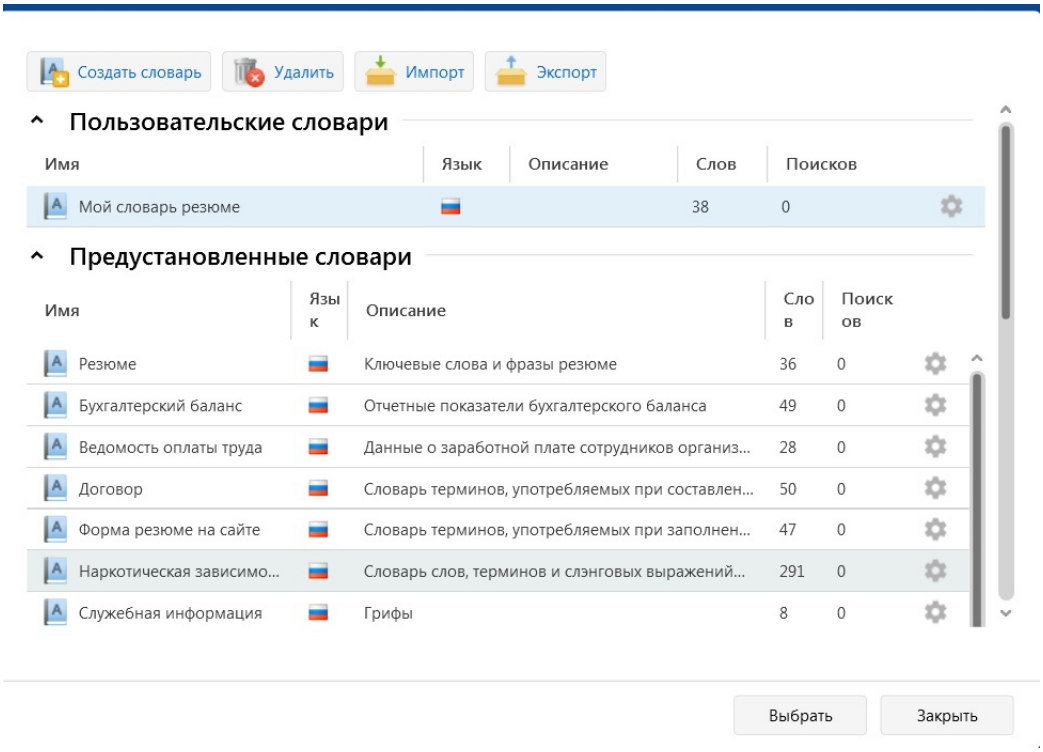
Научиться управлять работой Центра обеспечения безопасности Клиентской консоли Falcongaze SecureTower, получить опыт создания правил безопасности различных типов, освоить работу с уведомлениями об инцидентах безопасности.

Пункт 2.9 - Добавление правил



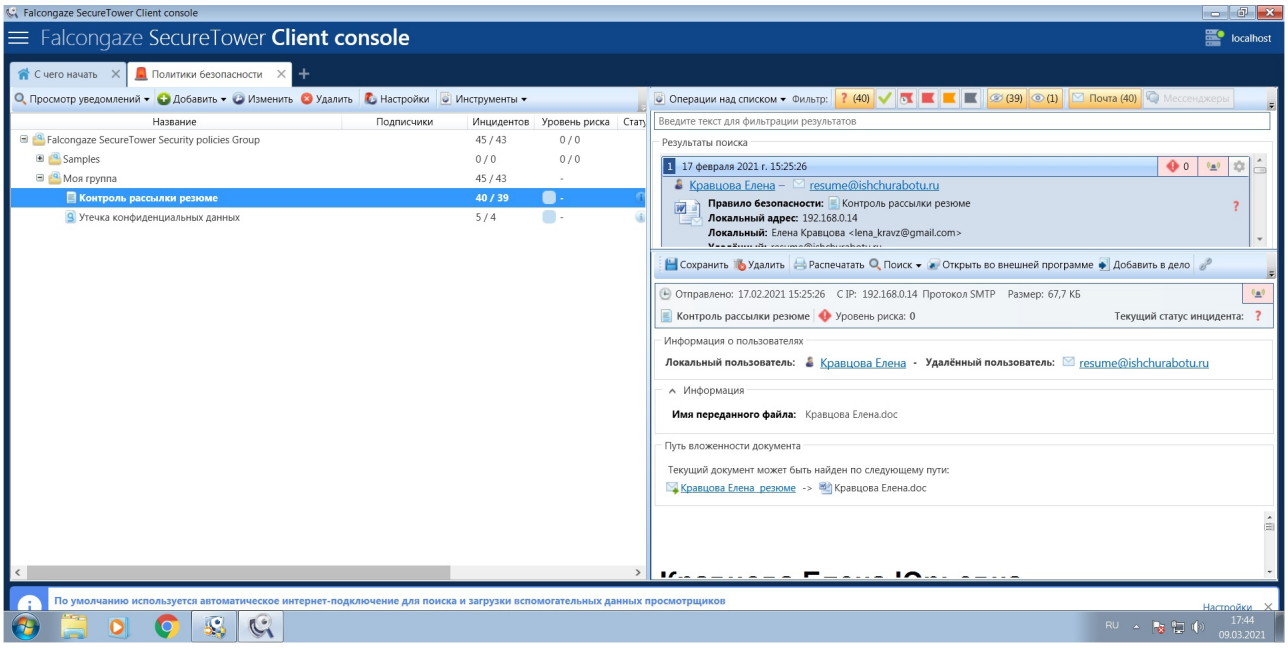
Правило отображается в папке Мои правила.

Пункт 3.4.5 - Создание словаря



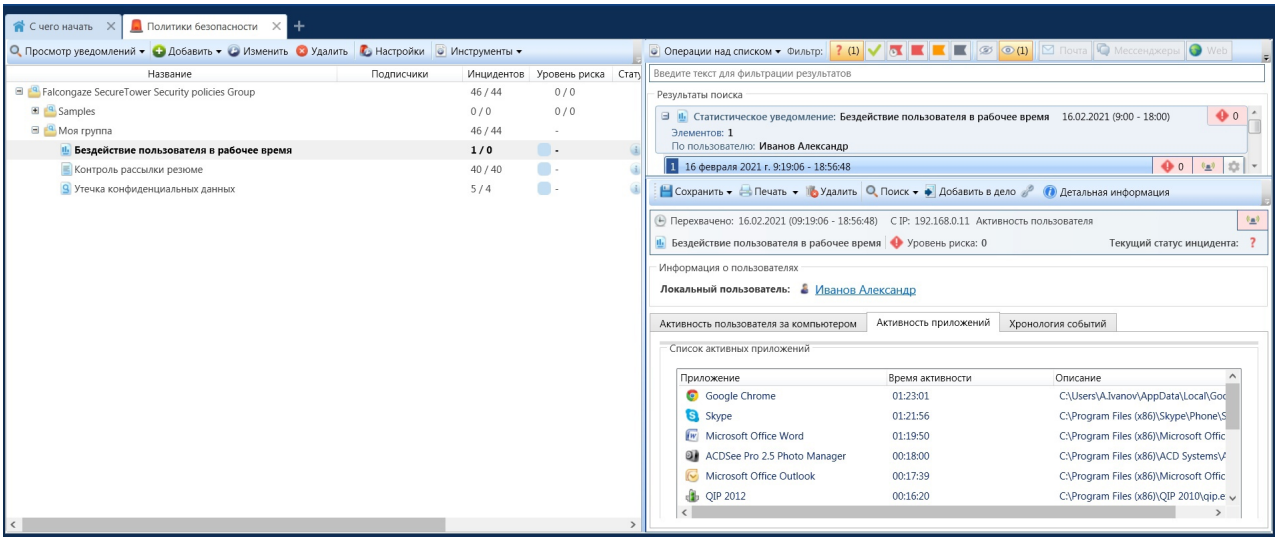
Имя словаря отображается в поле списка Словарь.

Пункт 3.9 - Применение правила для вывода результатов



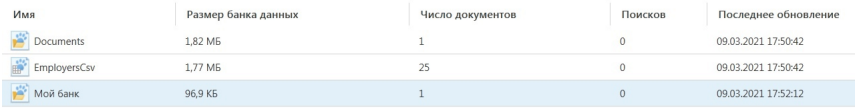
В результате обработки правила обнаружено 20 инцидентов безопасности.

Пункт 4.6.2 - Применение правила для вывода результатов



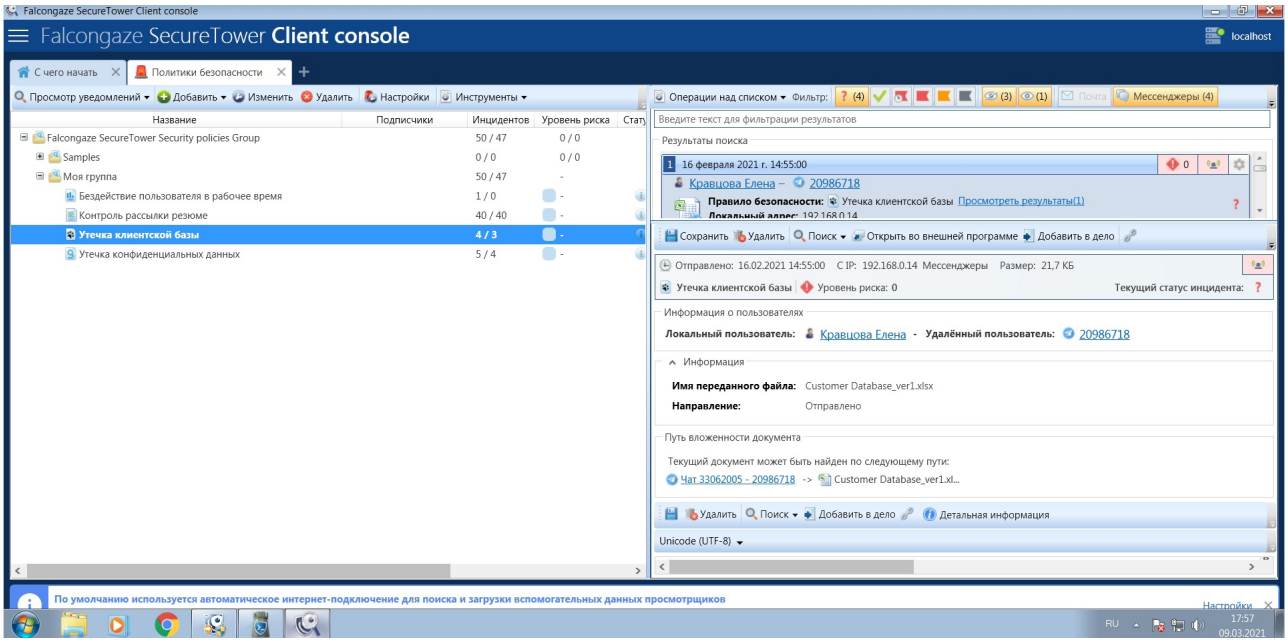
В результате обработки правила обнаружено 1 инцидента безопасности.

Пункт 5.2.3 - Добавление банка цифровых отпечатков



Имя банка отображается в списке цифровых отпечатков.

Пункт 5.9 - Применение правила для вывода результатов



В результате обработки правила обнаружен 1 инцидент безопасности.

Выводы:

В отличие от лабораторных работ 2.1 и 2.2, нами была произведена автоматизация контроля утечек информации и оповещение об этих инцидентах посредством SMTP. Автоматизация может быть произведена по 4 фильтрам: ключевые слова, словари, цифровые отпечатки, статистические правила.

Ответы на контрольные вопросы.

1. **Какие способы используются в системе SecureTower для оповещения о сетевых событиях, нарушающих политику безопасности?**

   Только SMTP-сервер.

2. **Какие виды правил безопасности доступны в Центре обеспечения безопасност**

   Обычное, контроль по словарю, статистическое, цифровые отпечатки

3. **Для каких источников данных доступна возможность создания цифровых отпечатков?**

   Для банков данных.

4. **В чем основные отличия контроля по тексту, по словарю от контроля за событиями безопасности по цифровым отпечаткам?**

   Поиск по цифровым отпечаткам ищет документы, по тексту ищет слова, по словарю - тематический поиск.