falcongaze®

Кейс клиента

Нелояльность сотрудников

Утечка информации

# Утечка входящих лидов к конкурентам

Любая компания может столкнуться с утечкой конфиденциальной информации. В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось обнаружить передачу входящих лидов конкурентам, а также выявить виновного в утечке.

## Проблема

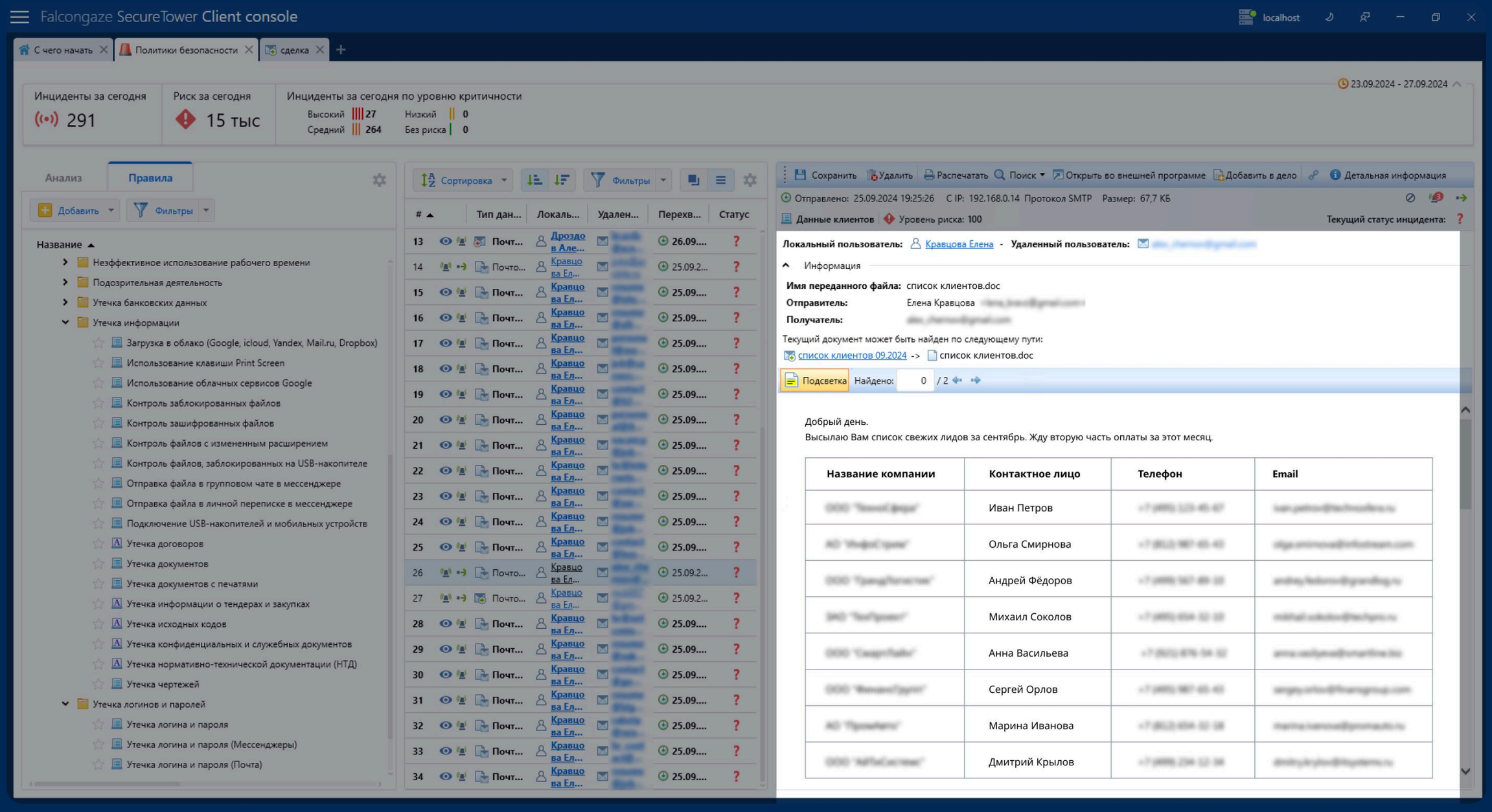
Компания, специализирующаяся на продаже CRM-систем, обнаружила существенное снижение выручки — «горячие» клиенты один за другим перестали покупать продукт. Позже выяснилось, что они приобретали систему у конкурентов по сниженной цене. Компания начала внутреннее расследование.

## Решение

Чтобы найти причину утечки лидов, компания приобрела SecureTower. Сразу после установки система начала контролировать действия менеджеров за рабочими компьютерами, в том числе действия удаленных сотрудников. Кроме того, было создано правило безопасности, которое должно было сработать, если сотрудник отправит письмо с вложением на почтовый адрес конкурентов. Помимо прочего, SecureTower анализировала:

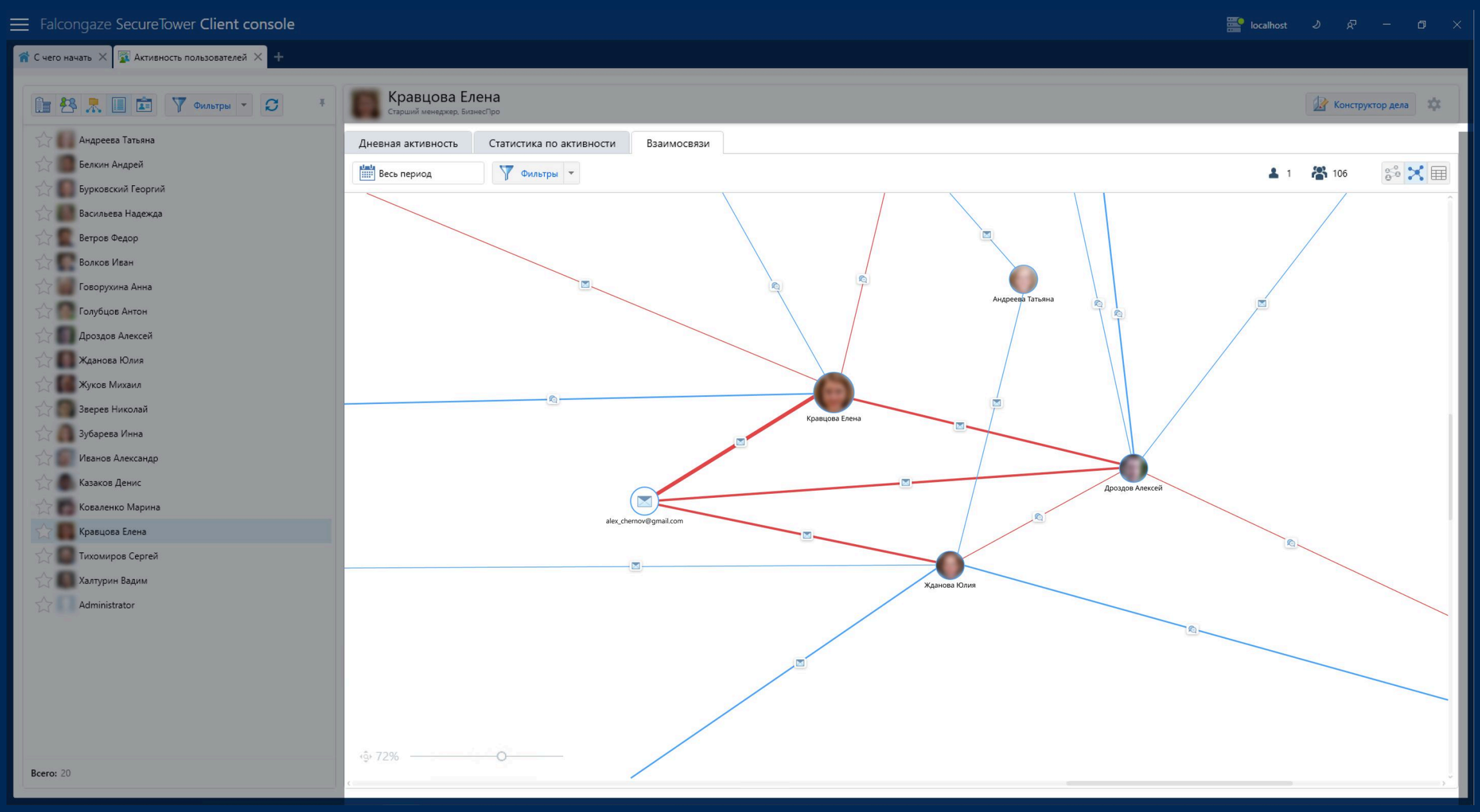
- передаваемые файлы;
- электронную почту;
- сообщения в мессенджерах;
- запускаемые приложения и проч.

Система сообщила о нарушении спустя трое суток после установки: менеджер отдела продаж отправила письмо с вложенным документом на e-mail конкурирующей организации. Используя функционал SecureTower, офицер по безопасности проанализировал содержание письма и обнаружил, что менеджер передала списки лидов неизвестному.




**Модуль «Политики безопасности» (область поиска — почта, мессенджеры)**

**На заметку!** Утечки персональных данных клиентов чреваты не только снижением числа сделок, но и штрафами от регуляторов: до 600 тысяч рублей для физлиц и до 15 миллионов для юрлиц. За повторные утечки данных для организаций предусмотрены оборотные штрафы.




Модуль «Активность пользователей» (взаимосвязи)

Менеджера уволили. Помимо этого, было установлено, что с незарегистрированным контактом вели переписку еще три менеджера из отдела продаж. Офицер безопасности выяснил это, используя функционал модуля «Активность пользователей» и инструмента «Графический анализатор». В модуле «Расследования» было создано Дело о взаимодействии с конкурентами. Добавлены все вовлеченные лица и их переписки, подтверждающие факт общения с конкурентом.

## Результат

- **Установлен факт передачи чувствительной информации**

  Были выявлены переписки и отправленные конкуренту письма, которые содержали информацию о клиентах компании.

- **Выявлены нелояльные сотрудники**

  Ряд сотрудников, замеченных в переписке с конкурентом, поставлены на особый контроль. Дело о взаимодействии с конкурентами из модуля «Расследования» добавлено в личные карточки каждого.

- **Настроена блокировка передачи конфиденциальных документов**

  Теперь SecureTower заблокирует операцию с чувствительными данными:

  - при попытке передачи по электронной почте (по протоколам SMTP, IMAP, MAPI и их шифрованным аналогам);
  - при отправке через браузеры и веб-версии электронной почты (по протоколам HTTP и HTTPS);
  - при отправке через мессенджеры (Telegram, Viber, Skype и проч.);
  - при попытке распечатать на локальных и сетевых принтерах;
  - при копировании в буфер обмена;
  - при копировании на внешние USB-устройства и проч.

- **Усилен контроль за процессом обработки лидов**

  Установлен дополнительный контроль за процессом обработки входящих лидов.

# Модули, которые были использованы:

- Политики безопасности
- Активность пользователей
- Комбинированный поиск
- Расследования

falcongaze®