

Лабораторный практикум

МОНИТОРИНГ СЕТЕВОЙ И КОМПЬЮТЕРНОЙ АКТИВНОСТИ
ПОЛЬЗОВАТЕЛЕЙ. Ч.1

при помощи Консоли пользователя Falcongaze SecureTower

Цель практического занятия: Научиться работе с Клиентской консолью **Falcongaze SecureTower** для проведения расследований и предупреждения инцидентов информационной безопасности организации, освоить различные виды поиска информации в объеме перехваченных данных. Научиться интерпретировать фотографию рабочего дня пользователя.

Оборудование и настройки: ПК с установленным комплексом **Falcongaze SecureTower**.

Содержание практикума

Общие сведения.....	3
Порядок выполнения работы.....	5
1. Запуск Консоли пользователя SecureTower Client Console.....	5
2. Поиск данных в объеме перехваченной информации.....	6
3. Создание комплексных поисковых запросов.....	9
4. Просмотр фотографии рабочего дня пользователя.....	13
Контрольные вопросы.....	17

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

Ярлык доступа к Консоли пользователя размещается на рабочем столе компьютера, если была выбрана соответствующая опция при установке программы. При входе в консоль требуется установить подключение к серверу. Если в системе используется внутренняя аутентификация, то для входа необходимо авторизоваться, используя данные, установленные администратором системы.

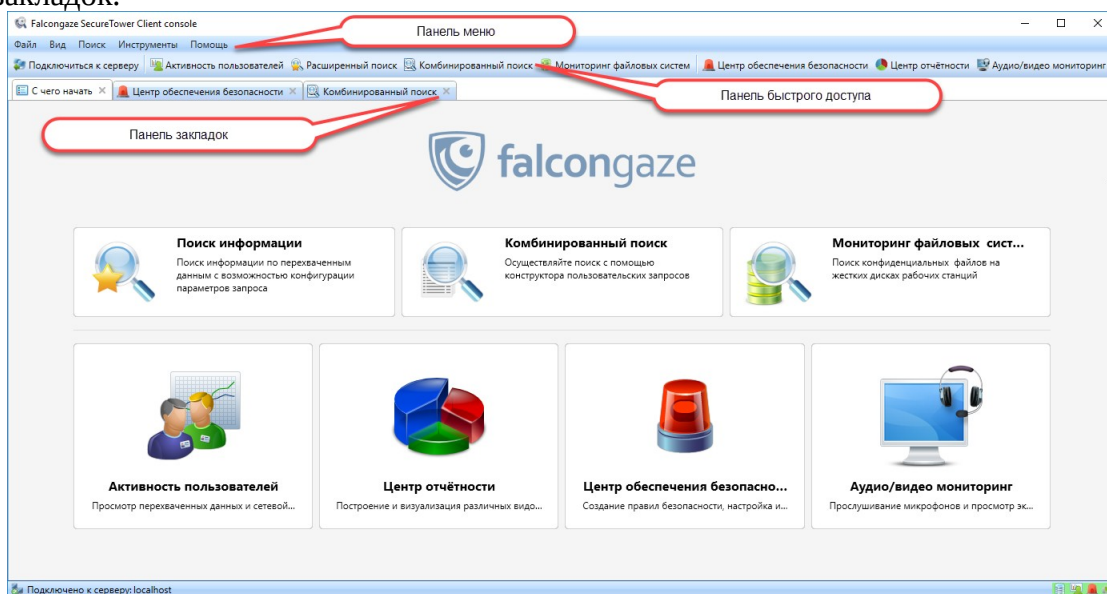
В рамках данного практикума используется сервер localhost, установленный на локальном компьютере, и вход без авторизации пользователя.

Для быстрой смены или повторного подключения к серверу, в случае потери соединения, на панели быстрого доступа главного окна консоли нажмите *Подключиться к серверу* или выберите аналогичный пункт в меню *Файл*.

Консоль Пользователя предоставляет доступ к шести компонентам:

- Активность пользователей
- Поиск информации
- Комбинированный поиск
- Центр обеспечения информации
- Центр отчетности
- Аудио/видео мониторинг
- Мониторинг файловых систем

Доступ к компонентам консоли производится со стартовой страницы путем выбора нужного компонента либо выбора кнопки компонента на панели быстрого доступа. Для быстрого переключения между открытыми окнами компонентов консоли используется панель закладок.



Одна из основных функций клиентского приложения – возможность поиска по информации, находящейся в подключенных к системе хранилищах данных. В системе поддерживается два основных режима поиска по перехваченным данным: **расширенный** и **комбинированный**. В первом случае можно уточнить поисковый запрос дополнительными параметрами содержащей набор определенных ключевых слов с учетом морфологии. Компонент поддерживает возможность учета расстояния между словами запроса, учет порядка слов, транслитерации и опечаток (нечеткий поиск).

Для формирования наиболее точных запросов система предоставляет возможности комбинированного поиска с учетом множества поисковых критериев.

Для получения полного спектра информации о всех видах компьютерной и сетевой активности пользователей используется компонент консоли *Активность пользователей*. Для анализа доступны также графики активности пользователя в различных областях,

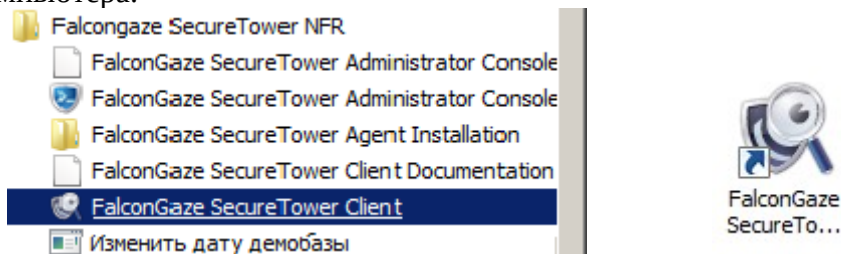
позволяющие оценить как количественные, так и качественные характеристики активности. Инструмент Граф - анализатор, который позволяет отобразить круг общения пользователя за текущий период как внутри организации, так и за ее пределами, позволяет просматривать содержание взаимосвязей пользователей, просматривать схемы коммуникаций и информацию о контактирующих пользователях.

Порядок выполнения работы

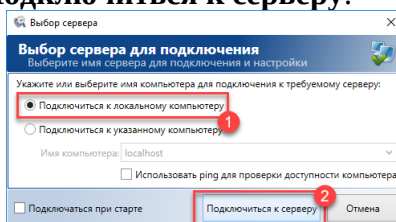
1. Запуск Консоли пользователя SecureTower Client Console

Алгоритм действий

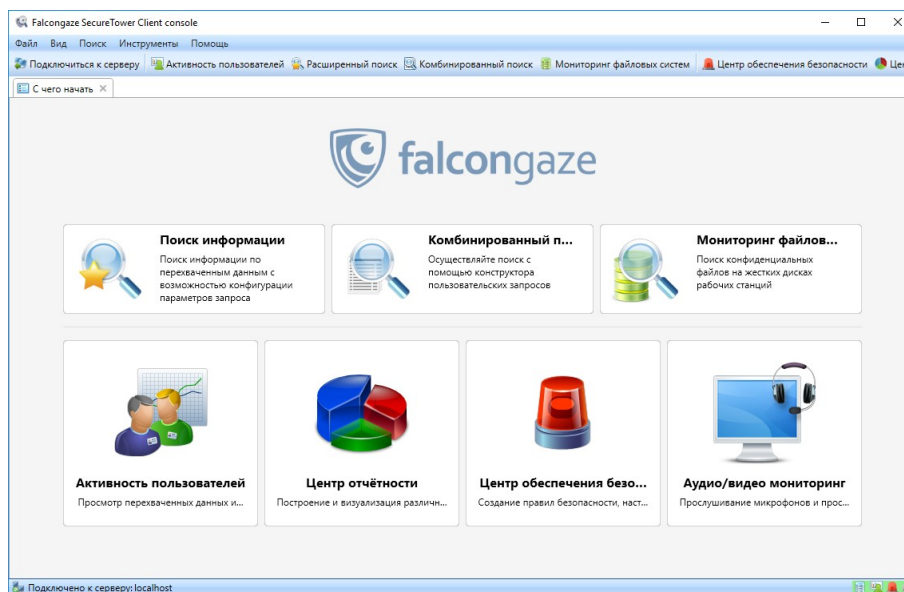
1.1 Запустите Клиентскую консоль, используя ярлык консоли, размещенный в папке *Falcongaze SecureTower NFR* в меню **Пуск** либо используйте ярлык консоли на рабочем столе компьютера.




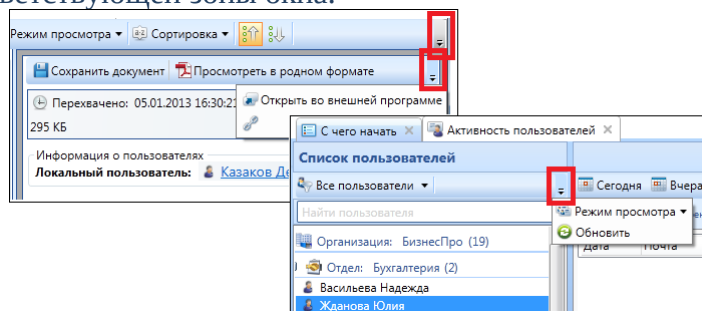
1.2 В открывшемся диалоговом окне выберите **Подключиться к локальному компьютеру** и нажмите кнопку **Подключиться к серверу**.



Результат: Консоль пользователя успешно подключилась к серверу. В окне консоли отображается стартовая страница. Все компоненты консоли доступны для использования.



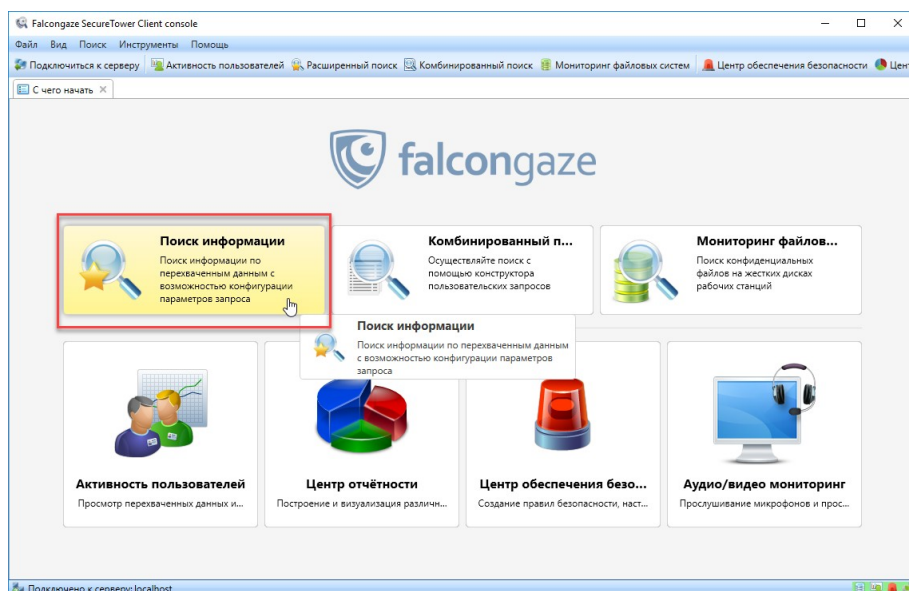
Внимание! Если окно Консоли пользователя находится в свернутом состоянии, то некоторые пункты меню могут быть скрыты. Для доступа к скрытым пунктам нажмите кнопку , расположенную в панелях инструментов вкладок компонентов, либо измените текущие границы соответствующей зоны окна.




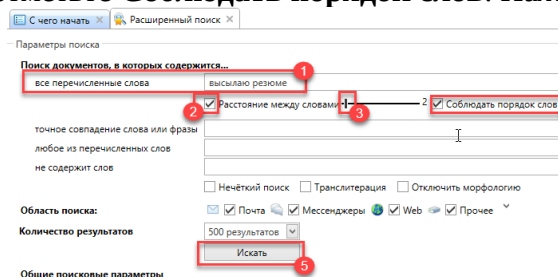
2. Поиск данных в объеме перехваченной информации

Алгоритм действий

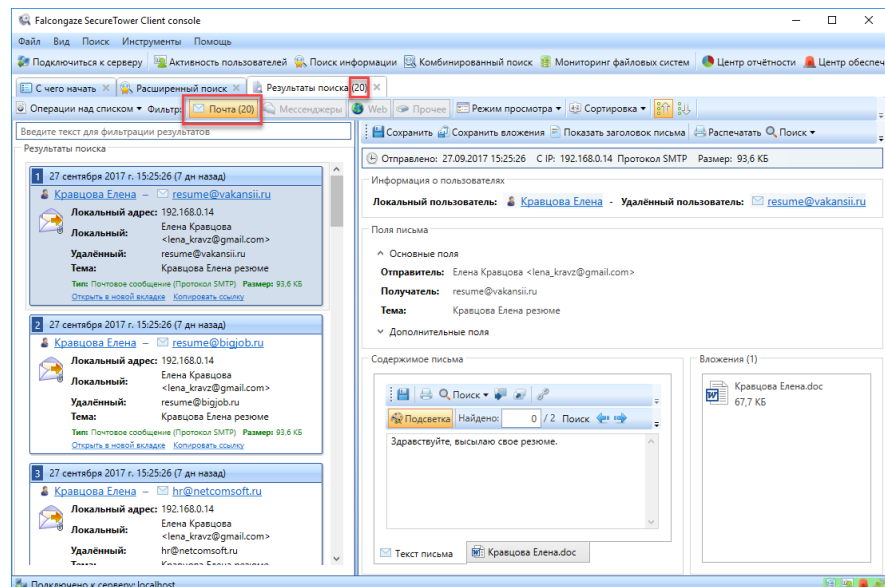
2.1 На стартовой странице Консоли пользователя кликните на панели **Поиск информации**.



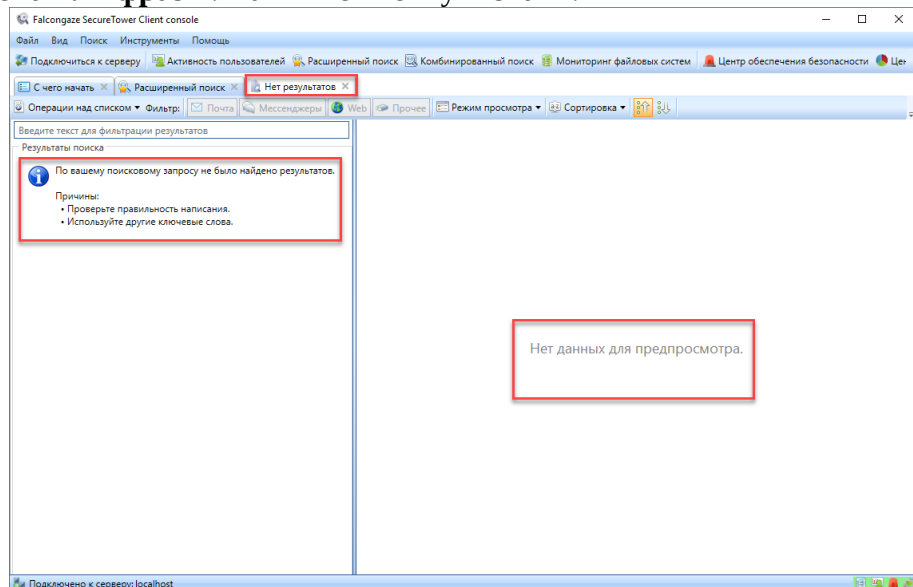
2.2 В поле ввода **все перечисленные слова** введите фразу «высылаю резюме». Раскройте поле с дополнительными параметрами поиска, нажав на кнопку раскрытия списка  справа. Отметьте опции **Расстояние между словами** и передвиньте ползунок в значение 2 (слова), затем отметьте **Соблюдать порядок слов**. Нажмите кнопку **Искать**.



В окне закладки **Результаты поиска** изучите полученные результаты и закройте закладку.



2.3 Перейдите на закладку **Расширенный поиск**. Очистите поле **все перечисленные слова** и введите фразу «*высылаю резюме*» в поле ввода **точное совпадение слова или фразы**. Нажмите кнопку **Искать**.

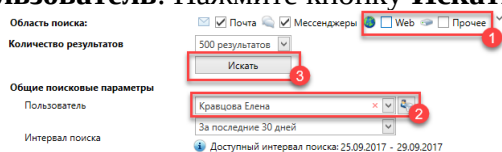


Убедитесь, что данных, отвечающих условиям поиска, найдено не было и закройте закладку **Результаты поиска**.

2.4 Перейдите на закладку **Расширенный поиск**. Очистите поле **точное совпадение слова или фразы**. Введите фразу «*высылаю резюме*» в поле **любое из перечисленных слов**. Нажмите кнопку **Искать**. Изучите результаты и закройте закладку.

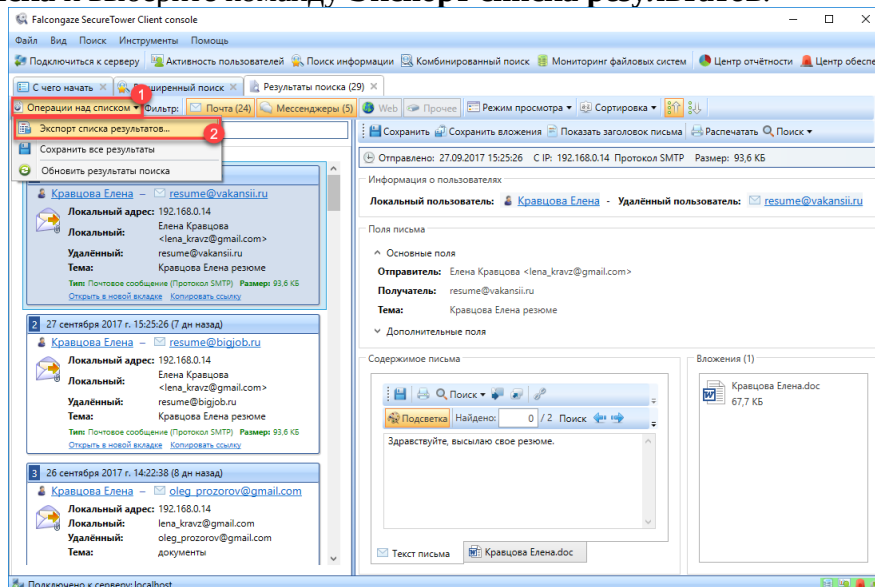
2.5 Отметьте опции **Нечеткий поиск** (положение слайдера-2) и **Транслитерация**. Нажмите кнопку **Искать**, изучите изменения в результатах поиска и закройте закладку.

2.6 Вернитесь на закладку **Расширенный поиск**. Отмените выбор для областей поиска **Web** и **Прочее**. В разделе **Общие поисковые параметры** выберите пользователя **Кравцова Елена** в списке **Пользователь**. Нажмите кнопку **Искать**.

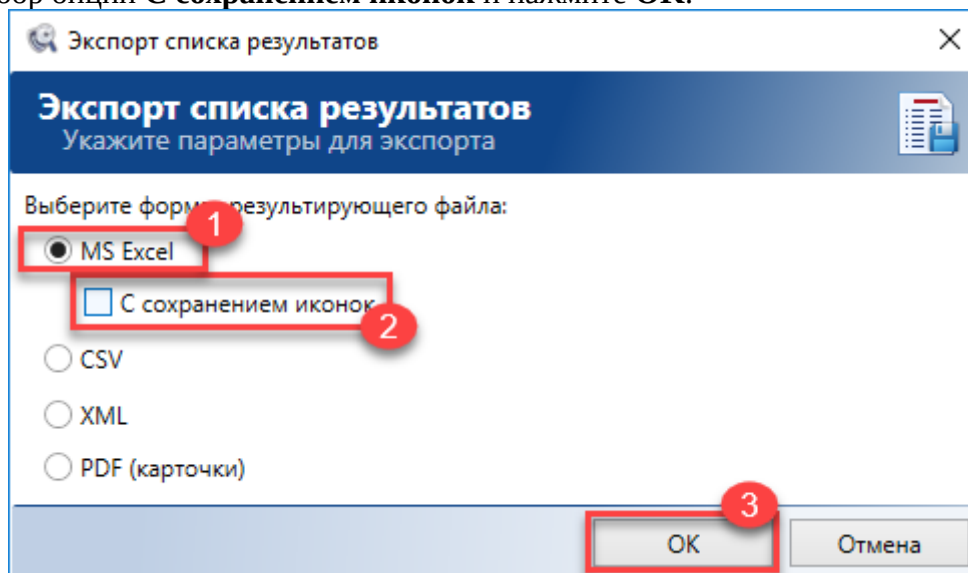


Изучите изменения в результатах поиска.

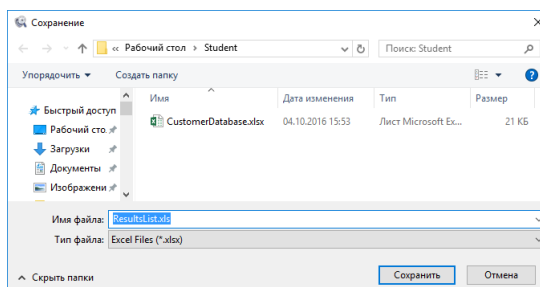
2.7 Нажмите кнопку **Операции над списком** на панели инструментов закладки **Результаты поиска** и выберите команду **Экспорт списка результатов**.



2.8 В диалоговом окне экспорта убедитесь, что выбран формат MS Excel, отмените выбор опции **С сохранением иконок** и нажмите **ОК**.



2.9 Сохраните полученный файл с ResultsList.xls в папку Student на рабочем столе компьютера.



2.10 Дождитесь сохранения и откройте Excel - файл результатов для просмотра.

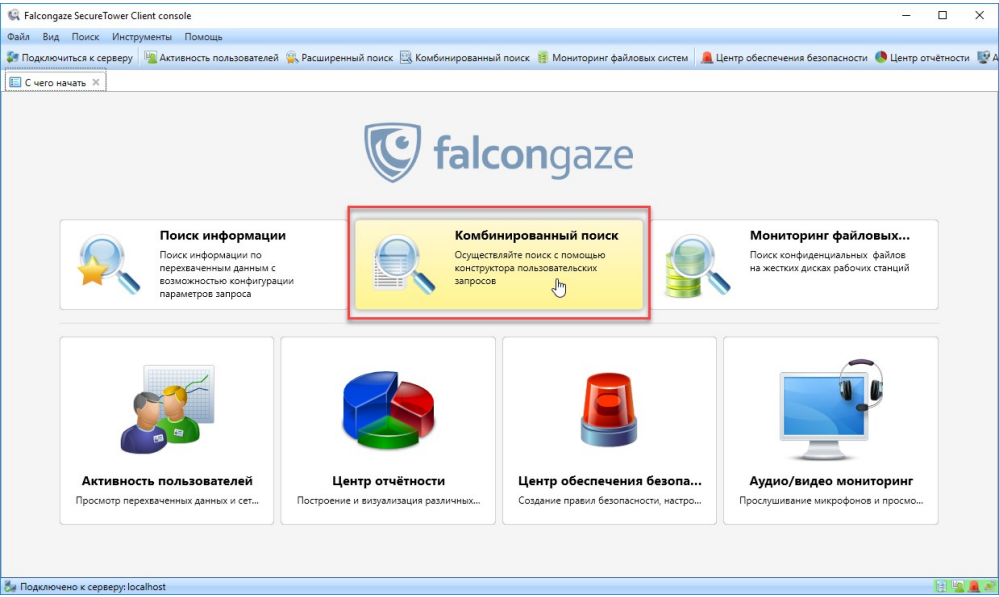
Тип данных	Локальный пользователь	Удалённый пользователь	Перехвачено	Размер	Прочая информация
ICQ-переписка (Протокол OSCAR (ICQ))	Кравцова Елена	Андреева Татьяна	02.01.2013 10:22:10	Сообщений: 17	Iena_kravz - tanya_andreeva
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме
Почтовое сообщение (Протокол SMTP)	Кравцова Елена	Неизвестный пользователь	03.01.2013 12:25:26	93,5 КБ	Кравцова Елена резюме

2.11 Закройте файл Excel, перейдите на стартовую страницу Консоли пользователя, закрыв все открытые ранее вкладки.

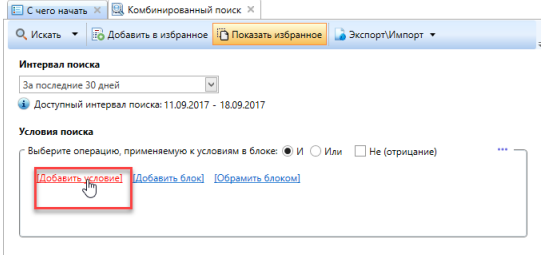
3. Создание комплексных поисковых запросов

Алгоритм действий

3.1 На стартовой странице Консоли пользователя кликните на панели **Комбинированный поиск**.

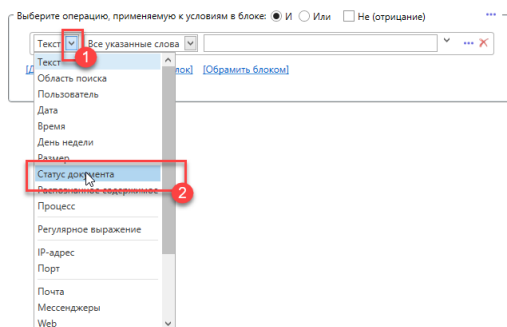


3.2 Нажмите ссылку **Добавить условие**.



3.3 Задайте поисковый запрос на обнаружение инцидентов передачи зашифрованных файлов в мессенджерах или всех случаев работы с приложением для шифрования TrueCrypt. Для этого следуйте рекомендациям пунктов 3.3.1- 3.3.10.

3.3.1 В списке типов условий поиска с предустановленным значением **Текст** выберите **Статус документа**.

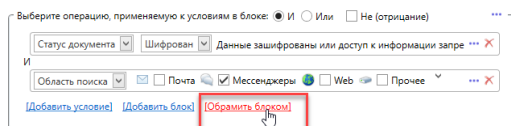


3.3.2 В списке статусов условия выберите **Шифрован** и установите значение **Да**.

3.3.3 Нажмите ссылку **Добавить условие**.

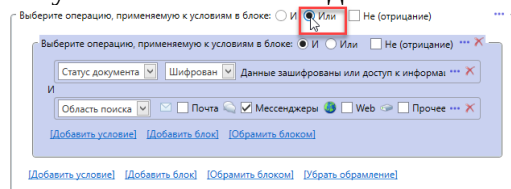
3.3.4 В списке условий поиска выберите **Область поиска** и снимите флажки в чекбоксах **Почта**, **Web**, **Прочее**. Оставьте установленным флажок в чекбоксе **Мессенджеры**.

3.3.5 Нажмите ссылку **Обрамить блоком**. Условия поиска в блоке объединены логическим «И».

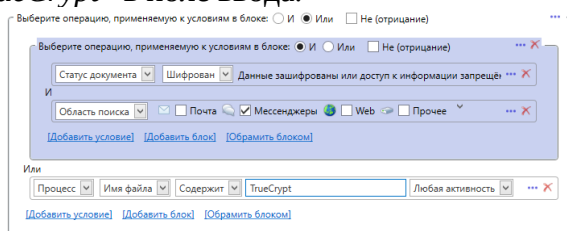


3.3.6 Нажмите **Добавить условие** под блоком, созданным на шаге 3.3.5.

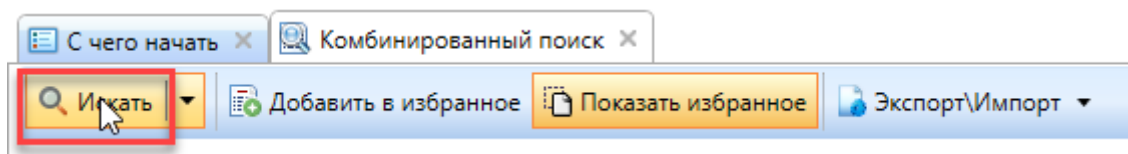
3.3.7 Нажмите переключатель **Или** в строке выбора логической операции, применяемой к условиям. Новое условие и блок объединены логическим **ИЛИ**.



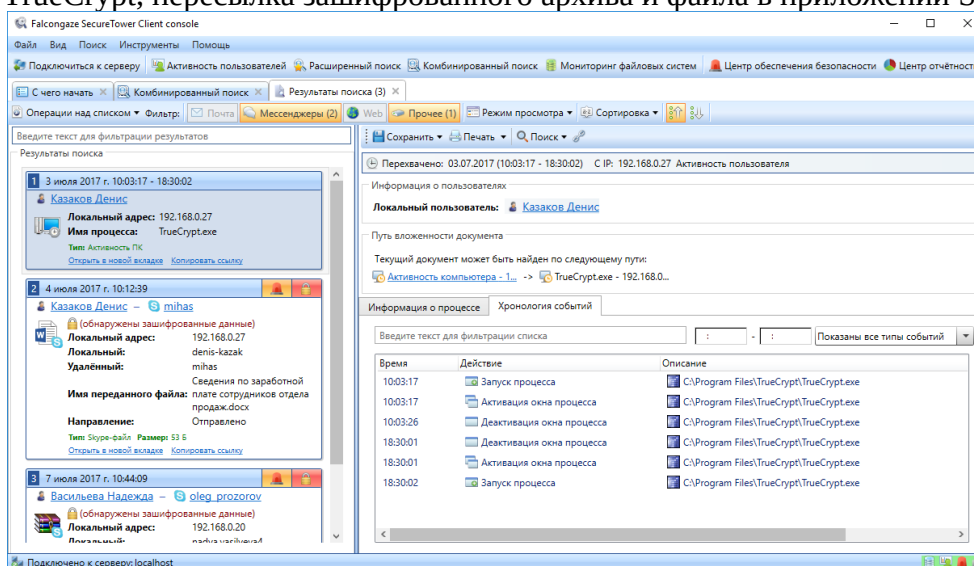
3.3.8 В списке условий поиска с предустановленным значением **Текст** выберите **Процесс** и введите имя «TrueCrypt» в поле ввода.



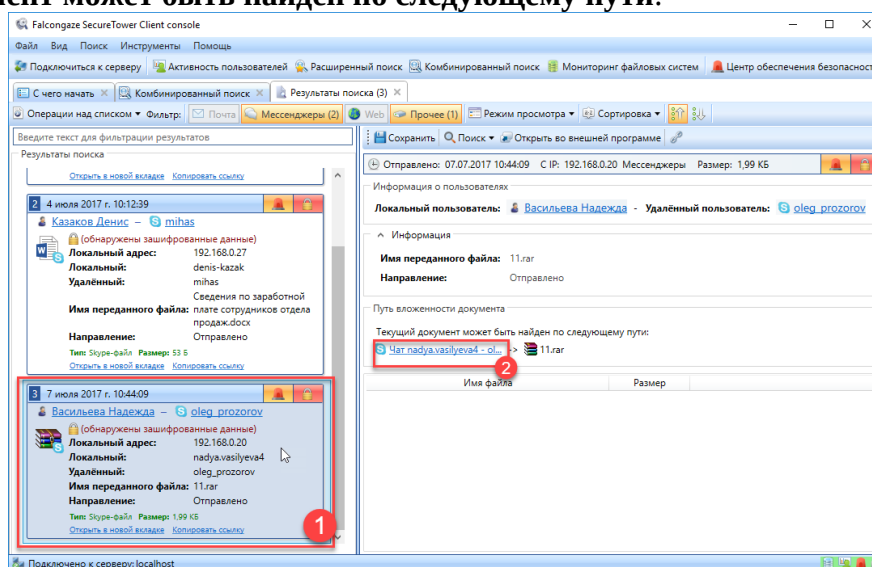
3.3.9 Нажмите **Искать** на панели инструментов закладки **Комбинированный поиск**.



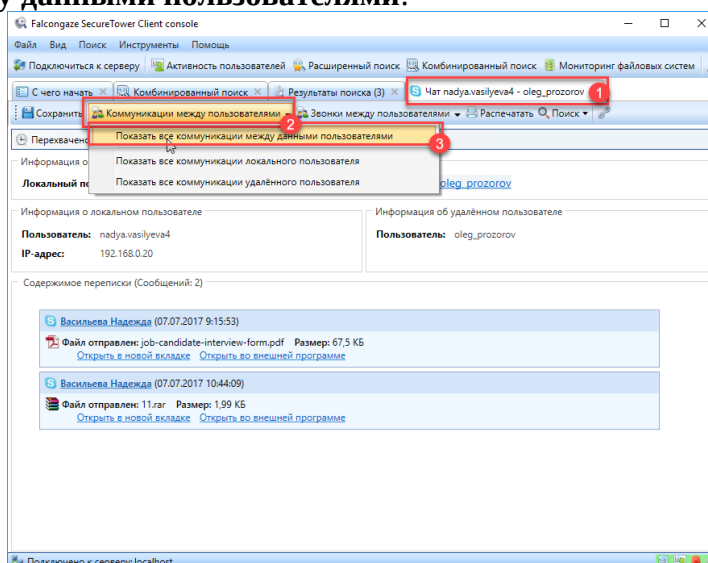
3.3.10 Изучите полученные результаты в окне закладки **Результаты поиска**.
Результат: В окне **Результаты поиска** отображается три результата: запуск приложения TrueCrypt, пересылка зашифрованного архива и файла в приложении Skype.



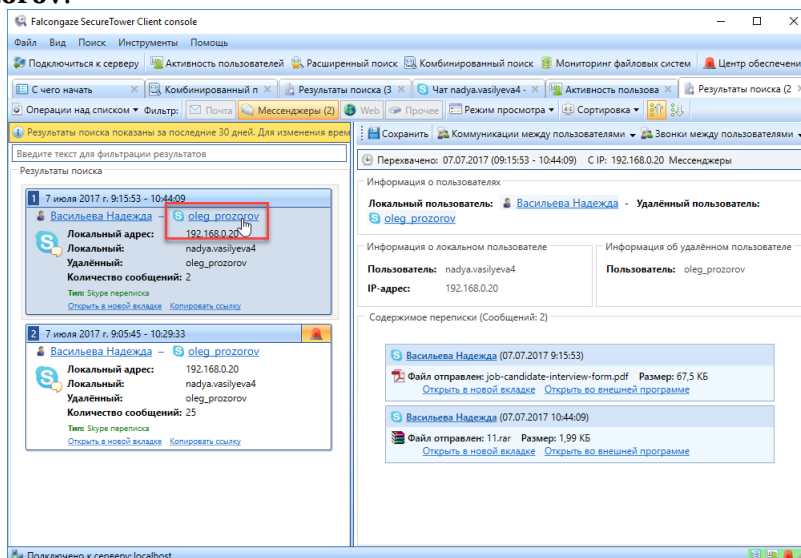
3.4 Выберите в списке результатов карточку инцидента пересылки архива в переписке Skype **Васильева Надежда - oleg_prozorov** и в зоне предпросмотра содержимого инцидента нажмите ссылку на документ верхнего уровня в разделе **Текущий документ может быть найден по следующему пути**.



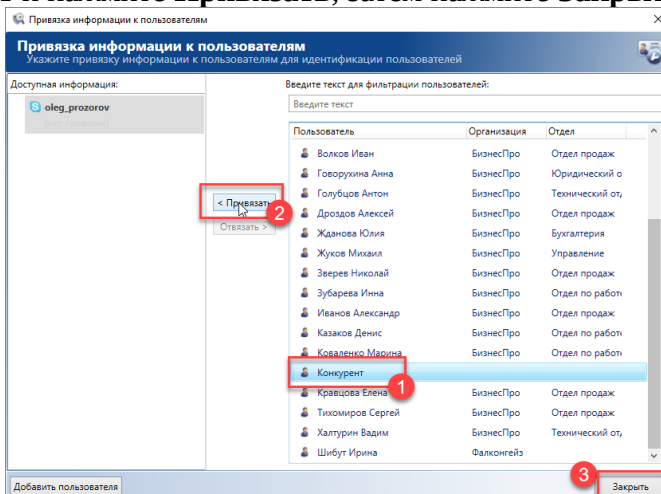
3.5 В окне закладки содержимого переписки на панели инструментов кликните **Коммуникации между пользователями**, затем выберите команду **Показать все коммуникации между данными пользователями**.



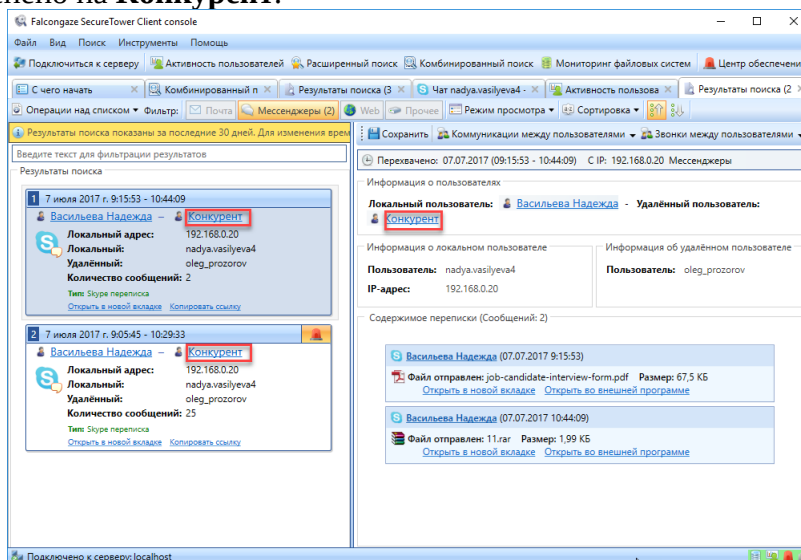
3.6 Во вновь открывшемся окне **Результаты поиска** кликните по имени контакта **oleg_prozorov**.



3.6.1 В списке пользователей в правой части открывшегося окна выберите имя пользователя **Конкурент** и нажмите **Привязать**, затем нажмите **Закреть**.



Результат: В окне **Результаты поиска** по коммуникациям имя контакта **oleg_prozorov** заменено на **Конкурент**.



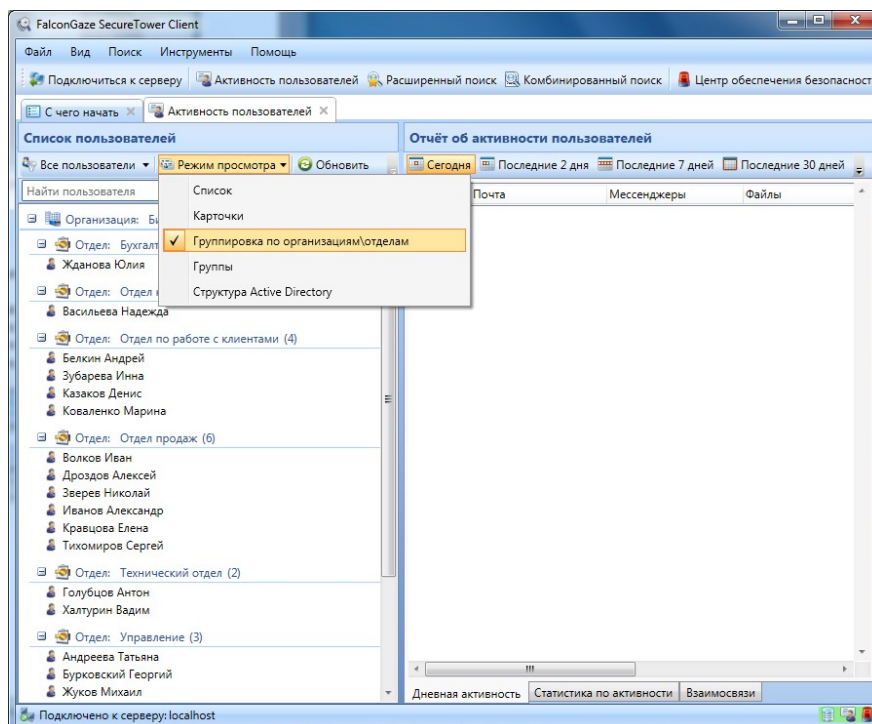
3.7 Закройте все открытые закладки, кроме стартовой страницы **С чего начать**.

4. Просмотр фотографии рабочего дня пользователя

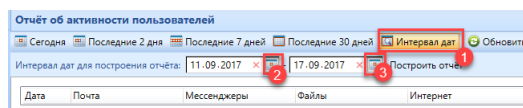
Алгоритм действий

4.1 На стартовой странице Консоли пользователя кликните на панели **Активность пользователей**.

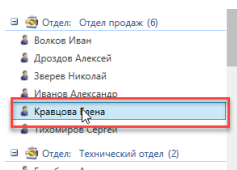
4.2 На панели инструментов вкладки **Активность пользователей** нажмите кнопку **Режим просмотра** и выберите команду **Группировка по организациям/отделам**.



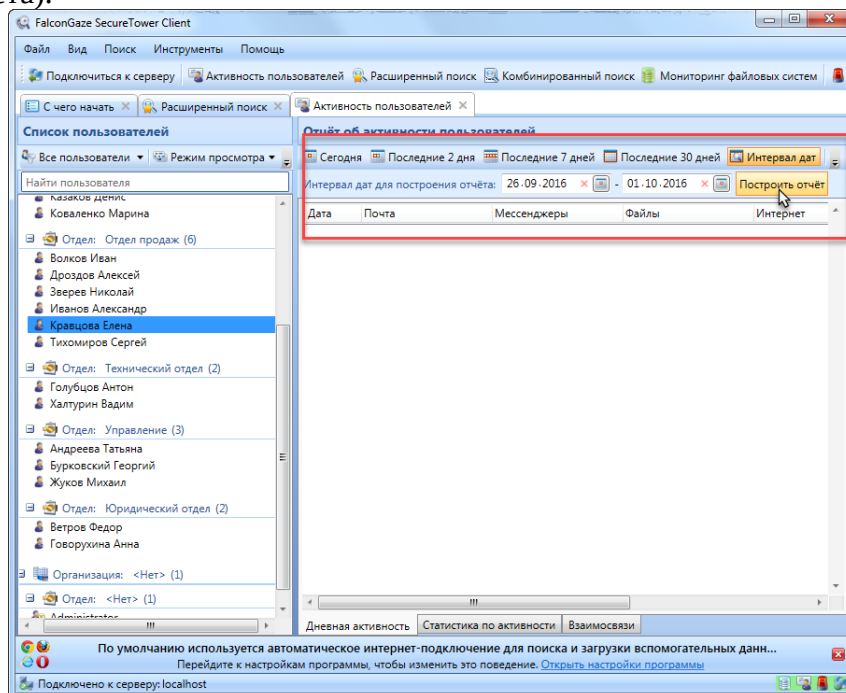
4.3 Нажмите **Интервал дат** на панели инструментов зоны просмотра фотографии рабочего дня и установите предыдущую рабочую неделю, как интервал дат для построения отчетов.



4.4 Выберите пользователя **Кравцова Елена** в группе **Отдел продаж** списка пользователей.

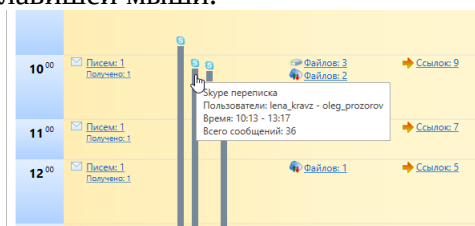


4.5 Постройте отчет об активности (двойной щелчок левой клавиши мыши по имени пользователя либо кнопка **Построить отчет** на панели инструментов зоны отображения отчета).

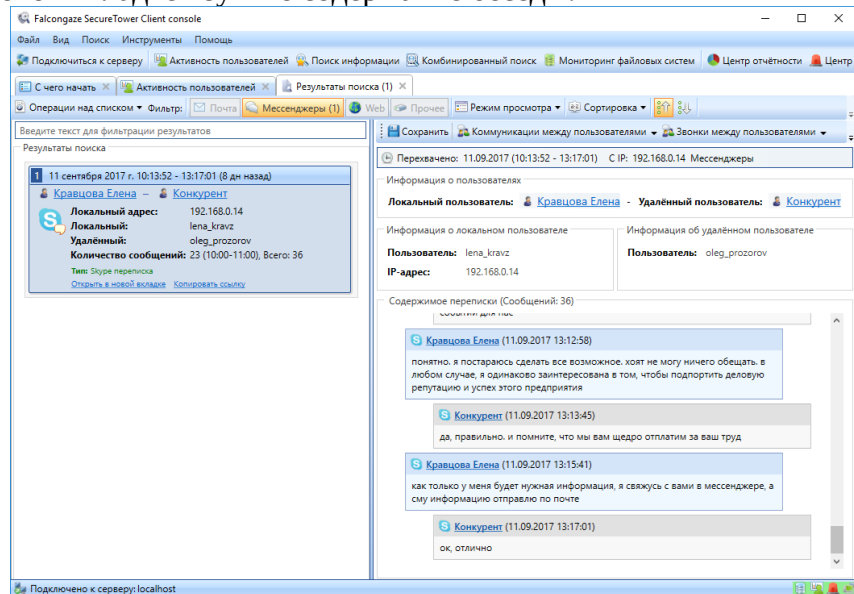


4.6 Перейдите к отчету за первый рабочий день отчетной недели и изучите активность пользователя в промежутке 10.00-12.00. Все элементы отчета кликабельны.

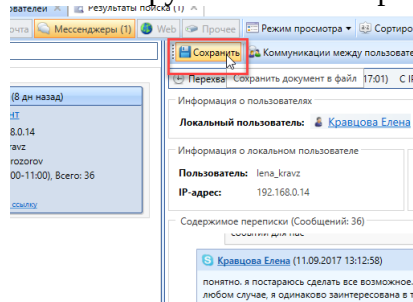
4.7 Наведите курсор на Skype-переписку пользователя, начатую в 10.13, и кликните по переписке левой клавишей мыши.



4.7.1 В новой вкладке изучите содержание беседы.



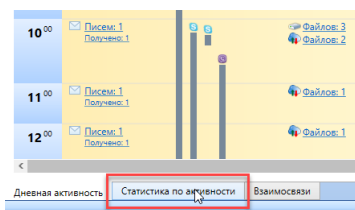
4.7.2 Выполните сохранение содержания беседы в отдельный файл с произвольным названием в папку Student на рабочем столе компьютера. Для сохранения нажмите кнопку **Сохранить** на панели инструментов зоны просмотра переписки.



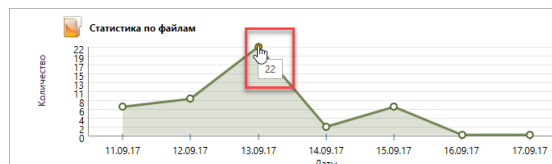
Результат: Файл *Skype conversation - lena_kravz_2017.09.11_10.13.52.rtf* сохранен в папке Student.

4.8 Вернитесь на вкладку **Активность пользователей**.

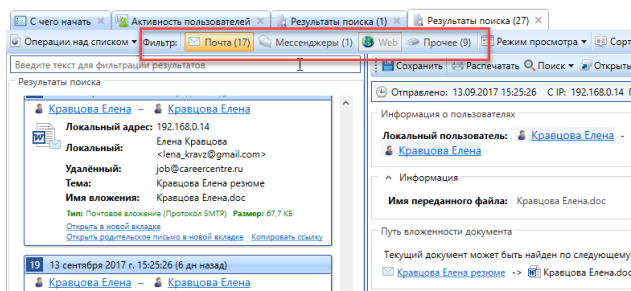
4.9 Выберите закладку **Статистика по активности** на нижней панели окна **Активность пользователей**.



4.10 Используя полосу прокрутки в зоне просмотра статистики, перейдите к графику **Статистика по файлам**. Наведите курсор на третий узел графика, соответствующий пиковой активности, и кликните по нему.



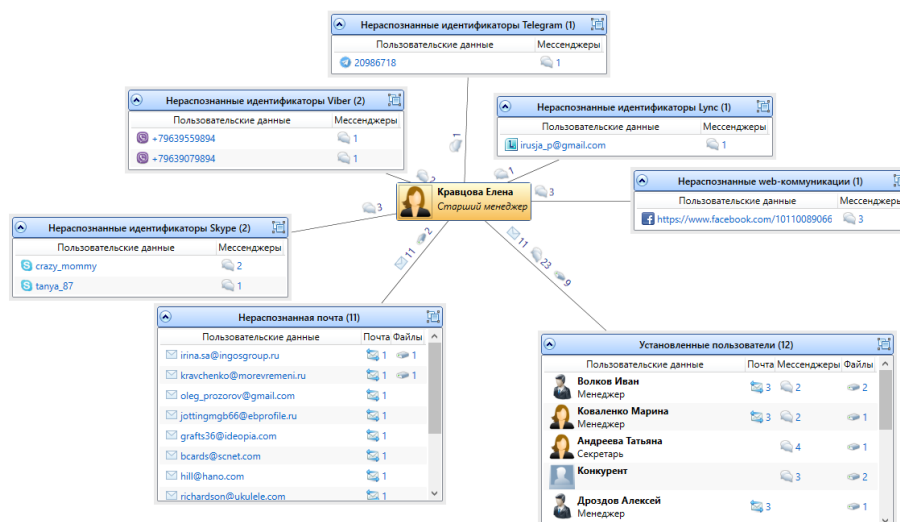
4.11 Изучите файлы, отправленные в почтовых программах за указанную дату. Для отключения отображения побочных файлов на панели инструментов вкладки **Результаты поиска** нажмите, чтобы отменить выбор, все кнопки фильтров, кроме кнопки **Почта**.



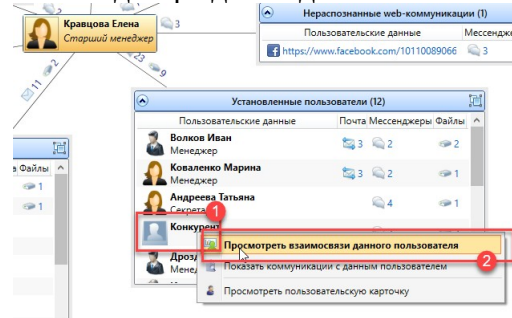
4.12 Вернитесь на вкладку **Активность пользователей**.

4.13 Выберите закладку **Взаимосвязи** на нижней панели окна **Активность пользователей**.

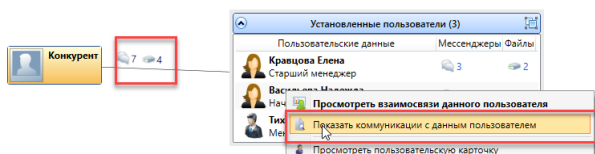
4.14 В новой вкладке изучите связи пользователя Елена Кравцова.



4.15 В таблице **Установленные пользователи** кликните правой клавишей мыши по имени **Конкурент** и выберите пункт **Просмотреть взаимосвязи** данного пользователя. Нажмите **Да** в окне подтверждения действия.



4.16 Изучите коммуникации пользователей, контролируемых системой, с пользователем **Конкурент**. Для просмотра содержимого коммуникаций, кликните правой клавишей мыши по имени пользователя из таблицы **Установленные пользователи** и выберите пункт **Показать коммуникации с данным пользователем** либо поочередно нажимайте пиктограммы в таблице или на линии взаимосвязи.



4.17 Закройте окно консоли.

4.18

Контрольные вопросы

1. Чем вызваны различия результатов поиска по ключевой фразе «высылаю резюме» при выполнении заданий на шагах 2.2 – 2.5?
2. Какие логические операторы могут применяться для создания поискового запроса при комбинированном поиске.
3. Как отрегулировать интервал. Данные за который должны быть проверены на соответствие условиям поискового запроса?
4. Возможно ли создать карточку для нового пользователя через Консоль пользователя?
5. Как быстро проверить все взаимосвязи одного пользователя с другими пользователями сети?
6. Каковы возможности компонентов консоли по отслеживанию коммуникаций с внешними контактами и их идентификации?
7. Какие виды активности пользователя отображаются в отчете о дневной активности пользователя.