

Нарушение законодательства

Утечка информации

Финансовые махинации и откаты

В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось раскрыть мошенническую схему внутри торговой компании.



Проблема

Руководство крупной торговой компании заметило сильное завышение цен на товары, что могло указывать на факт участия персонала в откатных схемах. Так как прямых доказательств мошеннических действий не было, приняли решение взять сотрудников на контроль.

Установление факта отката требует сбора доказательств, зачастую из множества источников: переписок в электронной почте и мессенджерах, подключаемых к рабочим станциям устройств с внешней памятью, отправленных на печать документов и проч.

В ходе выполнения задачи стало понятно, что установить контроль за действиями каждого сотрудника практически невозможно — особенно в крупной компании.

Решение

Для выявления мошенников была приобретена DLP-система Falcongaze SecureTower.

Система круглосуточно мониторила все каналы коммуникации, в том числе:

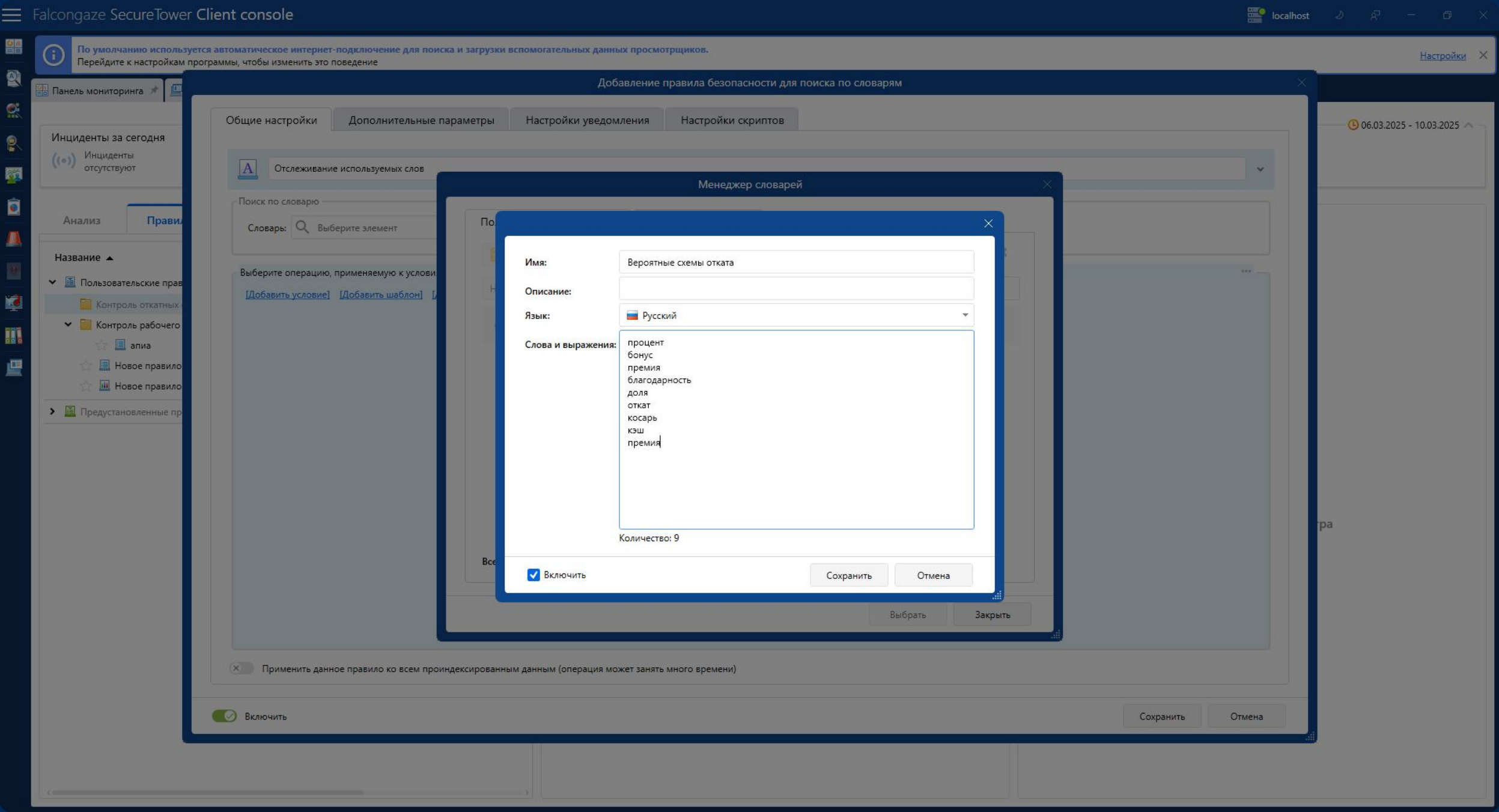
- мессенджеры и электронную почту;
- браузерную активность и поисковые запросы;
- локальные и сетевые принтеры;
- внешние USB-устройства и проч.

Также SecureTower перехватывала данные буфера обмена и кейлогера с рабочих станций.

Как правило, вероятность откатов высока в отделах, где работа подразумевает взаимодействие с контрагентами. Помимо этого, нарушителей часто прикрывают «сверху» — руководители отделов или филиалов.

Для выявления мошенников были созданы пользовательские правила безопасности, основанные на анализе всех переписок.

Новые правила реагировали на слова и словосочетания, характерные для сферы деятельности компании-клиента, а также на слова и словосочетания, которые могли указать на факт отката: «процент», «бонус», «премия», «благодарность», «доля» и иные.

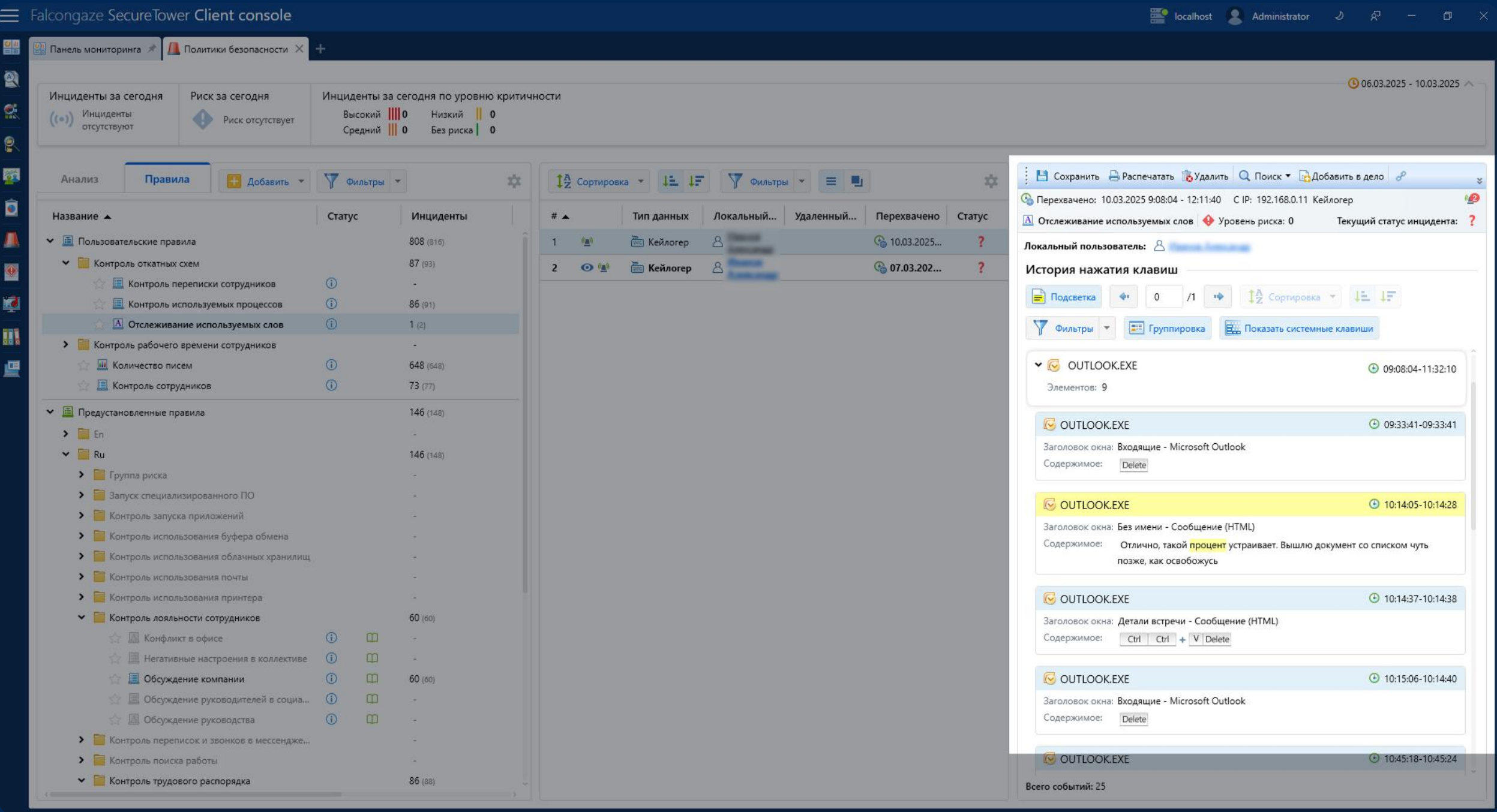


Консоль Пользователя (Настройка пользовательского словаря "Вероятные схемы отката")

На заметку! Зачастую мошенники используют в переговорах заменители слову «откат». Например, «косарь», «кэш», «благодарность», «премия», «бонус» и проч. В SecureTower вы можете создавать пользовательские словари, характерные для сферы деятельности вашей компании

Один из нарушителей — ведущий менеджер отдела материально-технического обеспечения — был выявлен следующим образом.

С помощью системы были проанализированы переписки в мессенджерах и электронной почте — ничего. Затем проанализировали кейлоггер данного сотрудника. Удалось обнаружить текстовый фрагмент «такой процент устраивает», набранный в черновике письма в некорпоративном аккаунте электронной почты. Затем черновик письма был удален.



Консоль Пользователя (Инциденты пользовательского правила безопасности для поиска по словарям "Отслеживание используемых слов")

После анализа перехваченных данных кейлоггера этого сотрудника сложилась полная картина обсуждения отката: вход был выполнен сразу с двух устройств — менеджер и контрагент авторизовались в одном аккаунте электронной почты и вели переписку в черновике.

Результат

- **Выявлен факт отката**
- **Компании удалось предотвратить финансовый ущерб**

Размер отката может достигать 20% от общей суммы сделки. При этом финансовый ущерб для компании от невыгодных торговых отношений может исчисляться сотнями миллионов рублей. В крупных компаниях размер ущерба может достигать несколько миллиардов рублей.

Модули, которые были использованы:



Политики безопасности



Агенты (консоль Администратора)

