Лабораторный практикум

по назначению политик безопасности в Центре обеспечения безопасности Клиентской консоли **Falcongaze SecureTower**

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

**Оборудование и настройки:** ПК, включенный в рабочую группу компьютеров (локальный компьютер с установленным комплексом **Falcongaze** **SecureTower**).

Содержание практикума

[**Общие сведения** 3](#_Toc493754548)

[**Порядок выполнения работы** 4](#_Toc493754549)

[**1.** **\* Настройка отправки уведомлений Центра обеспечения безопасности** 4](#_Toc493754550)

[**2.** **Создание Обычного поискового правила безопасности** 5](#_Toc493754551)

[**3.** **Создание правила Контроль по словарю** 8](#_Toc493754552)

[**4.** **Создание статистического правила** 10](#_Toc493754553)

[**5.** **Создание правила контроля по цифровым отпечаткам** 12](#_Toc493754554)

[**Контрольные вопросы** 14](#_Toc493754555)

**Рекомендации по выполнению работы**

Изучите теоретическую часть лабораторного практикума, изложенную в разделе **Общие сведения** перед выполнением практических заданий.

Выполнять задания лабораторного практикума следует строго в соответствии пунктами, как указано в разделе **Порядок выполнения работы**. Шаги и задания, помеченные «\*», выполняются по указанию преподавателя.

После каждого шага или при возникновении вопросов о выполнении задания сравните результат на экране с соответствующим рисунком. Для быстрого получения помощи в работе с программой а также получения дополнительной информации используйте команды меню *Помощь* либо обратитесь к преподавателю.

Чтобы проверить, насколько хорошо Вы усвоили материал, в конце работы ответьте на контрольные вопросы.

**Общие сведения**

Для создания правил политики безопасности и получения уведомлений о срабатывании правил в режиме реального времени необходимо настроить работу Центра обеспечения безопасности.

Система позволяет создавать четыре вида правил безопасности на основе различных методов обработки и поиска среди перехваченных данных с различными параметрами поиска:

* Обычное
* Контроль по словарю
* Статистическое
* Цифровые отпечатки.

Система позволяет искать данные с учетом морфологии слова, проводить нечеткий поиск, учитывать порядок указанных слов, если введено несколько, и производить поиск при использовании транслитерации.

**SecureTower** позволяет контролировать количественные характеристики определенных сетевых событий и уведомлять о превышении установленных ограничений за указанный промежуток времени по отдельному пользователю и сети в целом.

Помимо технологии полнотекстового поиска с учетом морфологии система поддерживает технологию **поиска по цифровым отпечаткам и словарям**.

Поисковые словари содержат слова и выражения, которые относятся к одной тематической области. При использовании словарей система позволяет выявлять в перехваченных данных документы определенной тематики. В системе содержится более 90 предустановленных словарей на русском, английском и испанском языках. Вы можете воспользоваться одним из них либо *Менеджером словарей* для создания пользовательского словаря.

Технология цифровых отпечатков позволяет при поиске сопоставлять каждый перехваченный документ с банком цифровых отпечатков и находить документы, имеющие определенное количество совпадений. Процент соответствия перехваченного документа документу в банке цифровых отпечатков настраивается и является основным критерием оценки уровня конфиденциальности передаваемого документа. Используя технологию, вы можете выполнить поиск документов, фрагменты которых или документ целиком содержатся в перехваченных данных.

Поиск по цифровым отпечаткам доступен непосредственно во время проведения комбинированного поиска, так и в полученных результатах по любому поисковому запросу.

Вы также можете использовать условия поиска по цифровым отпечаткам и словарям при создании правил безопасности в Центре безопасности.

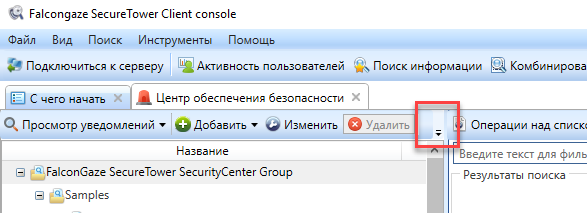
С помощью соответствующих настроек правил возможно осуществлять контроль за активностью процессов, событиями пересылки документов с определенным статусом, использованием внешних устройств, Интернет - активностью и многими другими сетевыми событиями.

**Порядок выполнения работы**

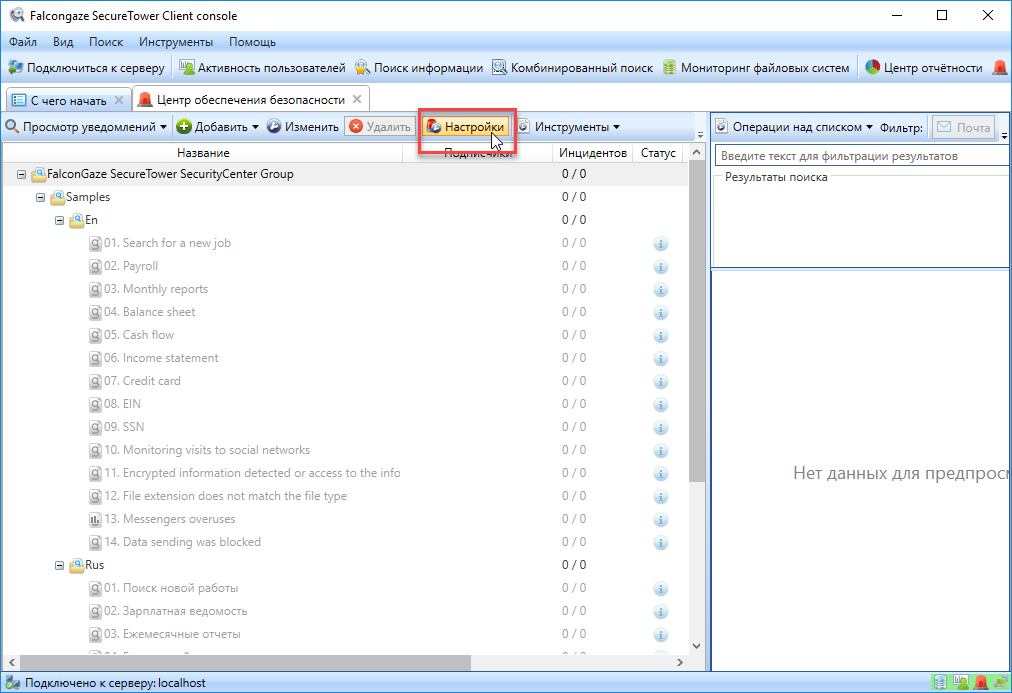
1. **\* Настройка отправки уведомлений Центра обеспечения безопасности**

Получите у преподавателя атрибуты SMTP-сервера и e-mail адресов, для настройки отправки и получения уведомлений о событиях безопасности.

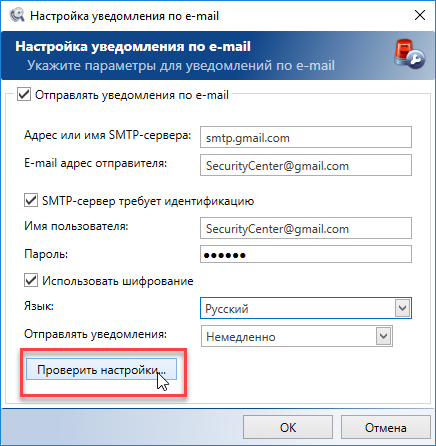
Внимание! Если окно Консоли пользователя находится в свернутом состоянии, то некоторые пункты меню могут быть скрыты. Для доступа к скрытым пунктам нажмите кнопку, расположенную в панелях меню окон компонентов.



* 1. Запустите Консоль пользователя.
  2. На стартовой странице главного окна консоли кликните по панели компонента **Центр обеспечения безопасности**.
  3. Нажмите кнопку **Настройки**на панели меню окна Центра безопасности*.*



* 1. Отметьте опцию **Отправлять уведомления по e-mail**и опцию **SMTP- требует идентификацию***.*
  2. Заполните поля формы настройки значениями атрибутов SMTP-сервера и e-mail адресов, полученных у преподавателя.
  3. Отметьте опцию **Использовать шифрование**(если того требует SMTP-сервер).



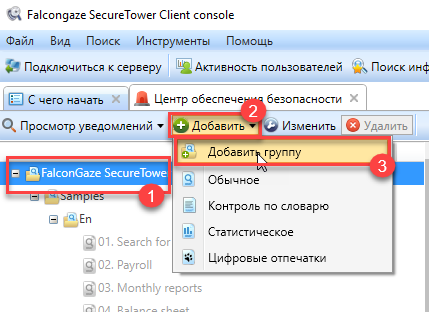
* 1. Нажмите кнопку **Проверить настройки** и введите E-mail адрес получателя уведомлений.

**Результат**: Тестовое письмо получено и доступно в почтовом ящике, имя которого было указано как E-mail адрес получателя.

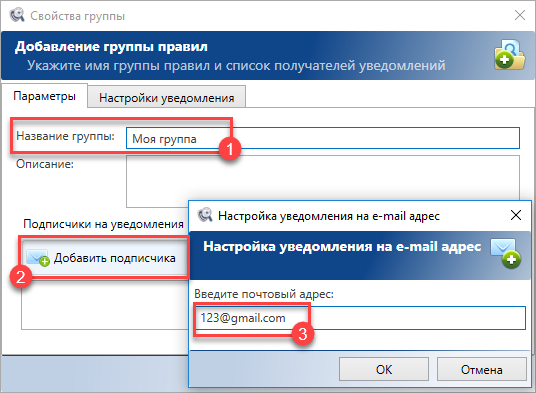
1. **Создание Обычного поискового правила безопасности**

**Алгоритм действий**

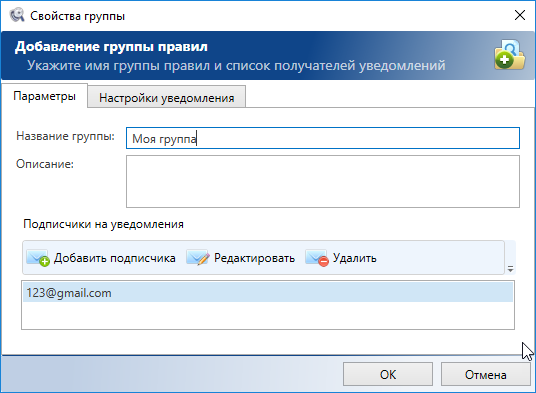
* 1. Перейдите в главное окно Центра обеспечения безопасности Консоли пользователя.
  2. Выберите корневую группу каталога правил **Falcongaze SecureTower SecurityСenter Group**, нажмите кнопку **Добавить** на панели меню и выберите пункт **Добавить группу***.*



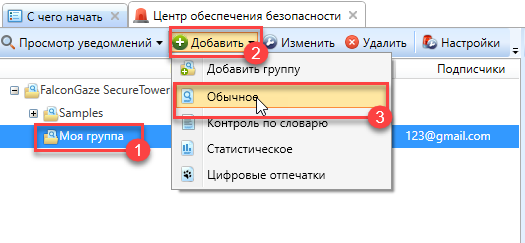
* 1. Введите *Моя группа* в поле **Название группы**. Введите описание группы в соответствующем поле по желанию.
  2. \* Нажмите кнопку **Добавить подписчика**и введите E-mail адрес получателя уведомлений о сработках правил безопасности, которые будут созданы далее в этой группе.



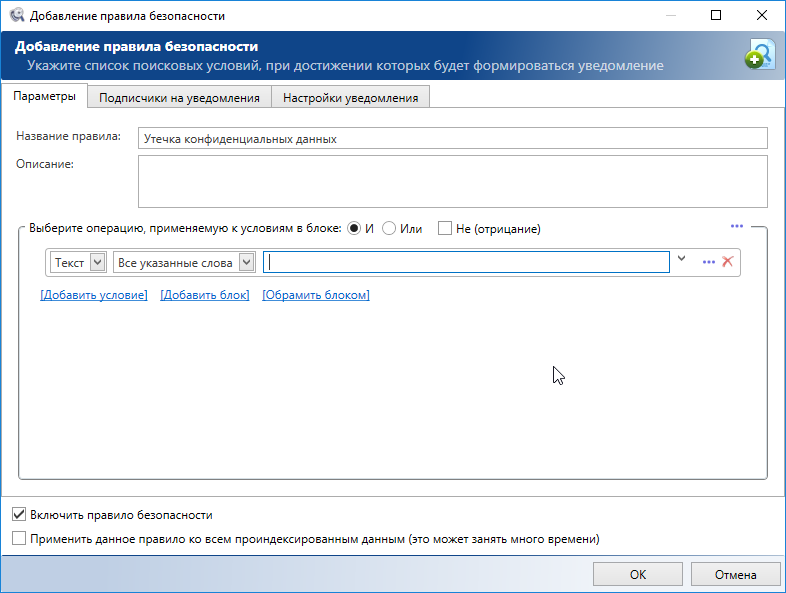
* 1. Нажмите **ОК**.



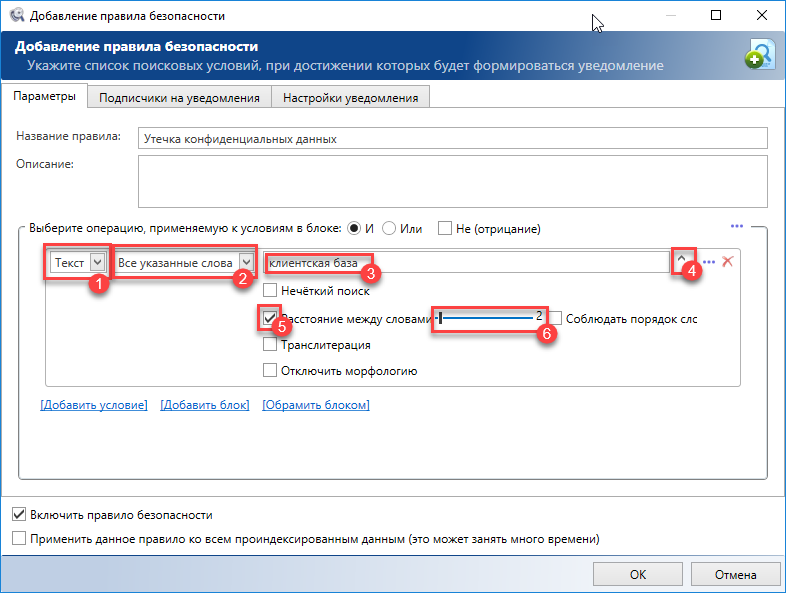
* 1. Подтвердите настройки свойств группы правил, нажав **OK**.
  2. Выберите созданную группу в списке.
  3. Нажмите кнопку **Добавить** на панели меню и выберите пункт **Обычное**либо воспользуйтесь контекстным меню группы (правая клавиша мыши)*.*



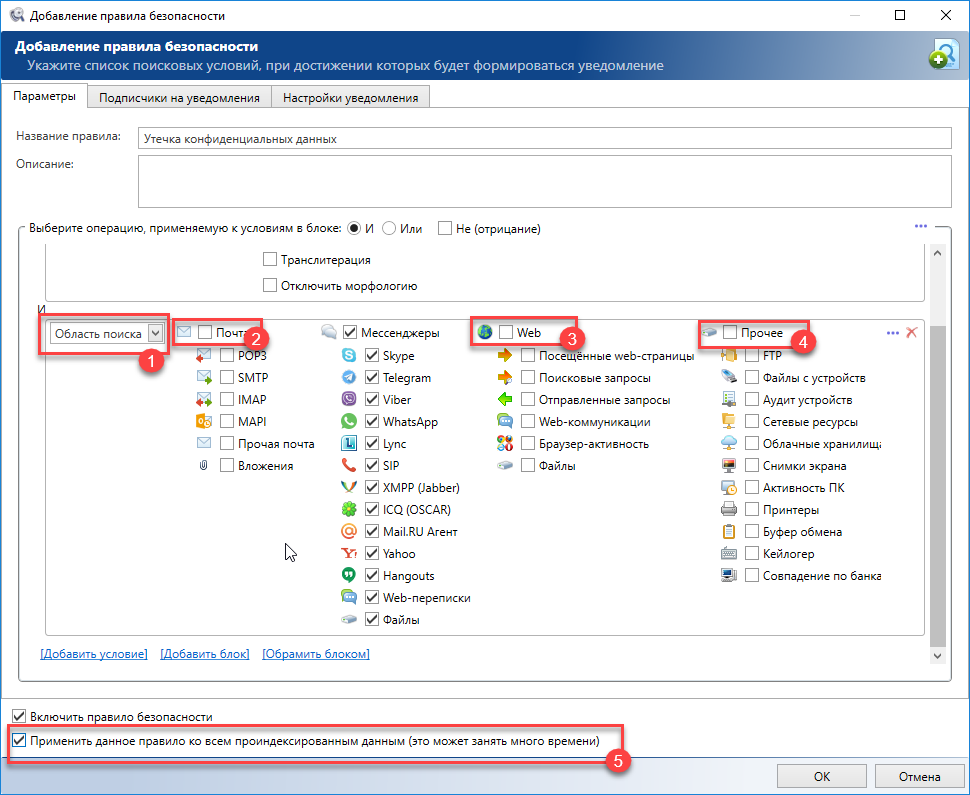
* 1. В окне добавления правила введите название правила *Утечка конфиденциальных данных*.



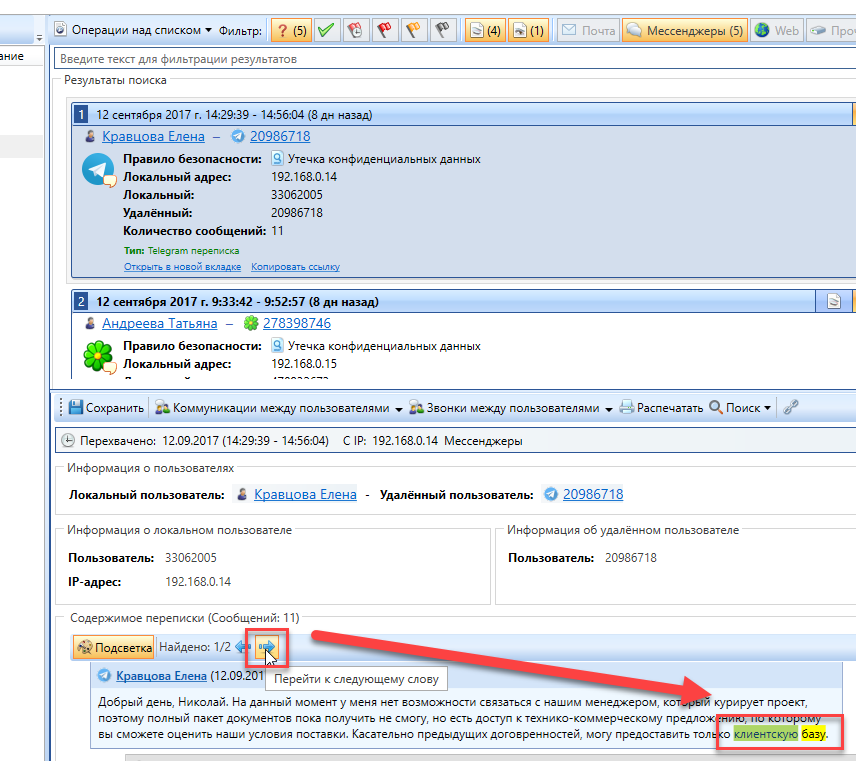
* + 1. Раскройте список **Текст** и ознакомьтесь с доступными условиями поиска. Выберите условие поиска **Текст**.
    2. Оставьте без изменений параметр **Все указанные слова** и введите словосочетание ***«****клиентская база****»*** в поле ввода.Раскройте поле с дополнительными параметрами поиска, нажав на кнопку раскрытия содержимого справа *,* отметьте опцию **Расстояние между словами** и установите расстояние между словами в 2 слова.



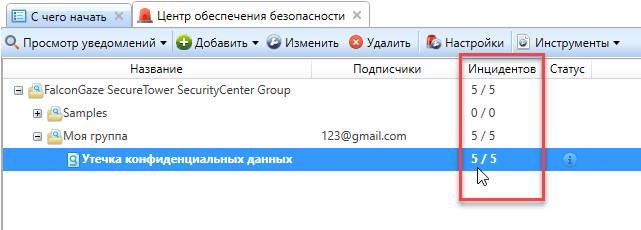
* + 1. Нажмите ссылку **Добавить условие***,* в списке условий поиска выберите**Область поиска**.
    2. Раскройте поле с дополнительными параметрами поиска и отмените выбор областей **Почта**, **Web**, **Прочее***.*
    3. Отметьте опцию **Применить данное правило ко всем проиндексированным данным***.*



* + 1. Нажмите**OK**для сохранения настроек и применения правила.
    2. Выберите строку вновь созданного правила и дважды кликните мышью по выбранному правилу. Дождитесь завершения обработки правила.
    3. Изучите атрибуты и содержимое уведомлений, выбирая строку соответствующего уведомления в списке уведомлений. Для перехода к месту в документе, где встречается искомая фраза, нажмите стрелку навигации на панели инструментов окна просмотра документа.



**Результат:** Правило отображается в папке **Мои правила**. Ключевая фраза присутствует во всех документах, об обнаружении которых получены уведомления. В результате обработки правила обнаружено 5 инцидентов безопасности.

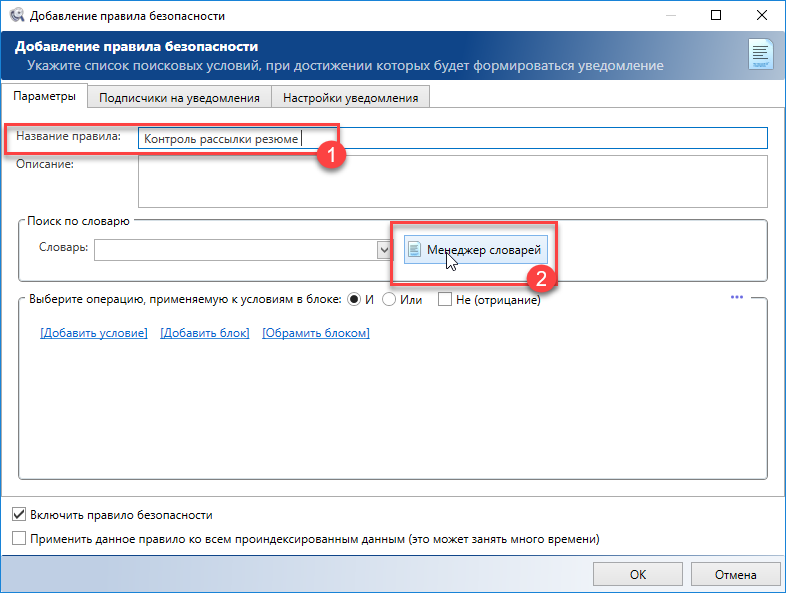


* 1. \*Перейдите в окно почтового клиента и откройте почтовый ящик, использованный на шаге 1.7. Перейдите в папку *Входящие* и откройте письмо от *Центра обеспечения безопасности.* Для просмотра деталей инцидента, вызвавшего срабатывание правила безопасности, кликните по одной из ссылок на инциденты, содержащихся в уведомлении.

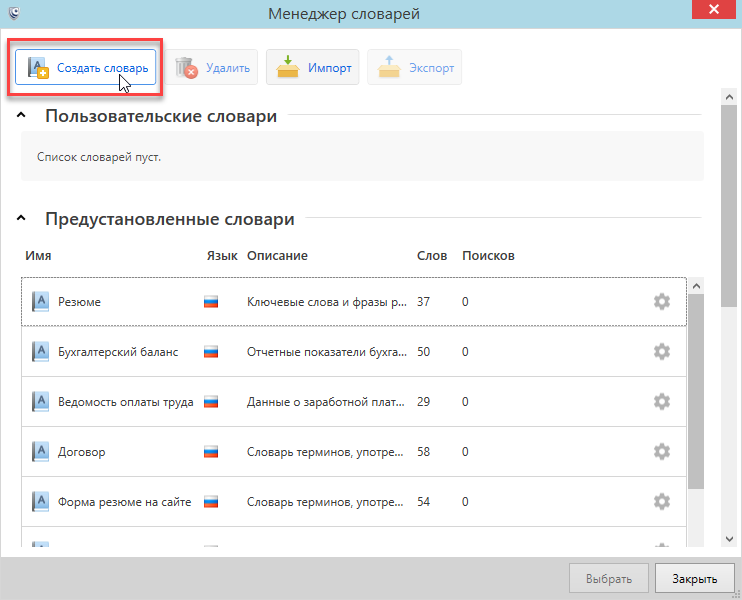
1. **Создание правила Контроль по словарю**

**Алгоритм действий**

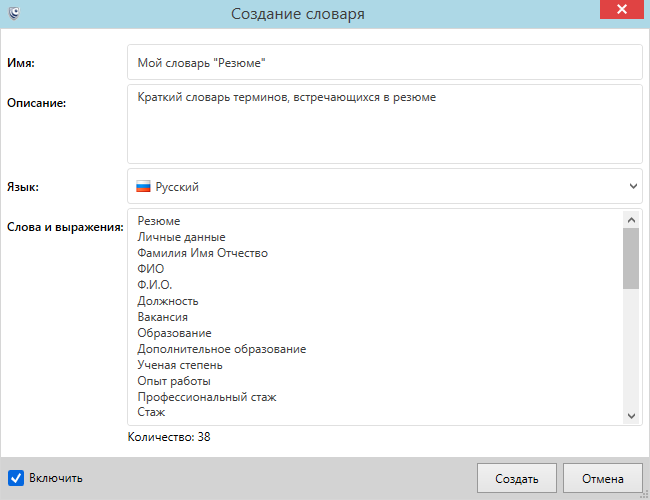
* 1. В списке правил Центра обеспечения безопасностивыберите группу **Моя группа**.
  2. Нажмите **Добавить** на панели меню и выберите пункт **Контроль по словарю***.*
  3. Введите название правила *Контроль рассылки резюме* в окне добавления правила.
  4. Нажмите кнопку **Менеджер словарей**.



* + 1. На панели команд окна менеджера выберите **Создать словарь**.

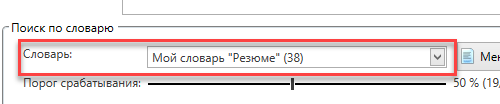


* + 1. Введите название словаря *Мой словарь "Резюме".*
    2. Откройте файл *Словарь Резюме.docx*, расположенном на рабочем столе Вашего компьютера в папке Student. Скопируйте термины, приведенные в файле, и вставьте в поле **Слова и выражения**, используя сочетание *CTRL+V* либо команду *Paste* контекстного меню.

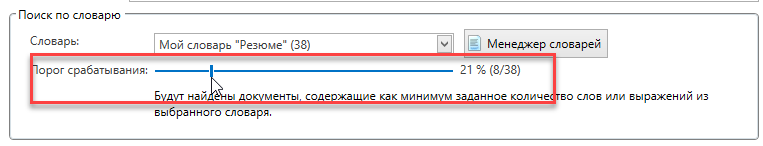


* + 1. Нажмите **Создать** для сохранения словаря.
    2. Выберите словарь *Мой словарь "Резюме"* в списке и нажмите **Выбрать**.

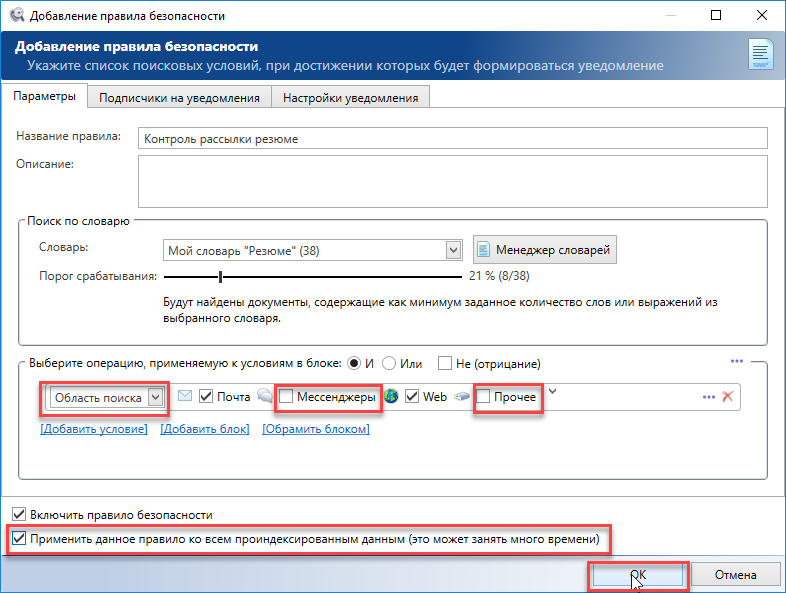
**Результат:** Имясловаря отображается в поле списка **Словарь**.



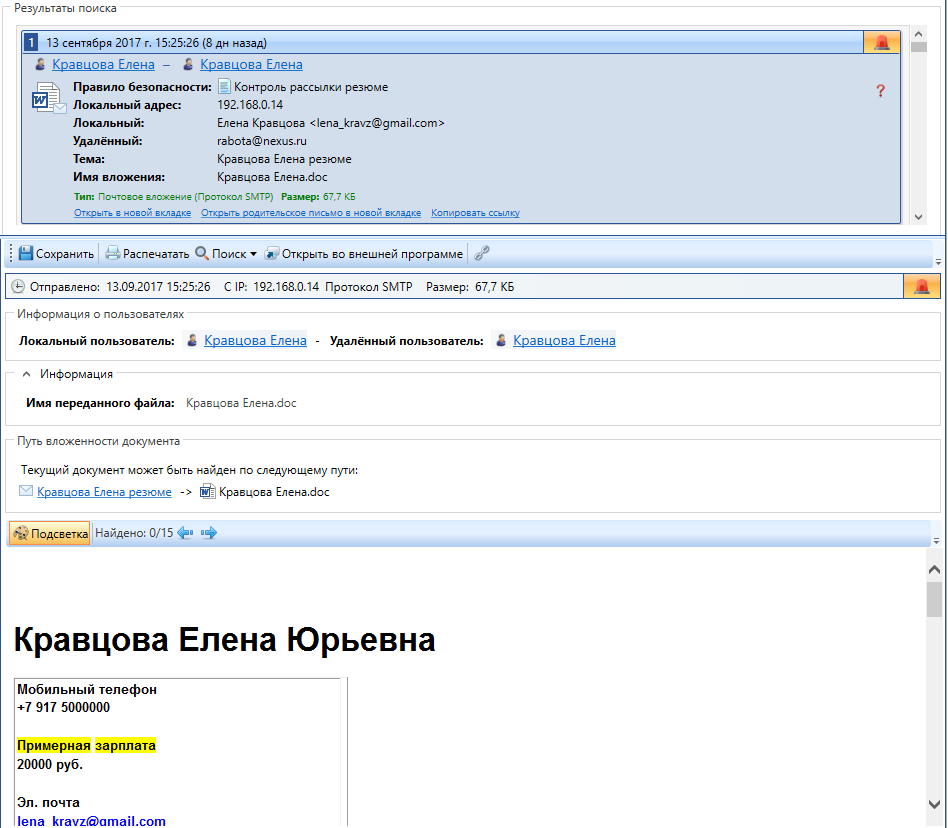
* 1. Передвиньте ползунок **Порог срабатывания** на значение 21% (8 слов из 38).



* 1. Нажмите ссылку **Добавить условие**.
  2. Выберите условие поиска **Область поиска** в списке условий. Раскройте поле с дополнительными параметрами и отмените выбор областей **Мессенджеры** и **Прочее** для осуществления поиска только в почтовых сообщениях и данным, отправленным в Интернет через браузер (электронная почта, посты на формах, соцсетях, веб-формы резюме).
  3. Отметьте **Применить правило ко всем проиндексированным данным** и нажмите ***OK***.



* 1. Дождитесь завершения обработки правила. Изучите полученные результаты срабатывания правила.



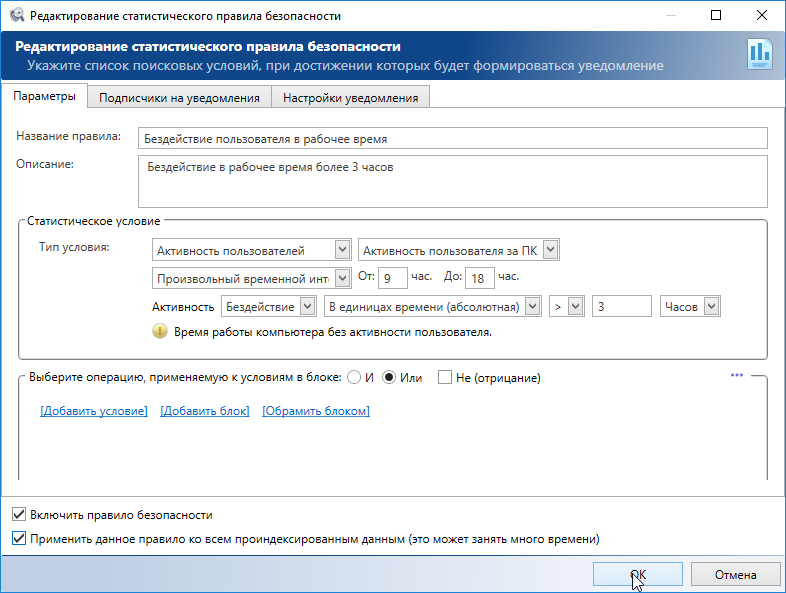
**Результат:** В результате обработки правила обнаружено 20 инцидентов безопасности.

* 1. Выберите правило по словарю в списке и нажмите **Изменить** на панели команд либо выберите команду в контекстном меню правила. Измените порог срабатывания на произвольный, примените правило ко всем проиндексированным данным и сохраните изменения. Обратите внимание, как это скажется на результатах срабатывания.

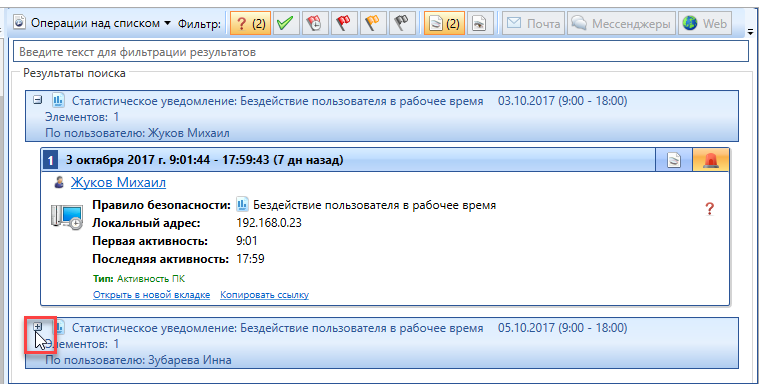
1. **Создание статистического правила**

**Алгоритм действий**

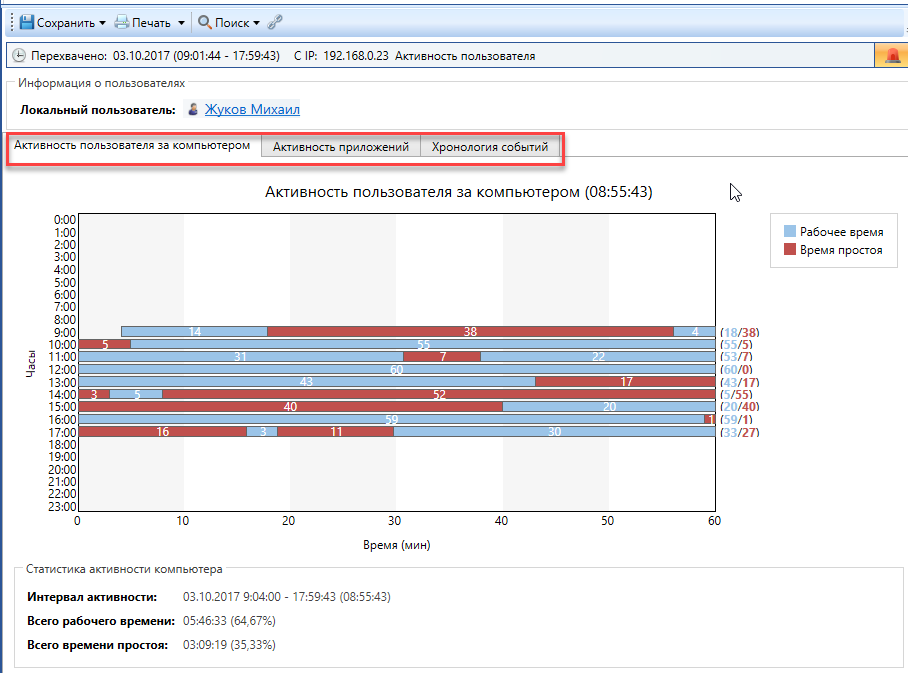
* 1. Создайте статистическое правило, выбрав соответствующий пункт в меню **Добавить**. Введите название правила *Бездействие пользователя в рабочее время*.
  2. Установите следующие значения в полях раздела **Тип условия**:
* **Активность пользователей / Активность пользователей за ПК**
* **Произвольный временной интервал: от 9 до 18 час**
* **Активность >1 часа**
  1. В полях раздела **Активность**: Бездействие > 3 Часов.
  2. Примените правило ко всем проиндексированным данным.



* 1. Нажмите **ОК** для сохранения настроек.
  2. Дважды кликните по имени правила после завершения обработки и изучите полученные результаты срабатывания правила.
     1. Для того чтобы развернуть/свернуть уведомление, нажмите соответствующую кнопку в левом верхнем углу карточки уведомления.



* + 1. Переключайтесь между закладками в зоне просмотра инцидента для отображения доступных отчетов об активности.

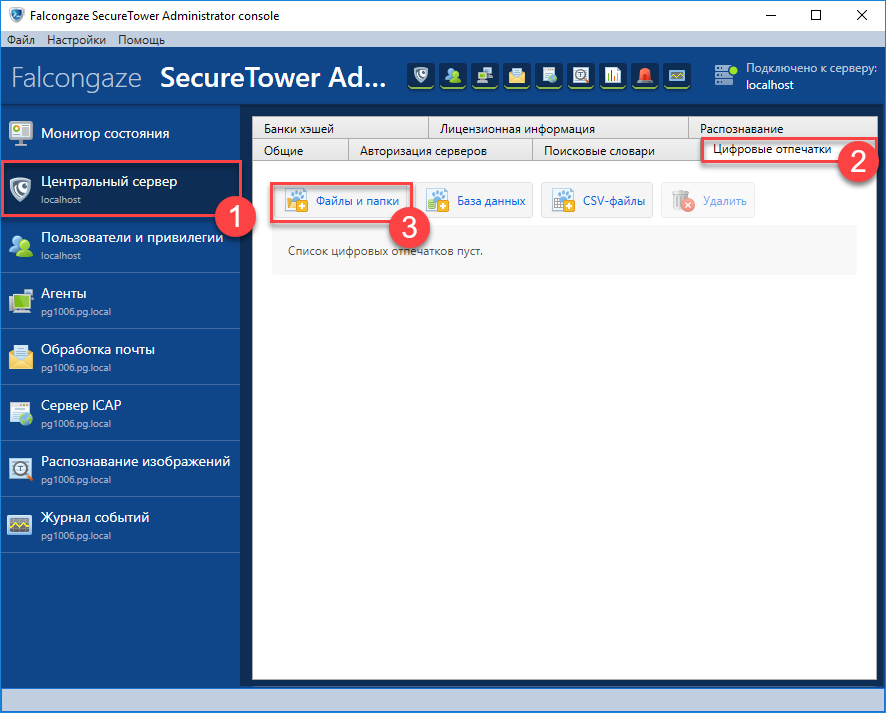


**Результат:** В результате обработки правила обнаружено 2 инцидента безопасности.

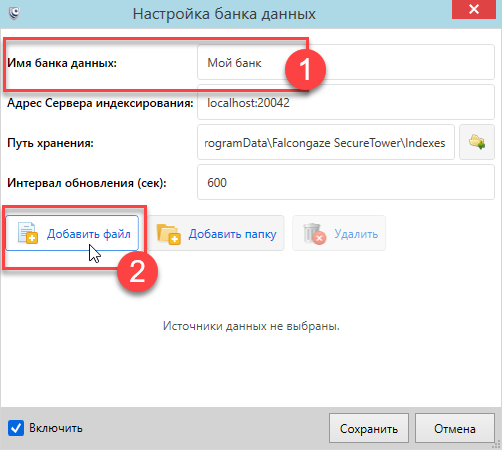
1. **Создание правила контроля по цифровым отпечаткам**

**Алгоритм действий**

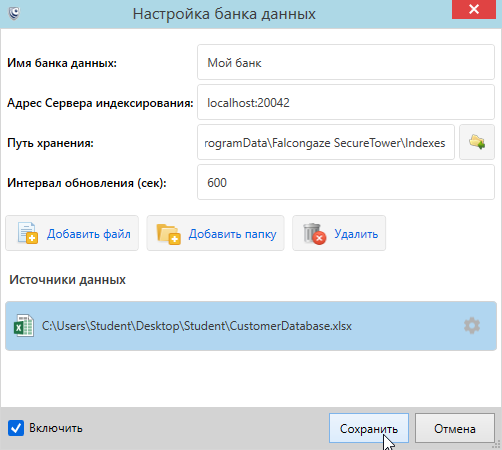
* 1. Откройте Консоль администратора **SecureTower**.
  2. Выберите вкладку **Центральный сервер** на боковой панели главного окна программы, перейдите на вкладку **Цифровые отпечатки** и нажмите **Файлы и папки**.



* + 1. Введите имя банка *Мой банк*и нажмите **Добавить файл** в окне настройке банка.

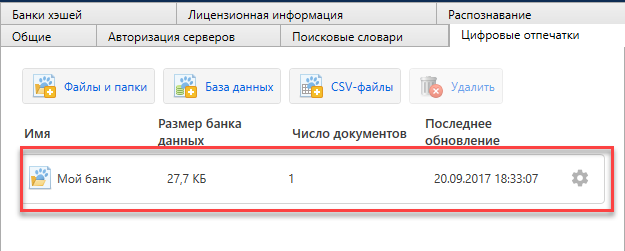


* + 1. В открывшемся окне выбора файла, укажите путь к файлу, для которого создается отпечаток *C:\Users\Student\Desktop\CustomerDatabase.xlsx*. Нажмите **Создать** для добавления банка данных в базу цифровых отпечатков.

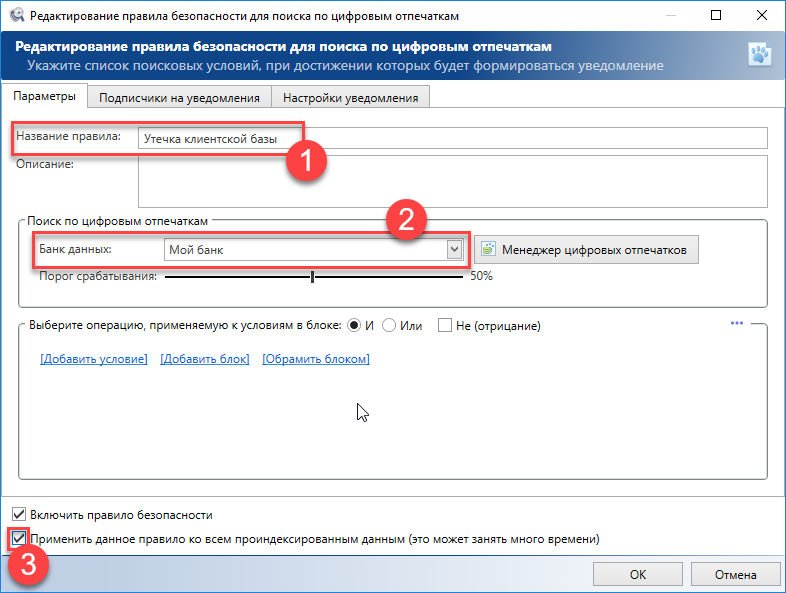


* + 1. Нажмите **Сохранить**.

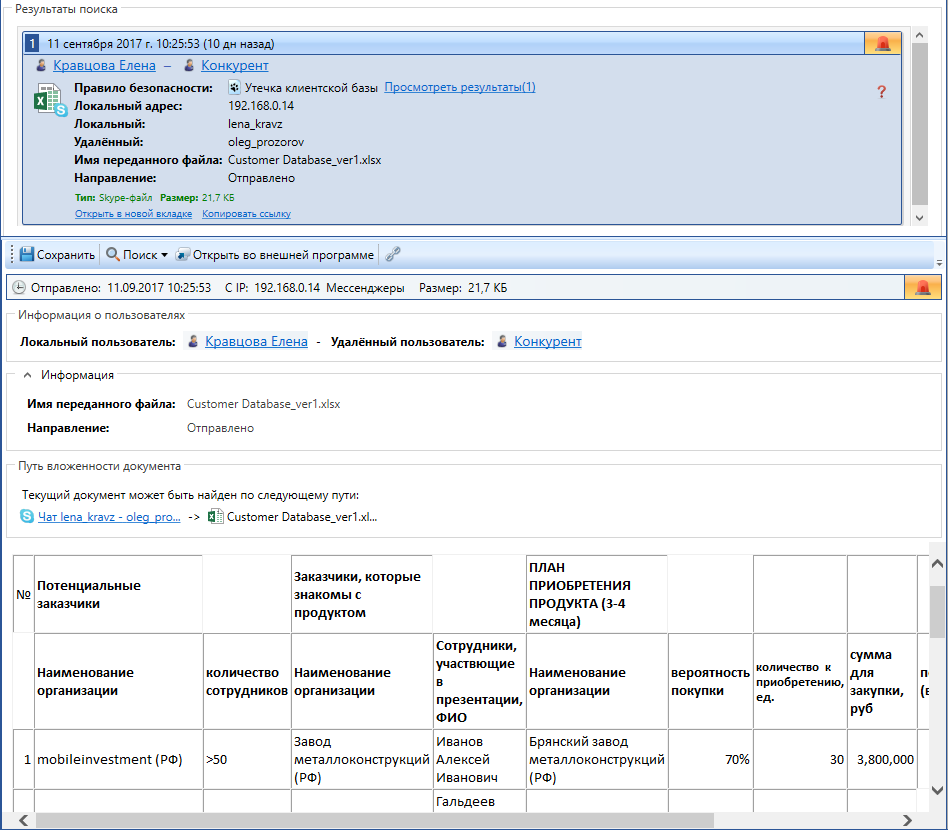
**Результат:** Имя банка отображается в списке цифровых отпечатков.



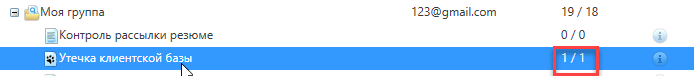
* 1. Перейдите в Консоль пользователя, выполните переподключение к серверу и перейдите в окно **Центр обеспечения безопасности**.
  2. Создайте правило поиска по цифровым отпечаткам, выбрав соответствующий пункт в меню **Добавить**.
  3. Введите название правила "*Утечка клиентской базы"*.
  4. Выберите **Мой банк** из списка поля **Банк данных**.
  5. Примените правило ко всем ранее перехваченным данным.



* 1. Нажмите ОК для сохранения настроек.
  2. Дважды кликните по имени правила после завершения обработки и изучите полученные результаты срабатывания правила.



**Результат:** В результате обработки правила обнаружен 1 инцидент безопасности.



* 1. \*Удалите все правила. Для этого выберите созданную Вами группу в списке и нажмите **Удалить** на панели команд вкладки **Центр обеспечения безопасности**.
  2. \*Нажмите кнопку **Настройки** и очистите все поля формы. Сохраните изменения.
  3. Закройте окно Клиентской консоли.
  4. \*Удалите банк ***CustomerData*** в Консоли администратора, выбрав имя банка в списке цифровых отпечатков и нажав кнопку **Удалить**на панели команд вкладки **Цифровые отпечатки**.

**Контрольные вопросы**

1. Какие способы используются в системе SecureTower для оповещения о сетевых событиях, нарушающих политику безопасности?
2. Какие виды правил безопасности доступны в Центре обеспечения безопасности?
3. Для каких источников данных доступна возможность создания цифровых отпечатков?
4. В чем основные отличия контроля по тексту, по словарю от контроля за событиями безопасности по цифровым отпечаткам?