КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

#CODEIB

ВАРИАТИВНОСТЬ ИСПОЛЬЗОВАНИЯ DLP-СИСТЕМЫ

Александр Кулик

Ведущий специалист

falcongaze

Falcongaze SecureTower

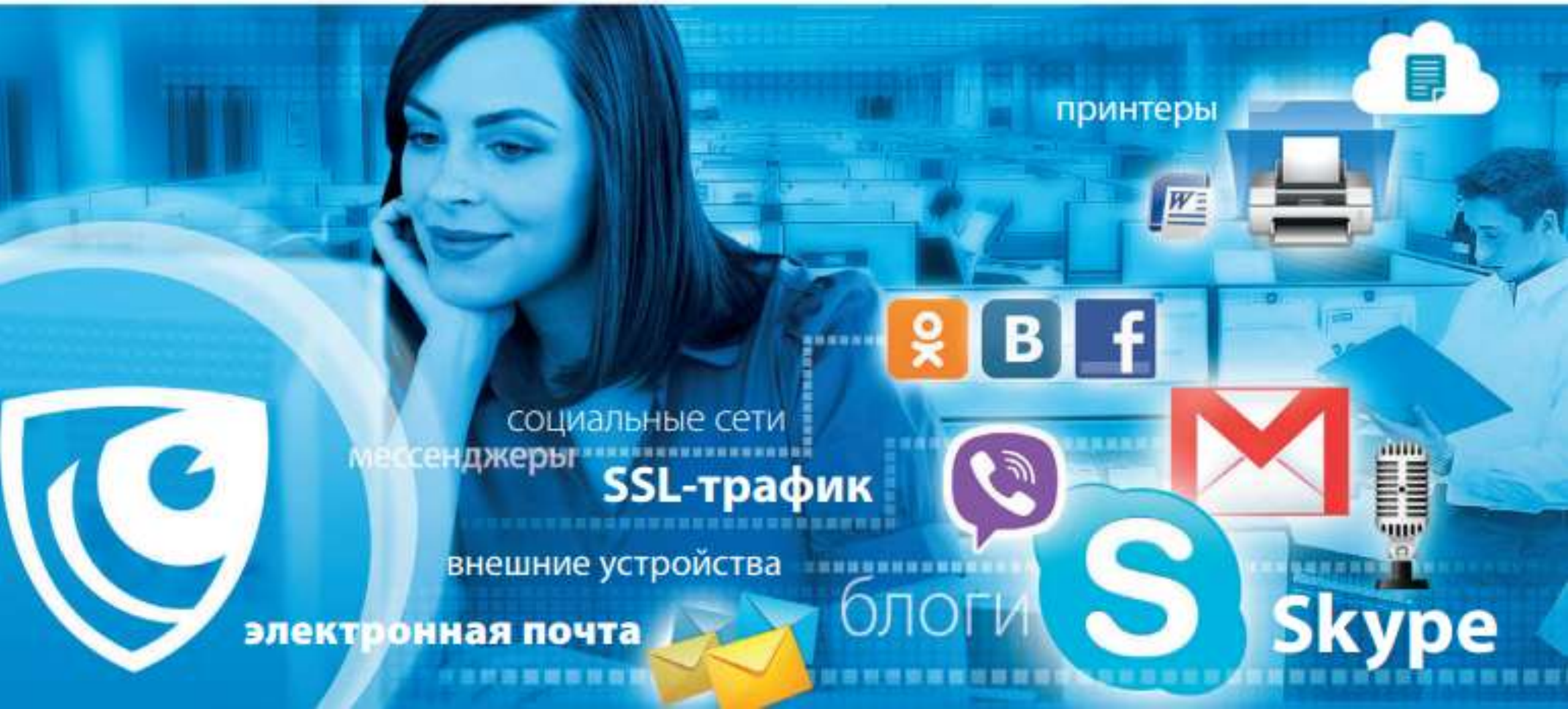
13 лет на рынке

30 стран

1000+ клиентов

falcongaze

КОНТРОЛИРУЕМЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ



90% утечек по вине персонала

50% уволенных сотрудников забирают конфиденциальные данные

«За любым внешним инцидентом стоит внутренняя ошибка»

Панкевич Иван Анатольевич,
Начальник комплаенс управления ОАО “БНБ-Банк”

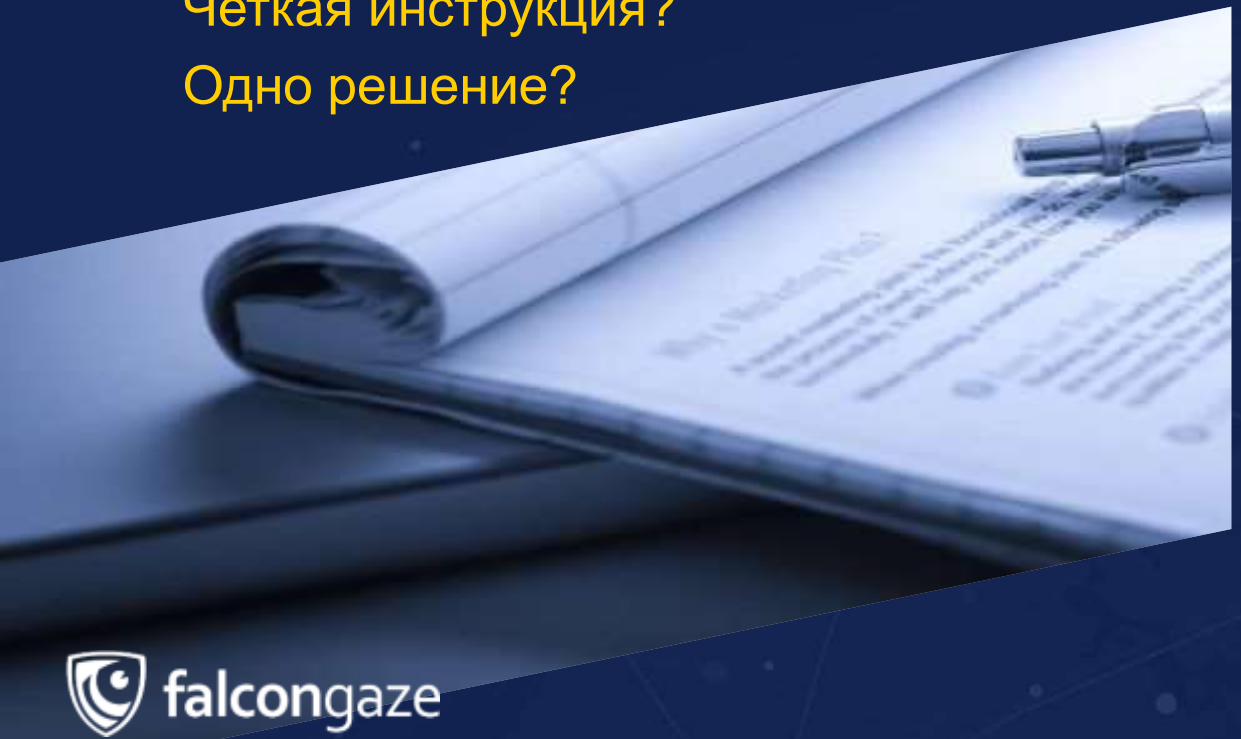
falcongaze

СУЩЕСТВУЕТ ЛИ ЕДИНСТВЕННО ВЕРНЫЙ МЕТОД?

Единое правило?

Четкая инструкция?

Одно решение?



КОМПЛЕКСНЫЙ ПОДХОД

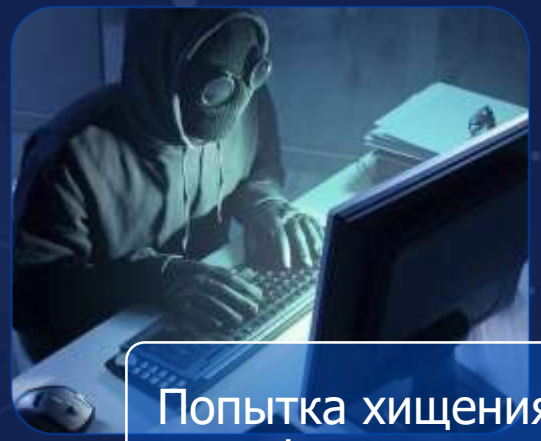
Все методы верны!
Какой выберите вы?

falcongaze

Кейс: сговор о предоставлении базы данных клиентов компании-конкуренту

Предложение от компании-конкурентов

Сговор с сотрудниками



Попытка хищения информации

falcongaze

- Правила безопасности:
  - по словарю
  - по цифровому отпечатку
  - статистические
- Граф-анализатор
- Модуль расследований

Предложение от компании-конкурентов

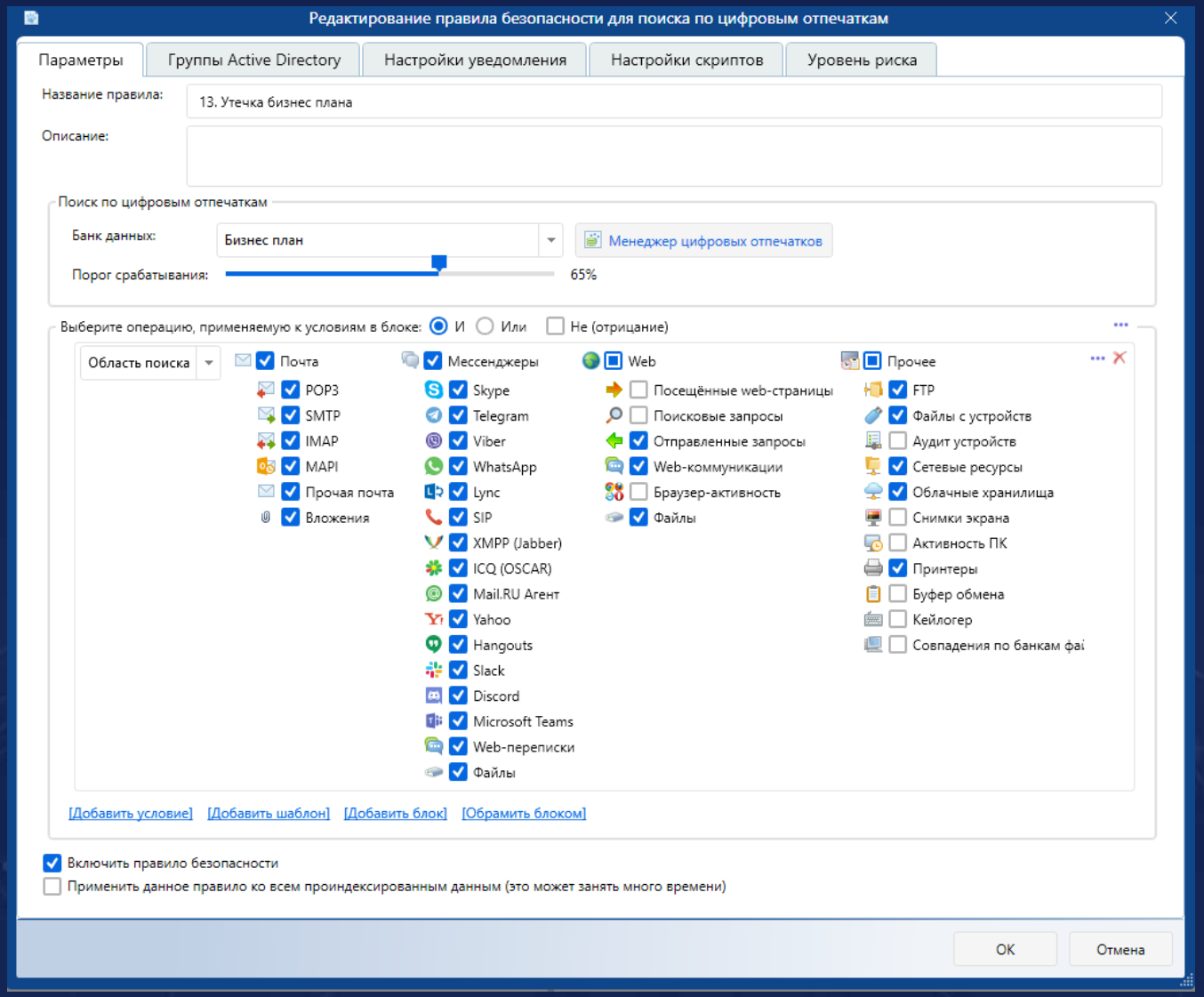
Сговор с сотрудниками

Попытка хищения информации

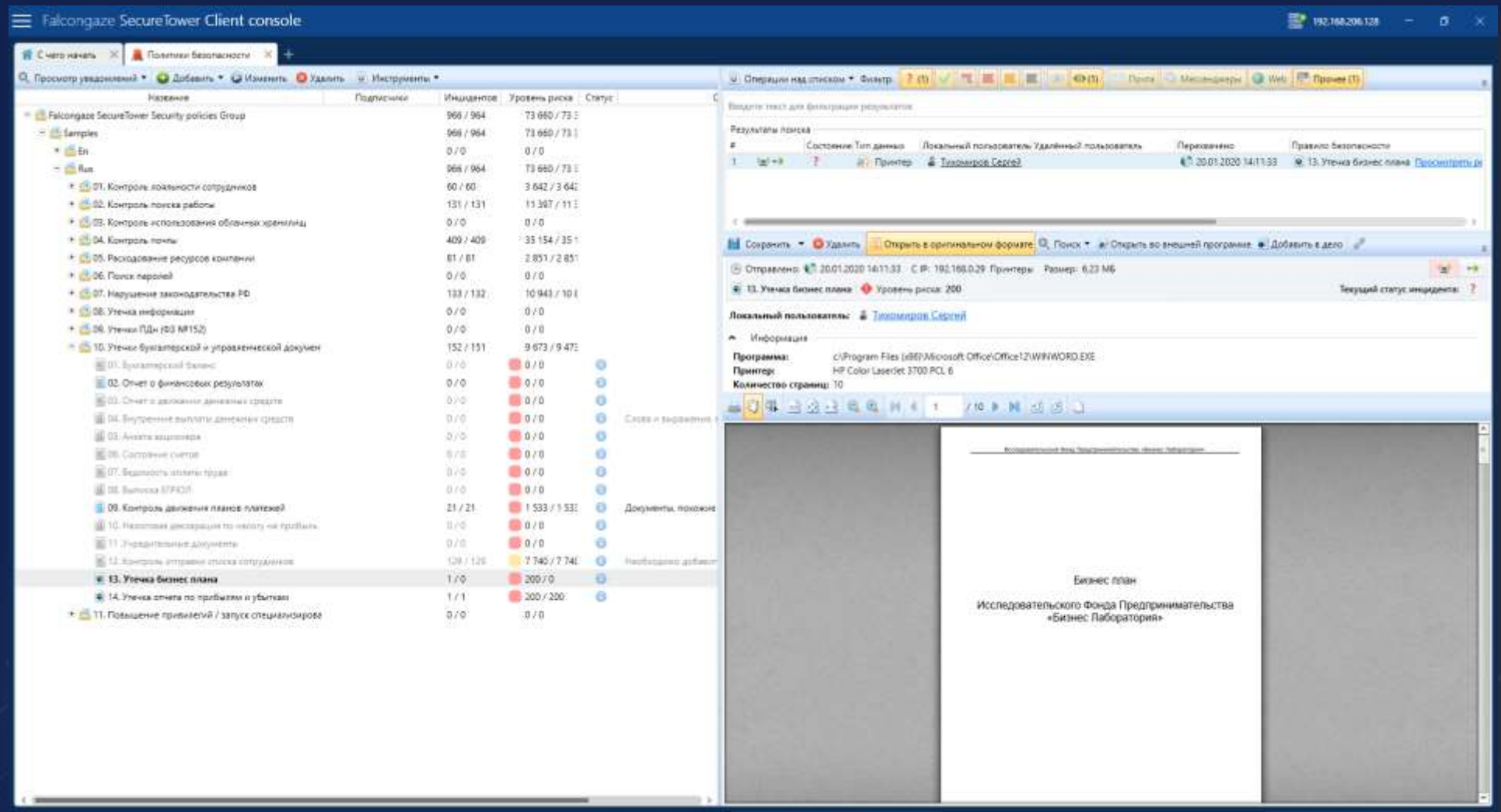
- Анализ рисков
- Поиск
- Перехват:
  - почты
  - Мессенджеры

  Голосовых сообщений (распознавание)

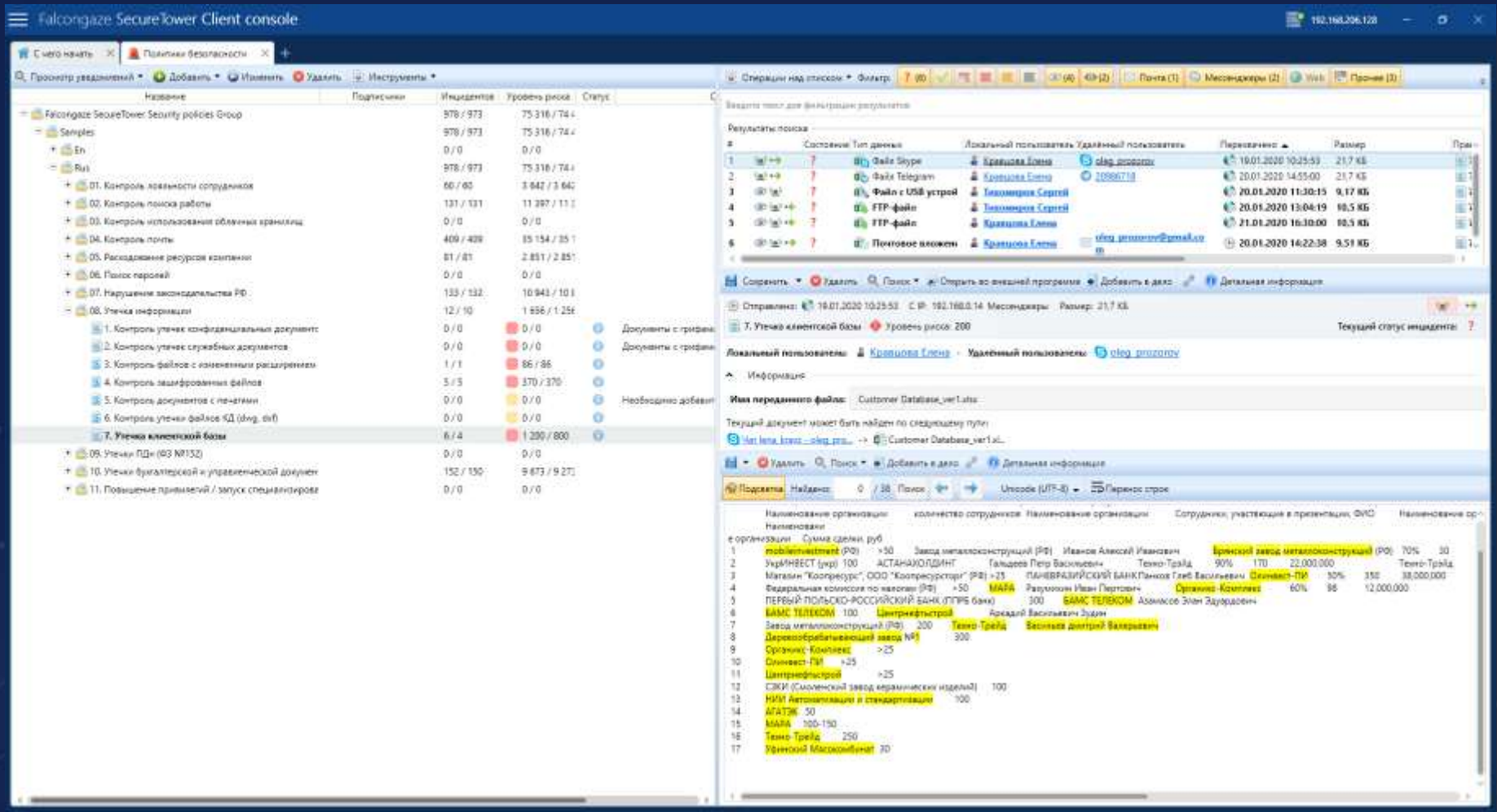
Правило безопасности – по цифровому отпечатку



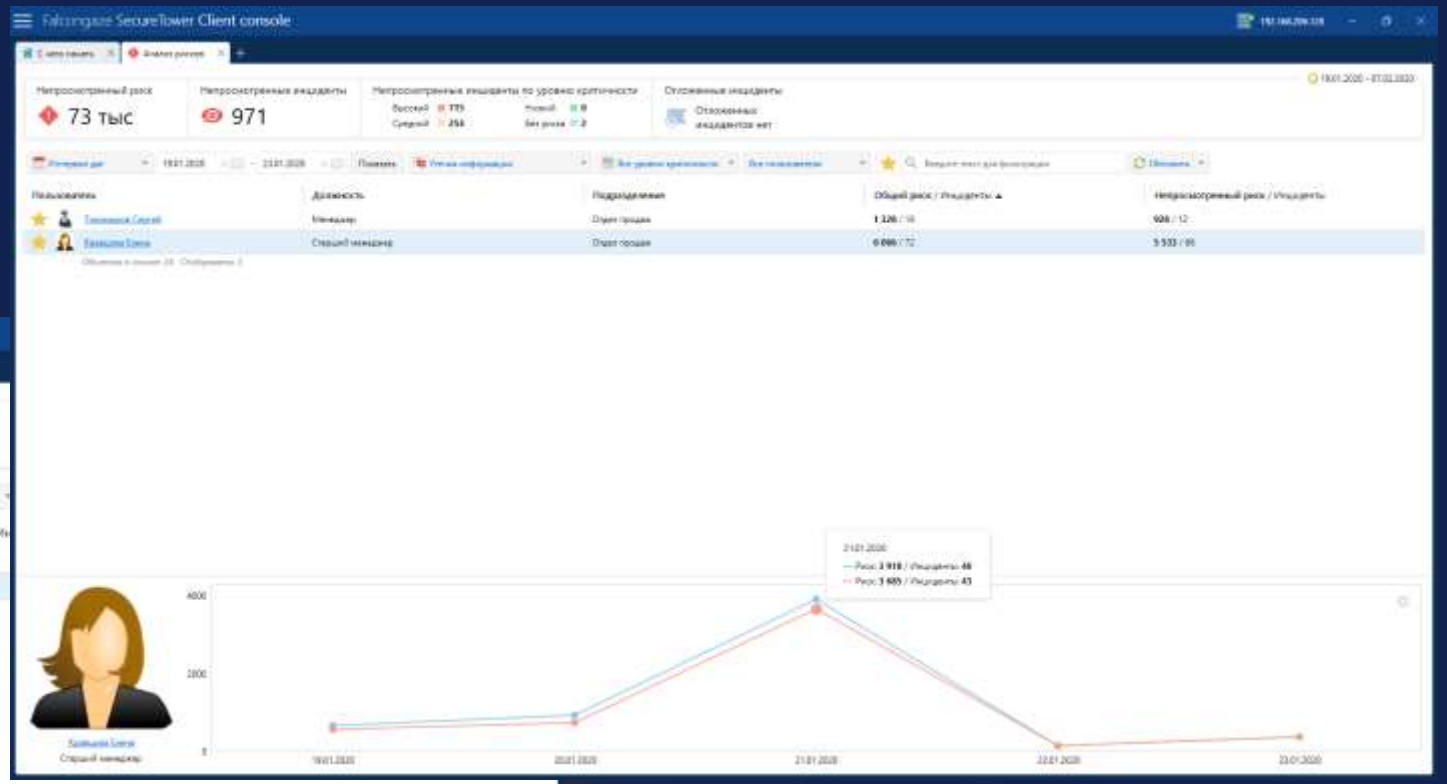
Правило безопасности – по цифровому отпечатку

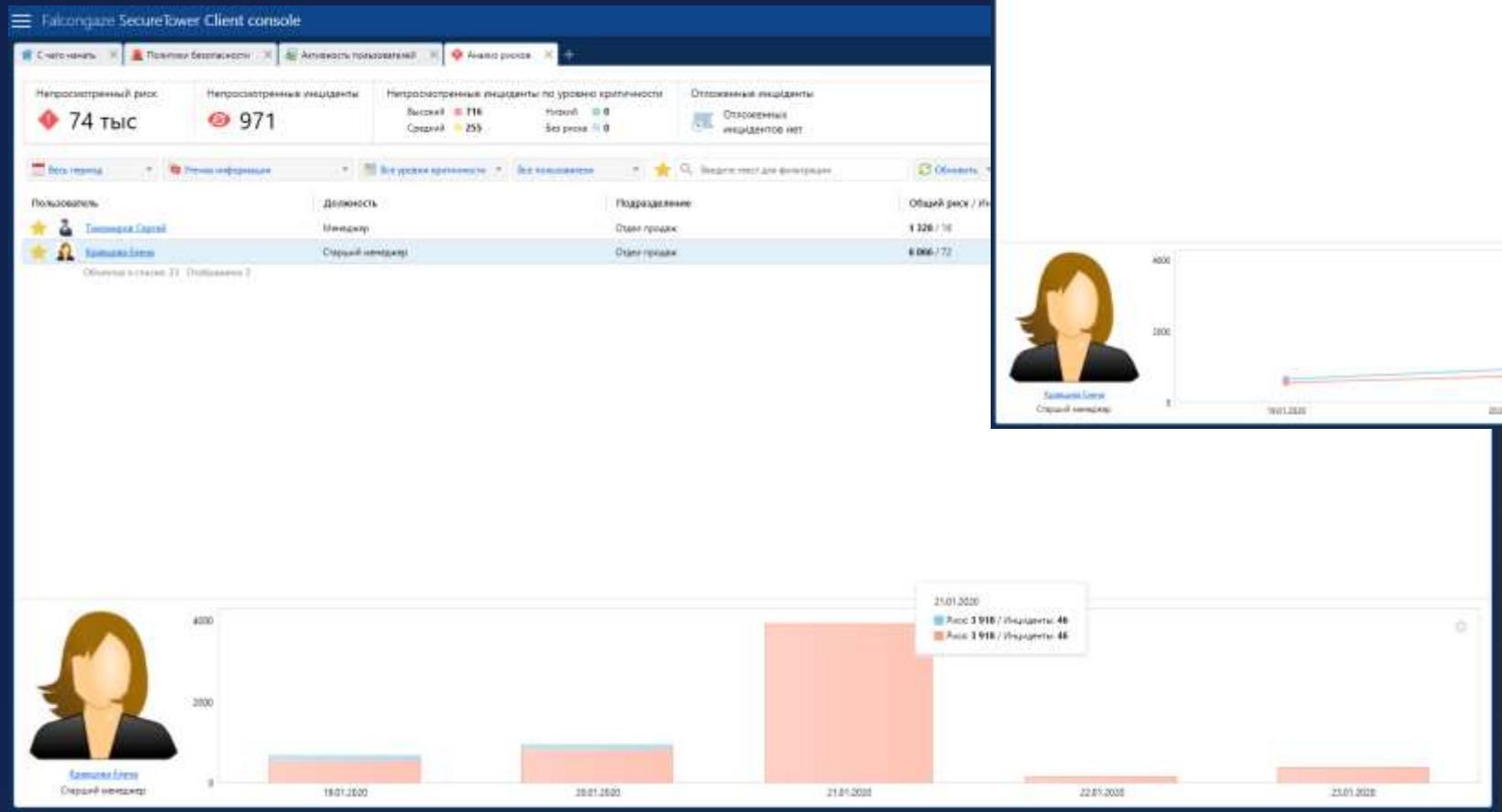


Правило безопасности – по словарю



Анализ рисков

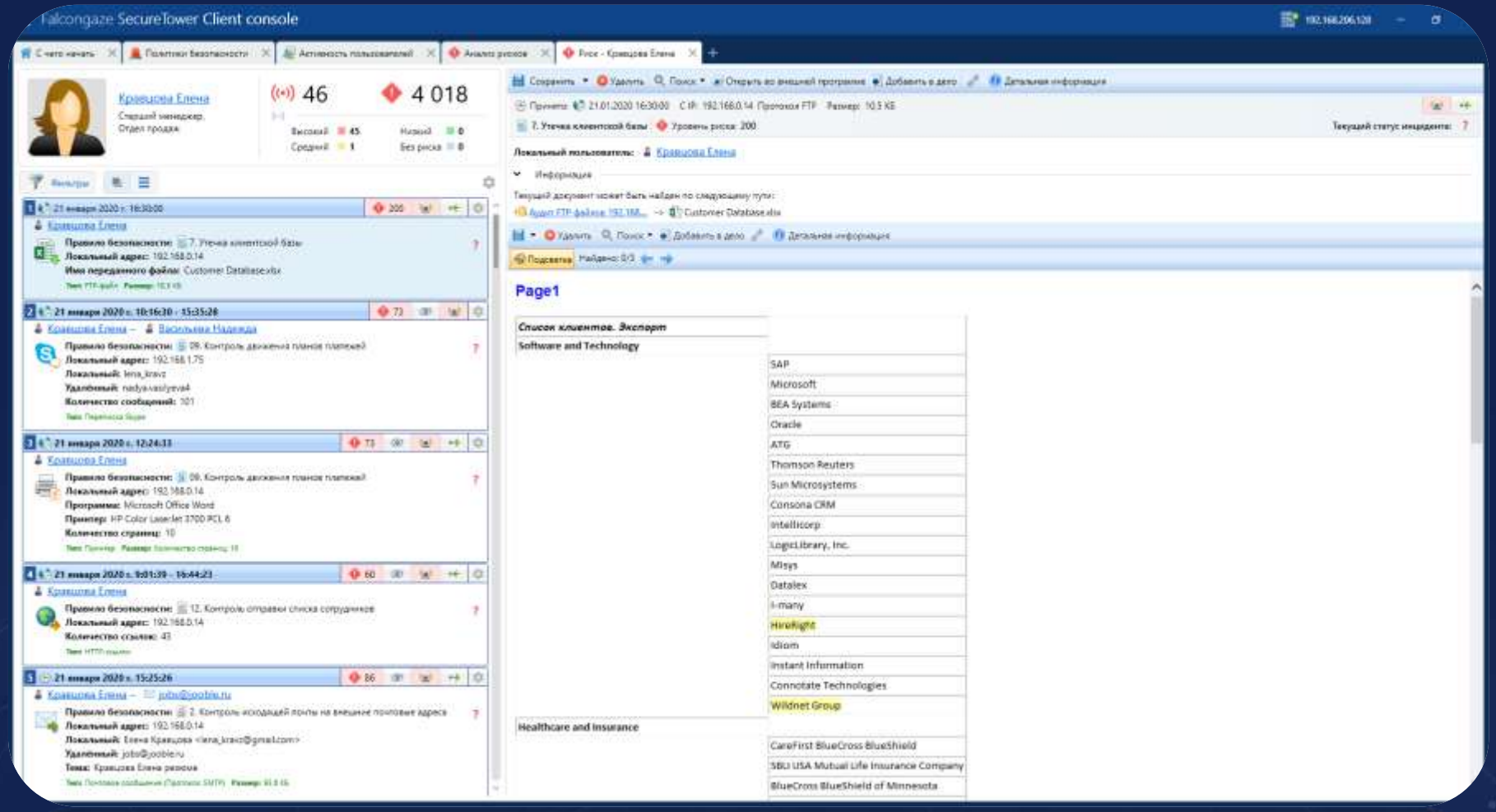




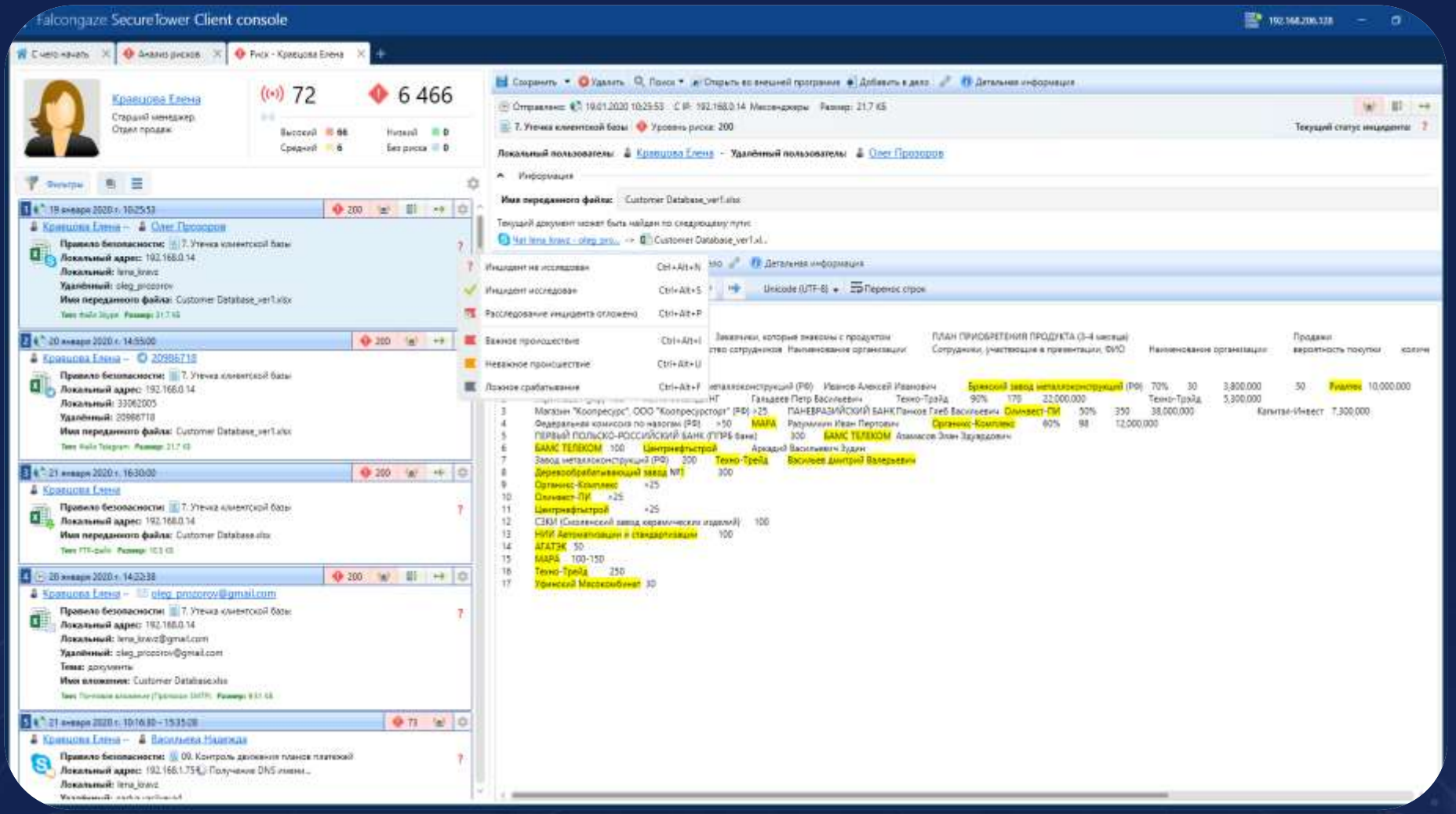
Вариативность отображения отчета

falcongaze

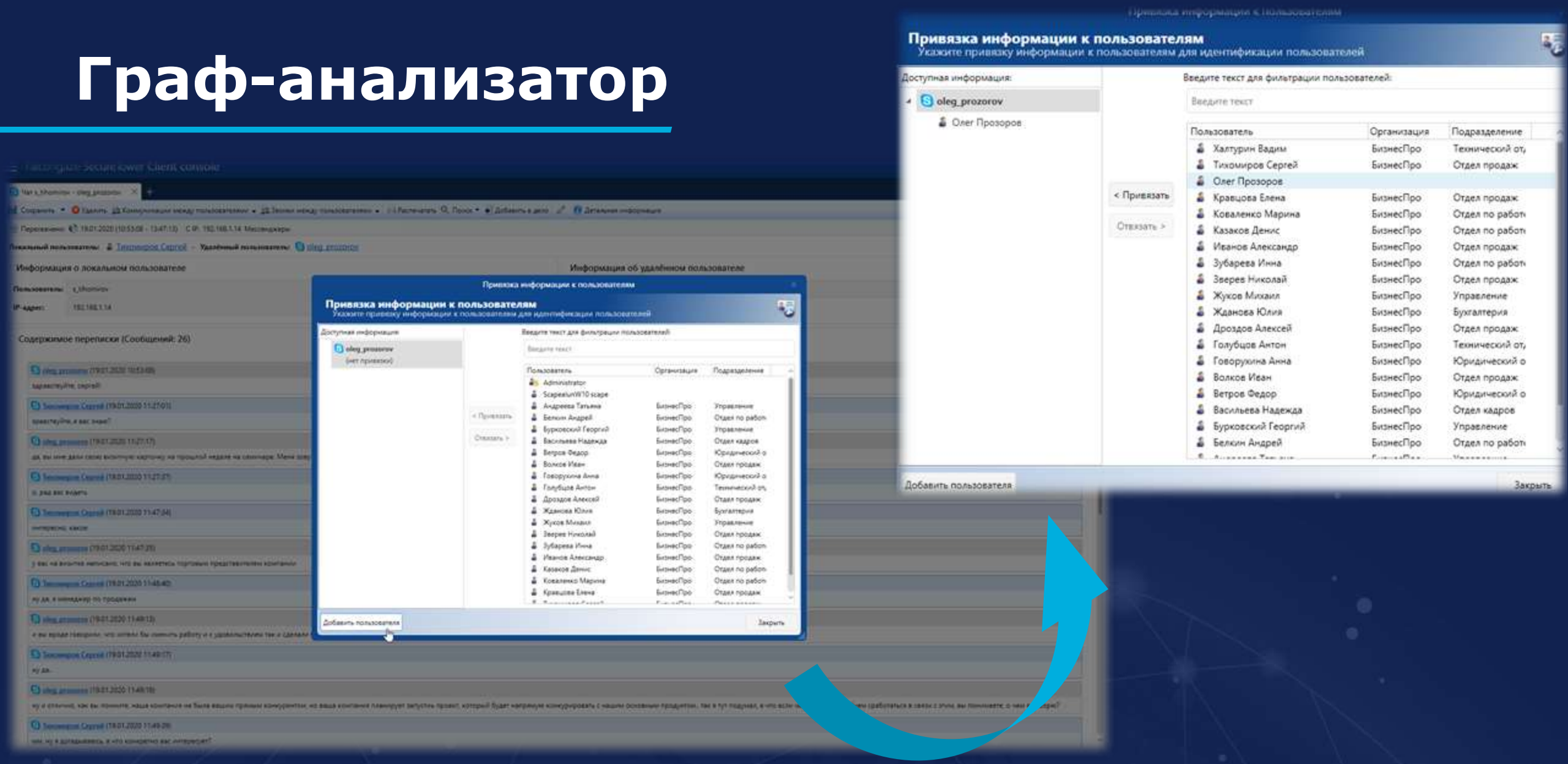
Анализ рисков



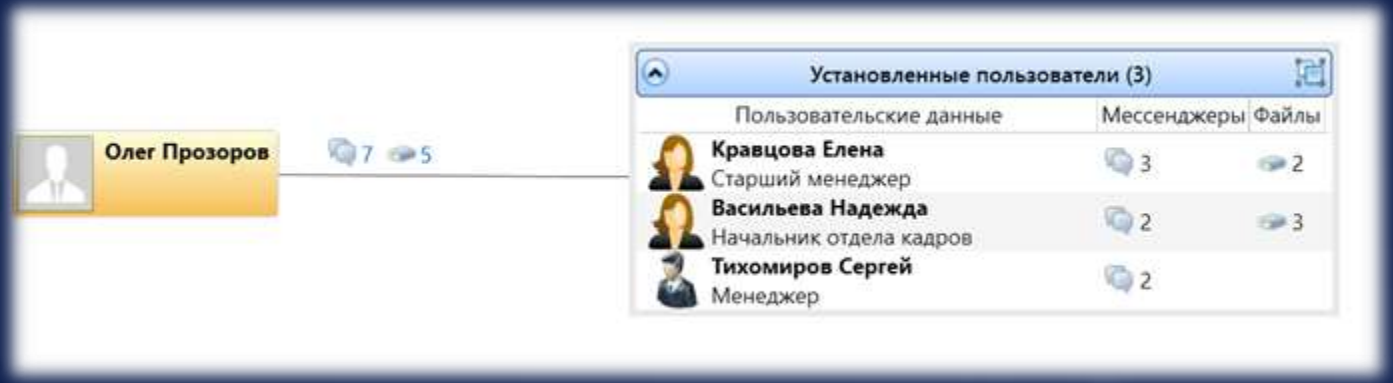
Анализ рисков



Граф-анализатор

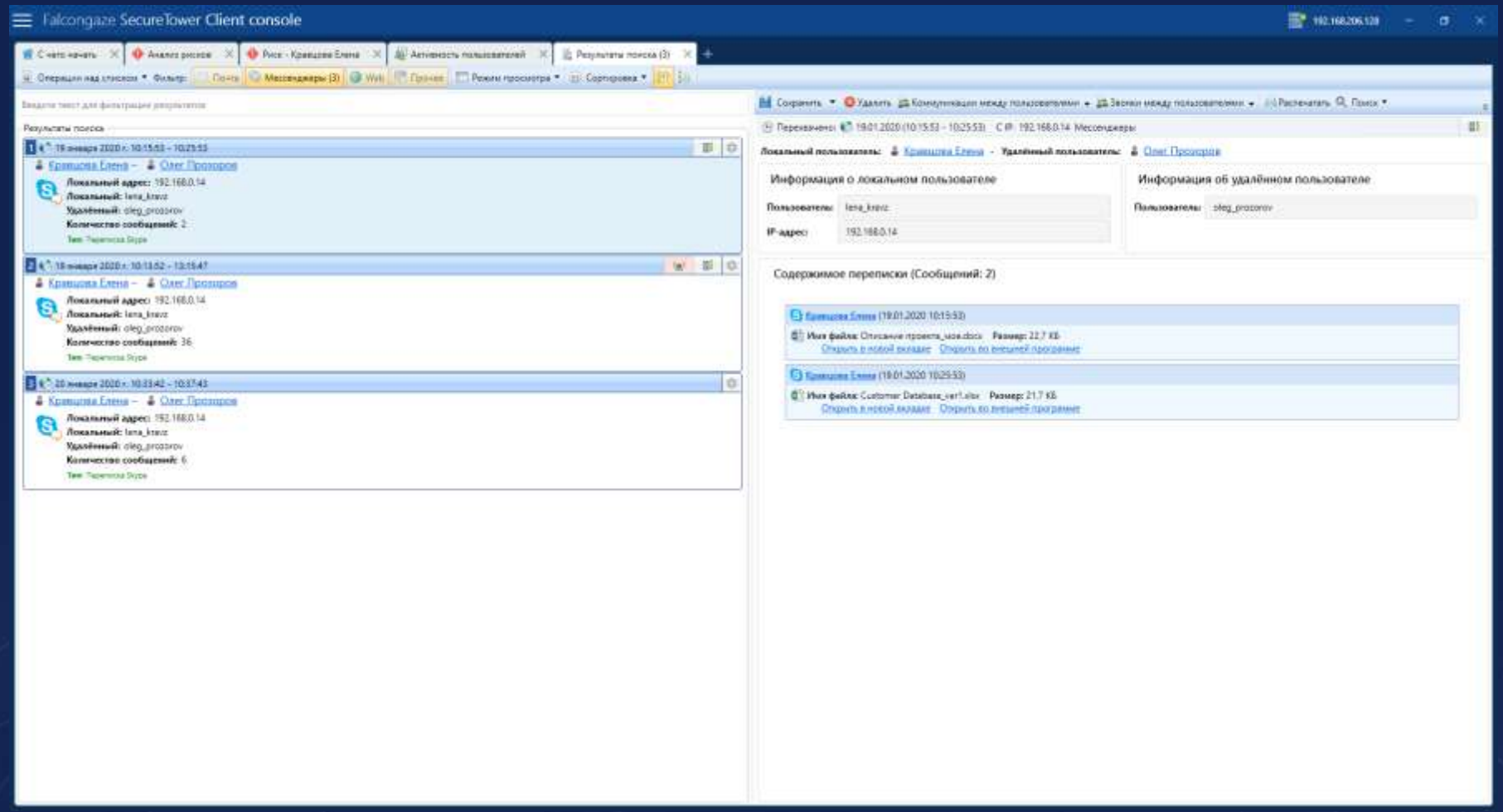


Граф-анализатор



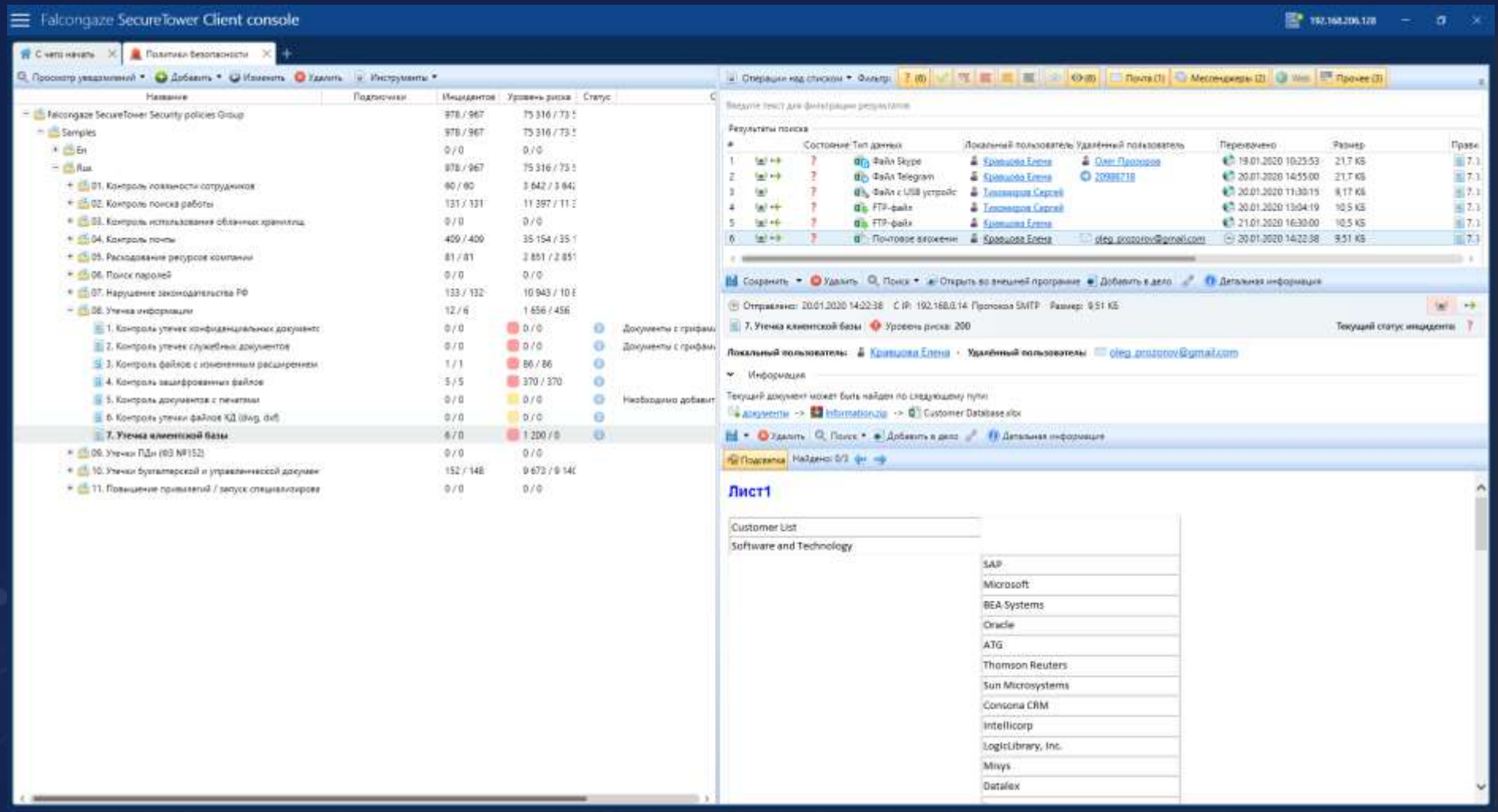
falcongaze

Граф-анализатор



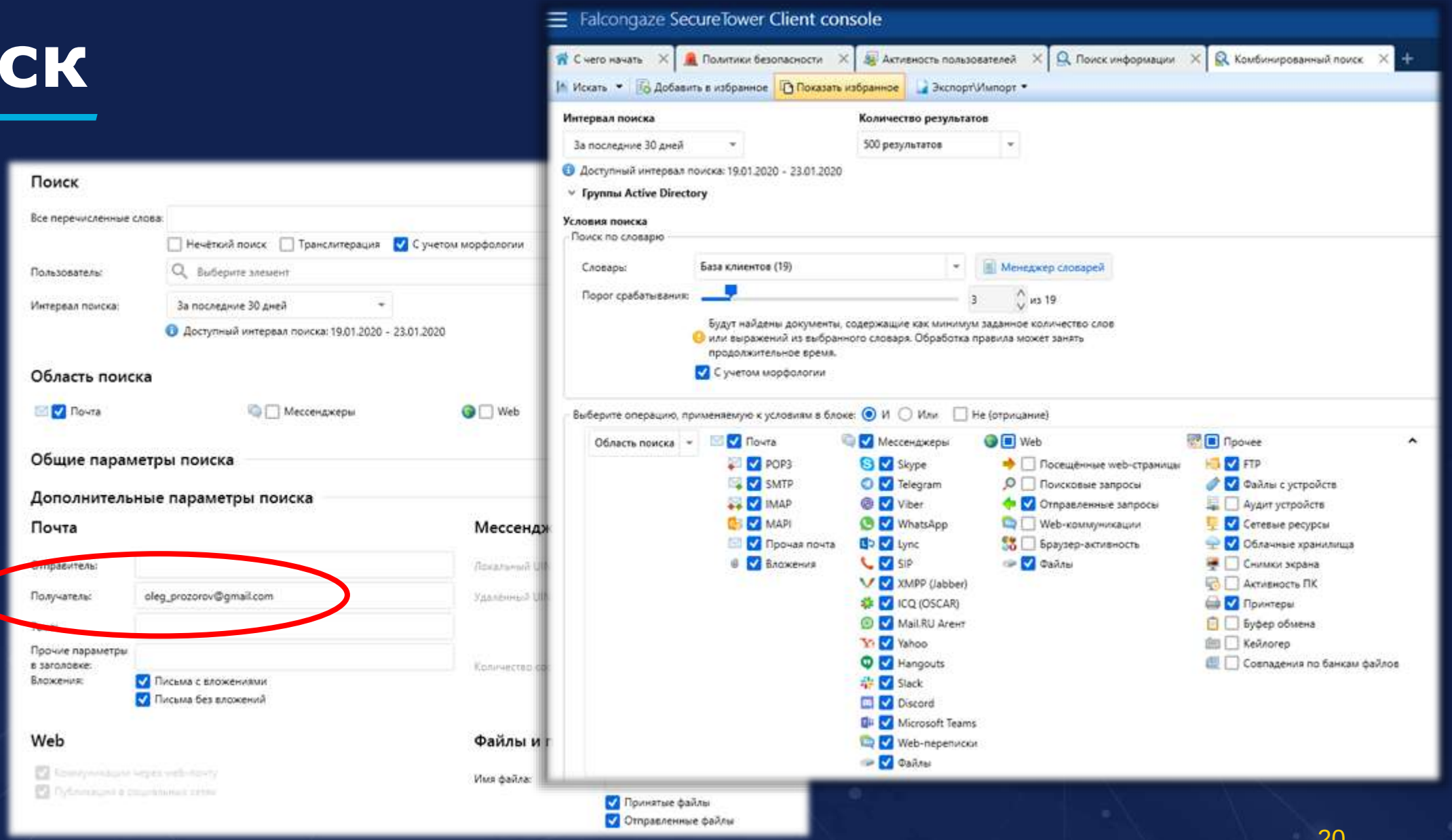
falcongaze

Перехват почты

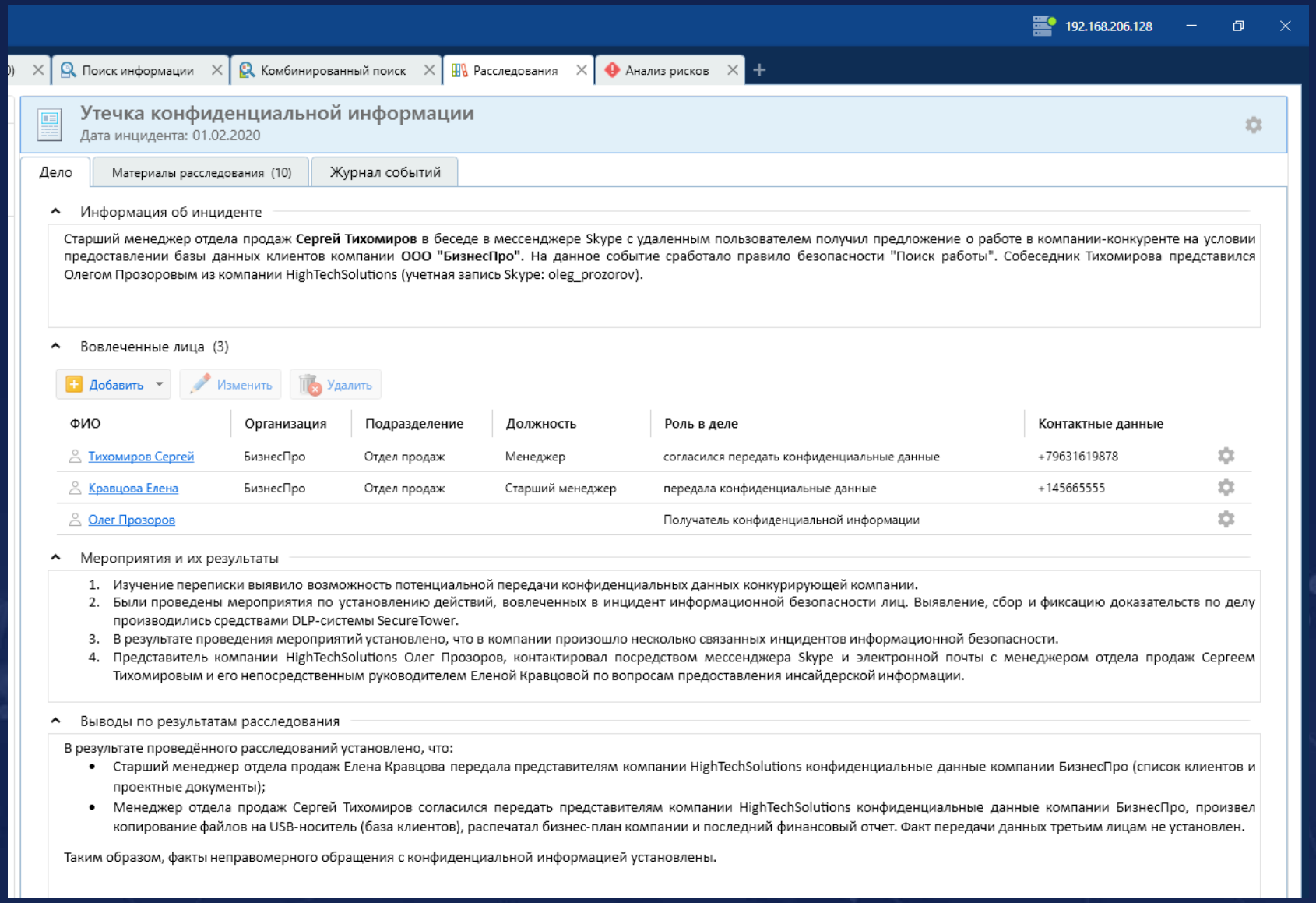


falcongaze

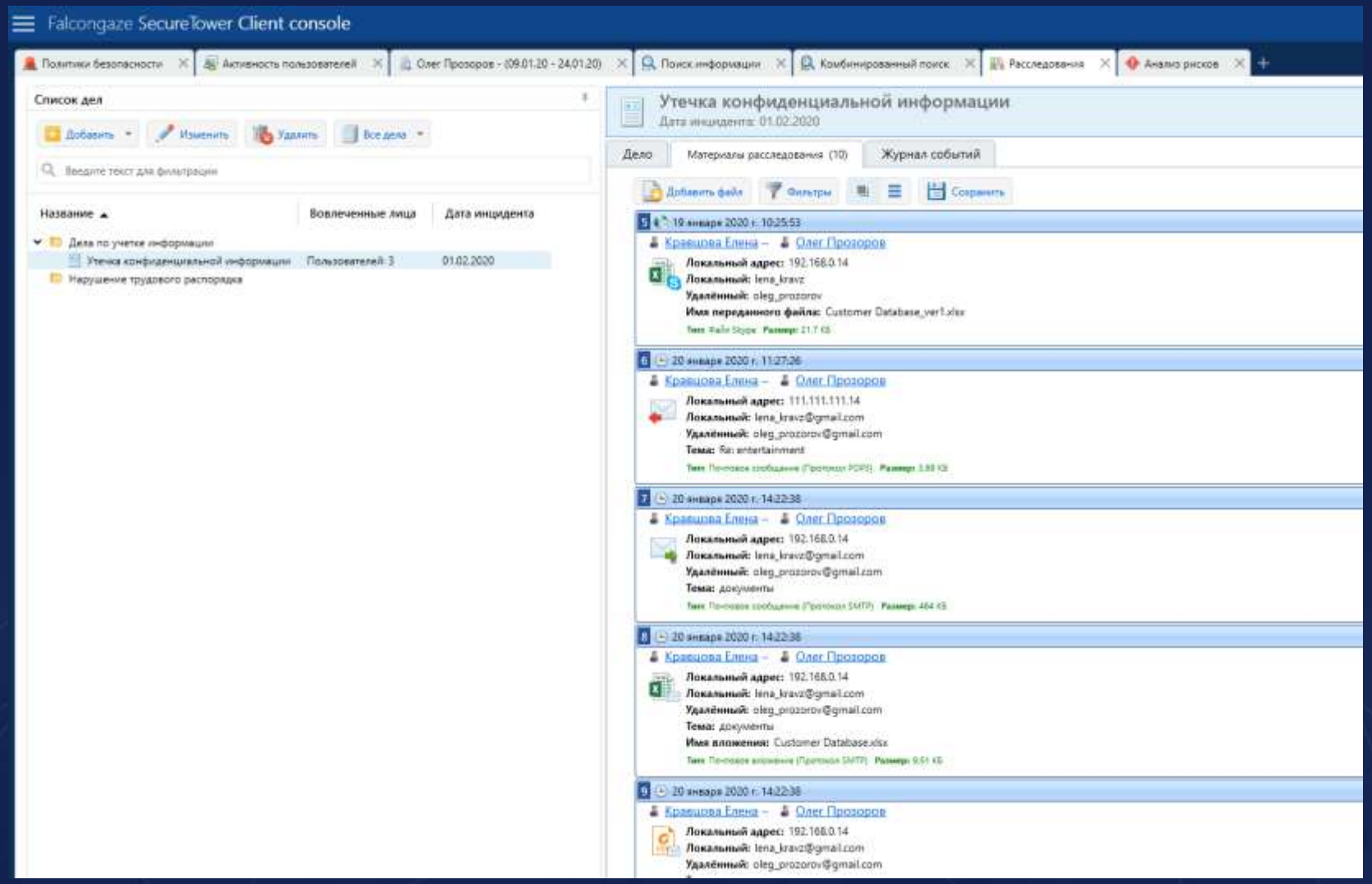
Поиск


Falcongaze SecureTower Client console
С чего начать
Политики безопасности
Активность пользователей
Поиск информации
Комбинированный поиск
Искать
Добавить в избранное
Показать избранное
Экспорт\Импорт
Интервал поиска
За последние 30 дней
Количество результатов
500 результатов
Доступный интервал поиска: 19.01.2020 - 23.01.2020
Группы Active Directory
Условия поиска
Поиск по словарю
Словари:
База клиентов (19)
Менеджер словарей
Порог срабатывания:
3
из 19
Будут найдены документы, содержащие как минимум заданное количество слов или выражений из выбранного словаря. Обработка правила может занять продолжительное время.
С учетом морфологии
Выберите операцию, применяемую к условиям в блоке:
И
Или
Не (отрицание)
Область поиска
Почта
POP3
SMTP
IMAP
MAPI
Прочая почта
Вложения
Мессенджеры
Skype
Telegram
Viber
WhatsApp
Lync
SIP
XMPP (Jabber)
ICQ (OSCAR)
Mail.RU Агент
Yahoo
Hangouts
Slack
Discord
Microsoft Teams
Web-переписки
Файлы
Web
Посещённые web-страницы
Поисковые запросы
Отправленные запросы
Web-коммуникации
Браузер-активность
Файлы
Прочее
FTP
Файлы с устройств
Аудит устройств
Сетевые ресурсы
Облачные хранилища
Снимки экрана
Активность ПК
Принтеры
Буфер обмена
Кейлогер
Совпадения по банкам файлов
Поиск
Все перечисленные слова:
Нечёткий поиск
Транслитерация
С учетом морфологии
Пользователи:
Выберите элемент
Интервал поиска:
За последние 30 дней
Доступный интервал поиска: 19.01.2020 - 23.01.2020
Область поиска
Почта
Мессенджеры
Web
Общие параметры поиска
Дополнительные параметры поиска
Почта
Получатели:
oleg_prozorov@gmail.com
Прочие параметры в заголовке:
Вложения:
Письма с вложениями
Письма без вложений
Web
Принятые файлы
Отправленные файлы

Модуль расследований



Модуль расследований



falcongaze

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

АЛЕКСАНДР КУЛИК
a.kulik@falcongaze.ru
+7(962)8568588