DLP система

Falcongaze® SecureTower®

как инструмент безопасности бизнеса

Роман Клименко

руководитель регионального представительства

О компании

Компания Falcongaze разрабатывает технологии и DLP-систему для защиты компаний от утечек конфиденциальной информации и обеспечения контроля эффективности и лояльности сотрудников. Главный продукт компании — DLP-система SecureTower



19

19 лет обеспечиваем информационную безопасность



1000000

около 1 000 000 компьютеров под защитой



1000

более 1000 клиентов в 20 странах



200

200 сотрудников, объединенных общей целью — сделать бизнес безопаснее

Наши клиенты

- Государственные учреждения
- Банковский и финансовый сектор
- Энергетика
- Торговые компании
- Телекоммуникация
- Промышленность
- Транспорт и логистика
- Научно-исследовательские центры
- Высокие технологии

Предотвратить утечку дешевле, чем устранять последствия

Что вас ожидает:

- Штрафы регуляторов, проверки, санкции
- Судебные иски, выплаты компенсаций
- Восстановление ИТ-инфраструктуры и бизнес-процессов
- Восстановление информационного актива
- Репутационные потери

Круглосуточный мониторинг действий сотрудников

Позволяет оперативно выявлять нарушения политик безопасности и трудовой дисциплины сотрудниками — независимо от их месторасположения



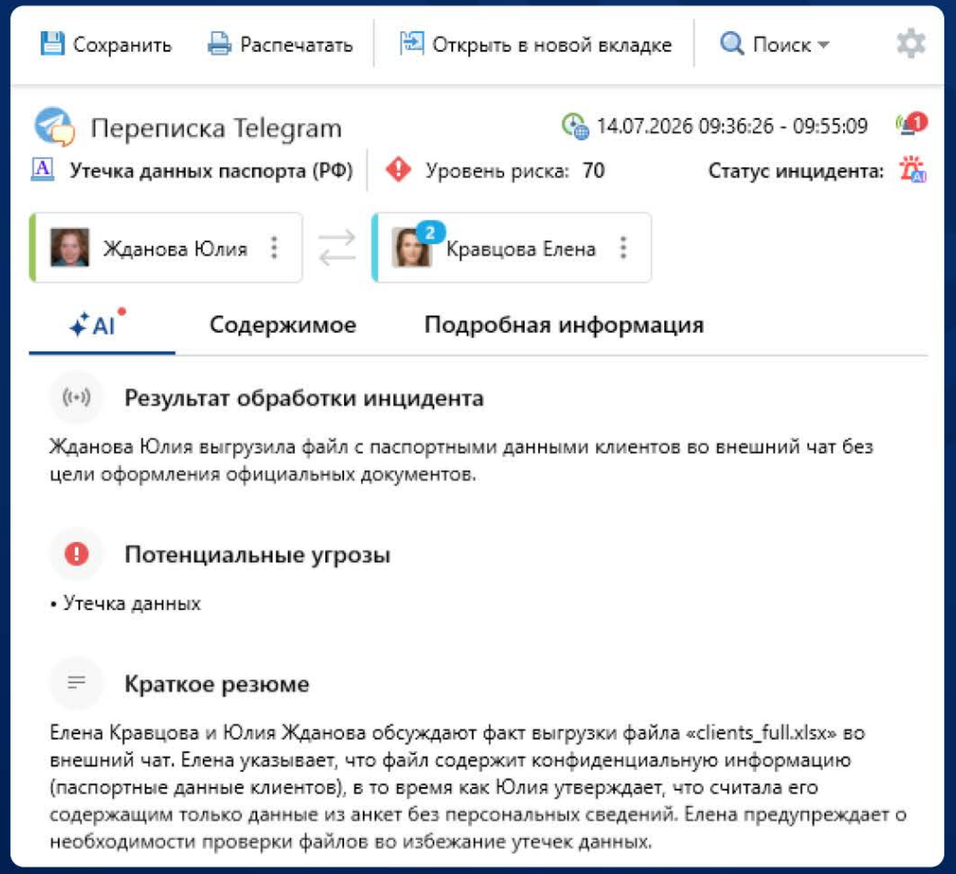
AI-функционал для анализа данных



Позволяет анализировать различные форматы файлов, включая документы и почтовые сообщения. AI выявляет потенциальные угрозы, формирует краткое содержание и помогает специалистам по безопасности быстрее анализировать инциденты

AI-обработка инцидентов

Позволяет автоматически проверять инциденты с помощью AI.
Поддерживает два режима работы: автоматическую установку статусов инцидентов и фильтрацию ложных срабатываний с уведомлением об опасных событиях



DCAP

- Позволяет выявлять случаи неправомерного хранения конфиденциальной информации и управлять хранением данных.

- Отображает статистику всех хранимых данных по типам файлов, классам и уровням критичности документов.

Мониторинг систем хранения в автоматическом режиме

Полный анализ содержимого хранимых данных

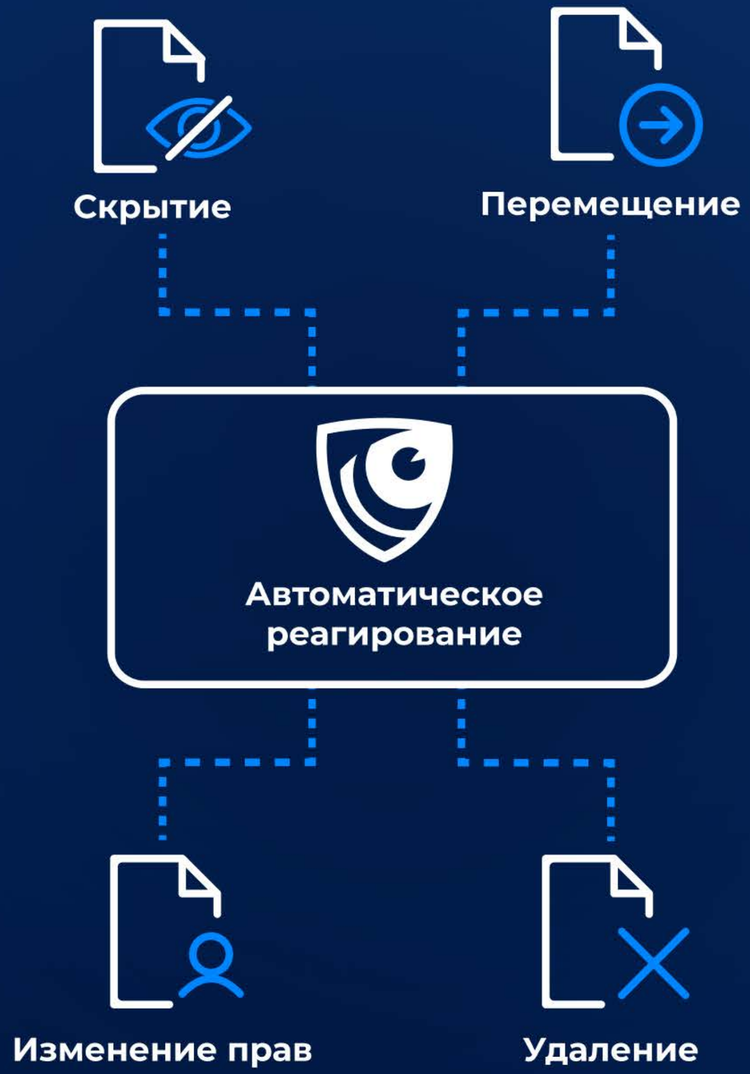
Автоматическая классификация данных

Настройка уровня критичности документа

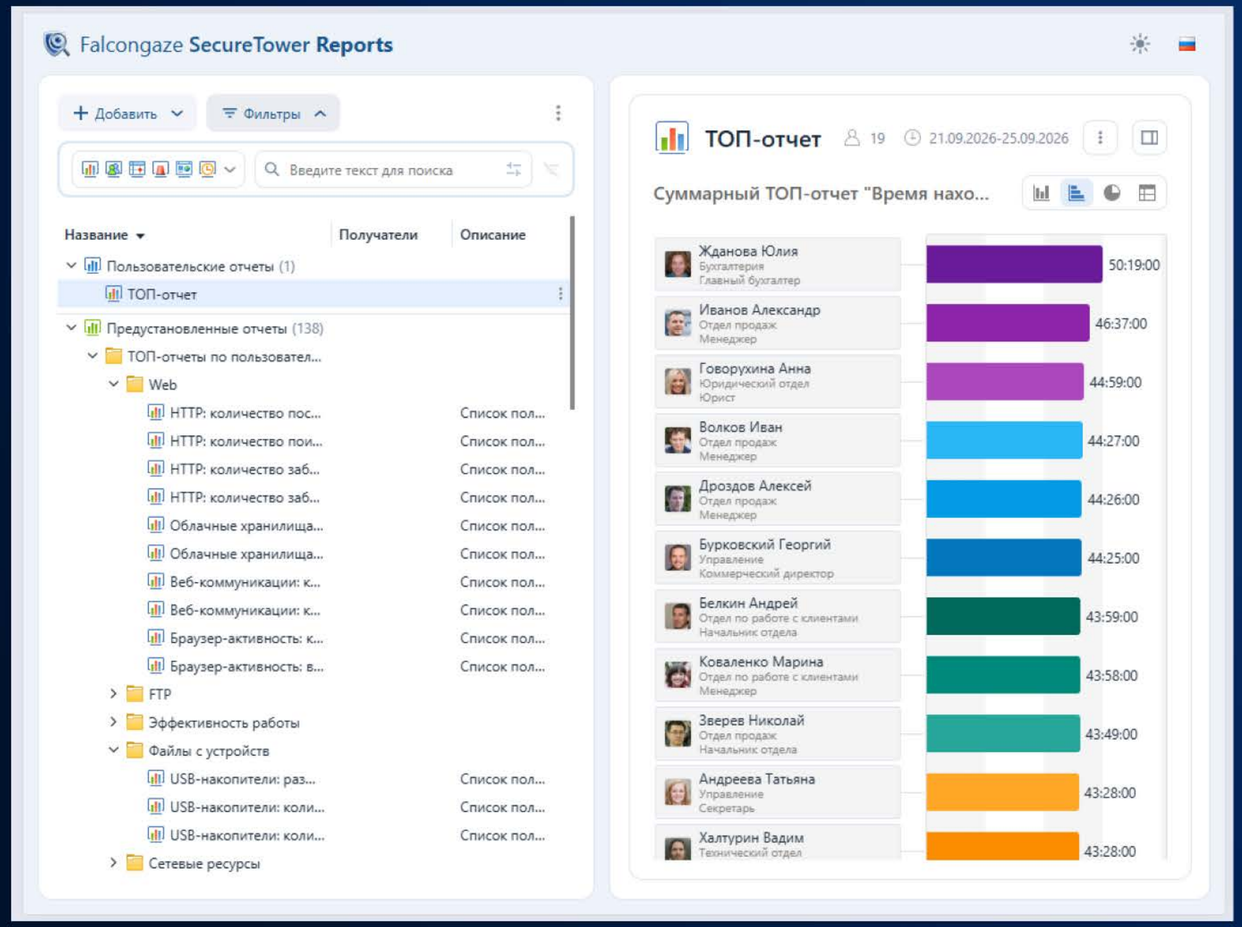
Бесшовная интеграция с SecureTower DLP

Создание инцидента при нарушении хранения данных

Уведомление сотрудника службы безопасности



Веб-консоль



- Управление всеми отчетами SecureTower из нашей веб-консоли

- Не требует установки консолей управления

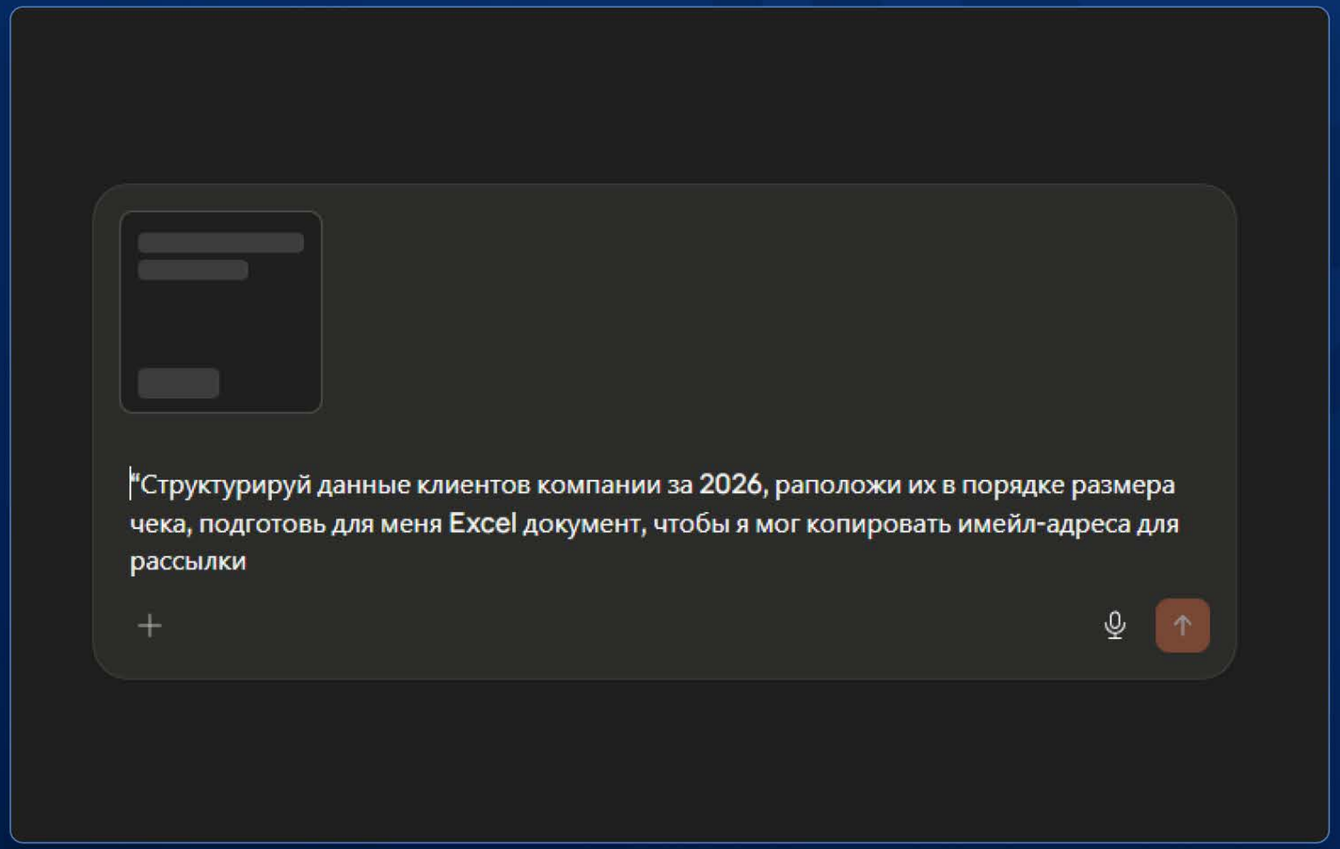
- Работа с отчетами на любых устройствах независимо от операционной системы

Перехват ИИ

- Перехват всех данных, отправляемых в ИИ-сервисы

- Поддержка наиболее популярных ИИ-инструментов

- Широкий набор инструментов анализа, в том числе при помощи ИИ-инструментов, когда ИИ контролирует ИИ



Другие улучшения системы SecureTower

- Новые каналы контроля на macOS
- Блокировка сетей WiFi
- Сохранение истории местоположений
- Уведомления об установленном местоположении
- Расширенные возможности распознавания речи
- Уведомления об отклонениях от конфигурации ПК

Выявление пользователей, представляющих наибольший риск



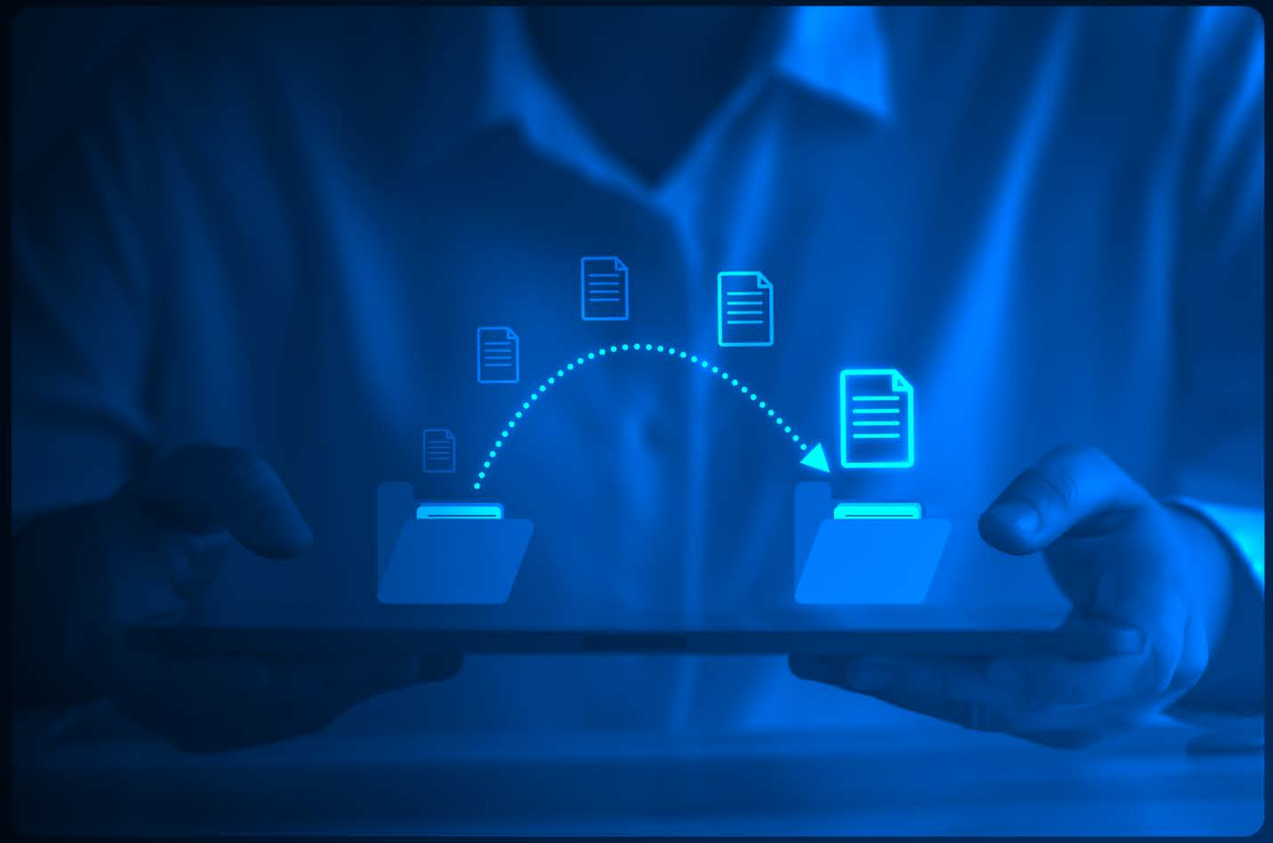
Позволяет устанавливать дополнительный контроль за сотрудниками, которые нарушают ИБ-политики, трудовой распорядок, или готовятся покинуть компанию в скором времени

Мониторинг движения данных внутри корпоративной сети

Позволяет выявлять наиболее часто используемые каналы передачи данных и усиливать контроль за ними через корректировку политик безопасности



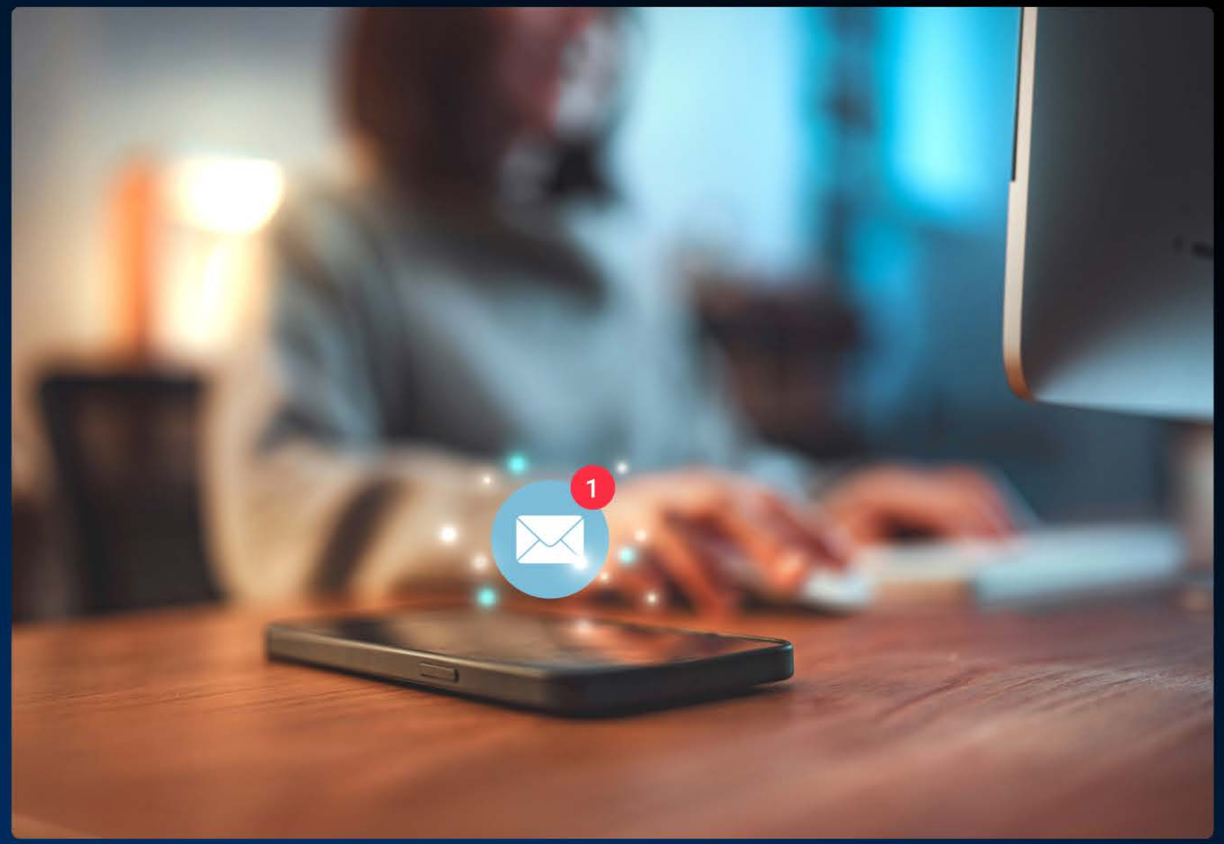
Поиск копий конфиденциальных документов



Позволяет дистанционно удалять, копировать, перемещать, скрывать копии документов на компьютерах персонала

Мгновенное реагирование на нарушения

Позволяет мгновенно оповещать уполномоченных сотрудников по удобному каналу, в том числе через Telegram, автоматически блокировать нежелательные операции с документами

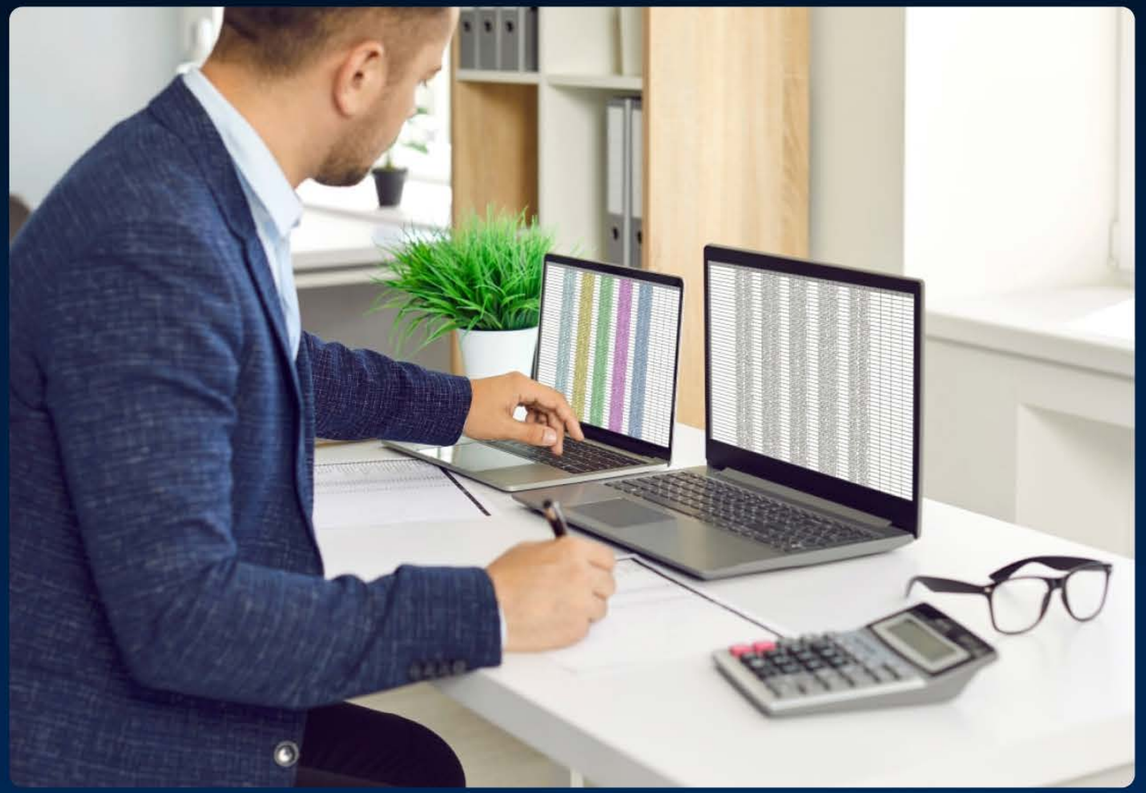


Кейс 1

falcongaze

Нелояльность сотрудников | Утечка информации | Высокие технологии

Предотвращение хищения данных о клиентах компании



В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось выявить факты нарушения трудового распорядка и предотвратить попытку хищения данных о клиентах компании.

Проблема

Склады и офисы компании-клиента распределены по всей России, и контролировать соблюдение трудового распорядка в подразделениях довольно проблематично. Помимо этого, за годы работы на рынке была собрана обширная горячая клиентская база, выстроены отношения с поставщиками.

Кейс 1

falcongaze

Решение

Для защиты данных от утечек и контроля за активностью персонала компания приобрела SecureTower.

Система перехватывала данные в большинстве каналов коммуникации. Помимо этого, она мониторила активность сотрудников: начало и завершение работы, контроль запускаемых приложений, время простоя компьютера и проч.

Удалось подтвердить, что несколько сотрудников нарушали трудовой распорядок: ежедневно опаздывали, уходили раньше, решали свои личные вопросы в рабочее время.

Также SecureTower зафиксировала факт копирования нескольких больших фрагментов данных о клиентах в текстовый документ облачного хранилища.
Попытка копирования была пресечена заранее настроенным правилом блокировки.

Результат

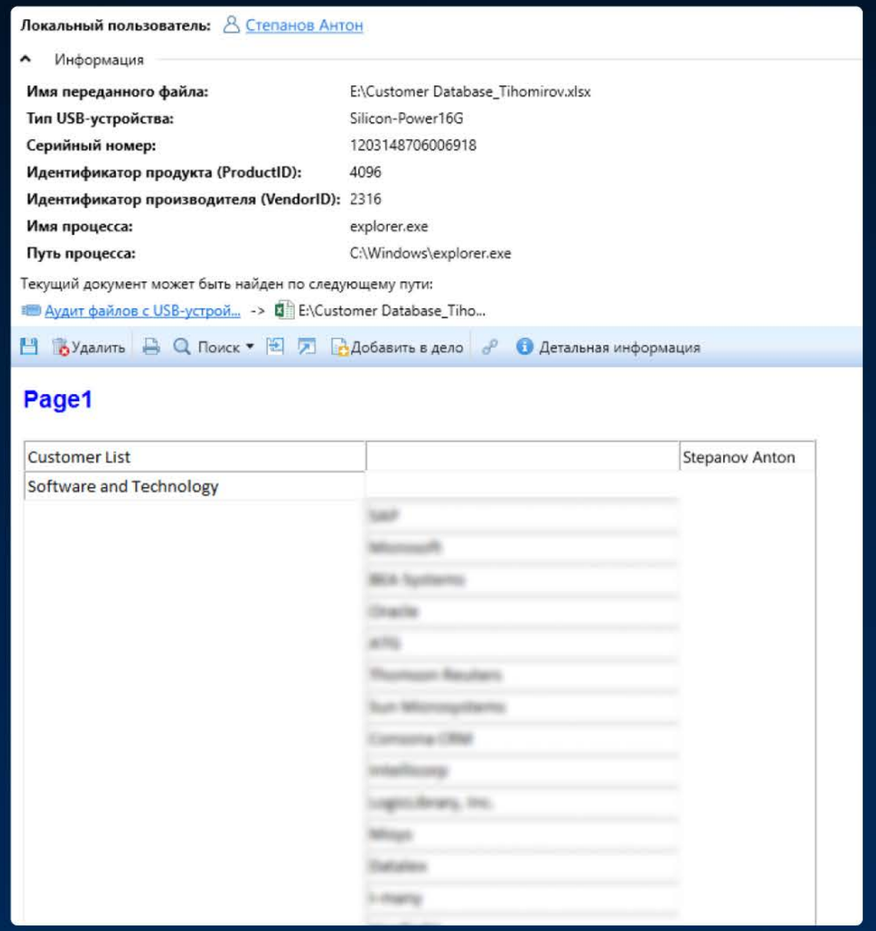
- Подтвержден факт злостного нарушения трудового распорядка
- Пресечена попытка хищения данных о клиентах компании

Модули, которые были использованы:

Комбинированный поиск

Активность пользователей

Агенты (Консоль Администратора)



Комбинированный поиск (Область поиска - почта, мессенджеры)

Кейс 2

falcongaze

Расходование ресурсов компании | Непродуктивная деятельность

Выявление сотрудников-фрилансеров



В этом кейсе мы разберем, как на этапе бесплатного тестирования DLP-системы Falcongaze SecureTower удалось установить факт нецелевого использования рабочего времени и программного обеспечения компании.

Проблема

Компания-клиент работает в проектной сфере. Одна из проблем — в конструкторском отделе постоянно срывались сроки исполнения заказов. Как итог, клиенты уходили, планы не выполнялись.

Сотрудники конструкторского отдела объясняли срывы сроков острой нехваткой времени из-за необходимости постоянно вносить правки в уже переданные на реализацию проекты.

Главный конструктор, учитывая этот факт, рассчитывал сроки выполнения проектов с большим запасом. Тем не менее, сотрудники не успевали.

Кейс 2

falcongaze

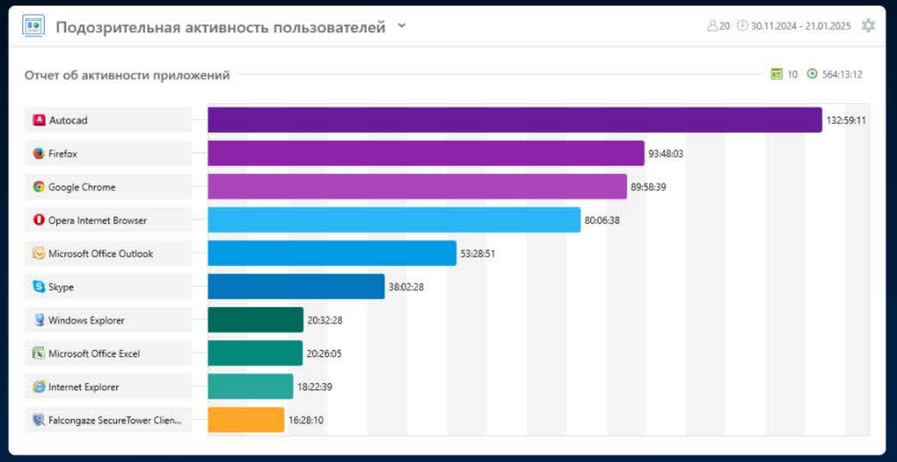
Решение

Компания установила пробную 30-дневную версию SecureTower.

Сперва был проанализирован отчет «Табель рабочего времени» — время начала и завершения работы совпадало с установленным графиком.

Затем в модуле «Отчеты» проанализировали, какие приложения запускают сотрудники. На первом месте значился процесс программы Autocad.

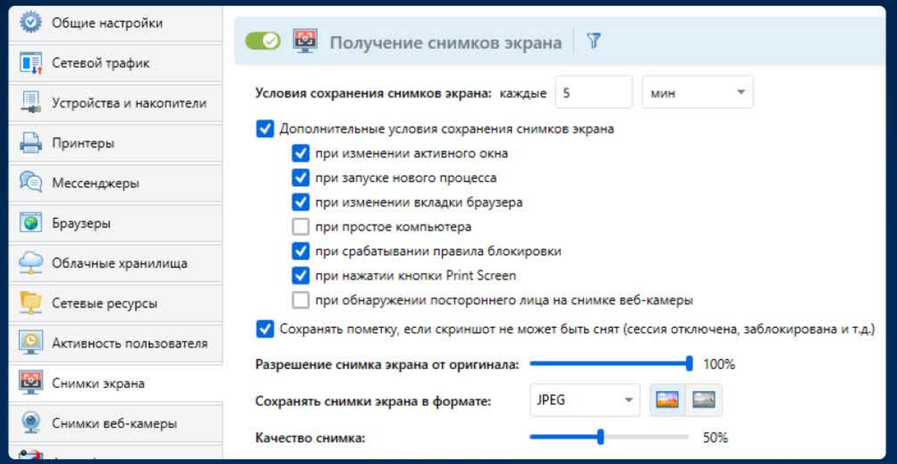
Далее с помощью снимков экрана, которые система выполняла на рабочих станциях персонала каждые 5 минут, установили, что работа ведется не над проектами компании — попавшие на снимки чертежи не имеют отношения к текущим проектам компании.



Модуль «Отчеты» (Отчет об активности пользователей)

Результат

- Выявлен факт нецелевого использования рабочего времени и программного обеспечения компании
- Сотрудников-нарушителей подвергли дисциплинарному взысканию



Консоль администратора (Настройки профиля агентов - Настройка получения снимков экрана)

Модули, которые были использованы:

Политики безопасности

Отчеты

Кейс 3

falcongaze

Нелояльность сотрудников

Утечка информации

Превышение полномочий сотрудниками крупного банка



В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось установить факт передачи конкурентам ценных данных о предстоящей промо-акции, а также выявить виновного и разорвать с ним трудовые отношения.

Проблема

В крупной финансовой организации существенно выросло число неплатежеспособных клиентов по ипотеке. Под подозрение попали консультанты банка, которые могли завышать платежеспособность клиентов. Тем не менее, прямых доказательств мошенничества со стороны персонала не было.

Кейс 3

Решение

Для решения этой и других проблем информационной безопасности приобрели SecureTower. Система перехватывала и анализировала данные в таких информационных каналах:

- электронная почта по протоколам POP3, SMTP, IMAP, MAPI и по их шифрованным аналогам;
- мессенджеры (Skype, Telegram, и еще 15 менее популярных)
- интернет (социальные сети, web-версии электронной почты, облачные хранилища);
- локальные и сетевые принтеры и проч.

Факт превышения полномочий был подтвержден через сработку правила по словарю «Финансовые махинации».

Система перехватила переписки с клиентами в мессенджерах, проанализировала их на содержание заданного количества слов или выражений из предустановленного словаря — и обнаружила сообщения, указывающие на мошеннические действия со стороны персонала.

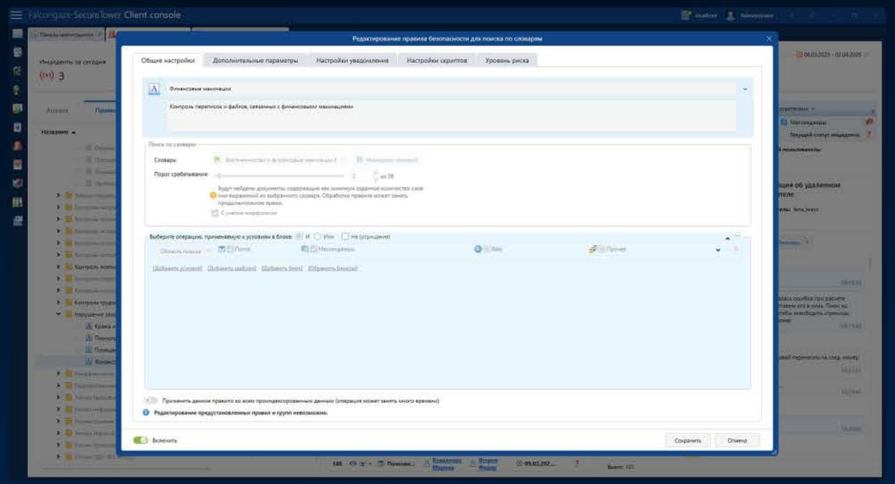
Результат

- Выявлена недобросовестная сотрудница

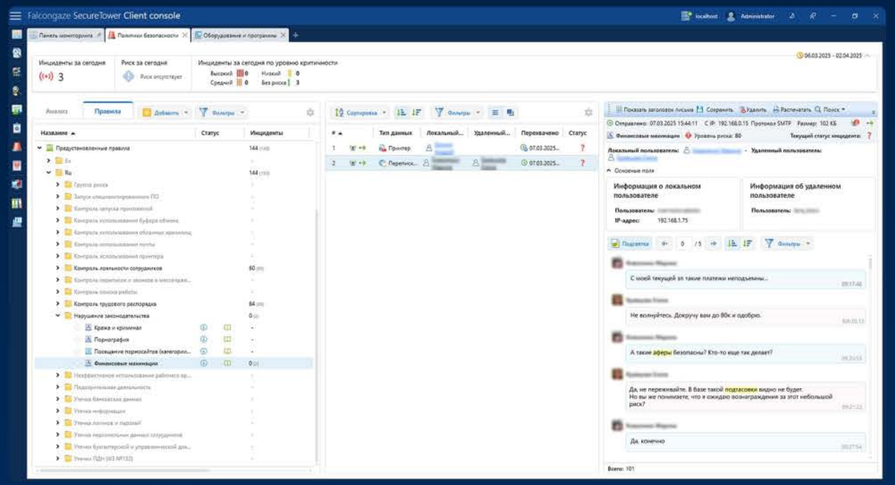
Модули, которые были использованы:

Политики безопасности

Агенты (Консоль Администратора)



Модуль «Отчеты» (Отчет об активности пользователей)



Консоль администратора (Настройки профиля агентов - Настройка получения снимков экрана)

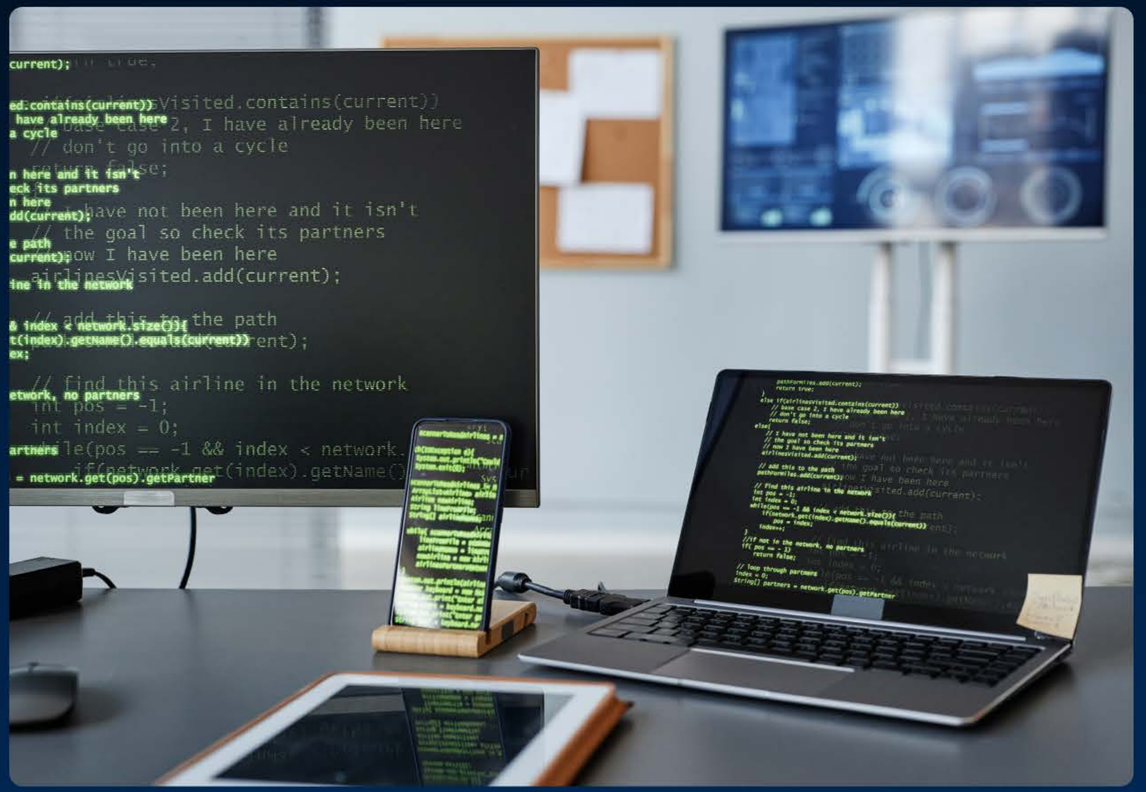
Кейс 4

falcongaze

Нелояльность сотрудников | Утечка информации

Утечка информации о предстоящих акциях

В этом кейсе мы разберем, как с помощью DLP-системы Falcongaze SecureTower удалось установить факт передачи конкурентам ценных данных о предстоящей промо-акции, а также выявить виновного и разорвать с ним трудовые отношения.



Проблема

В торговой сети произошла утечка данных о предстоящей промо-акции. Акция провалилась, торговая сеть не получила желаемую прибыль. В утечке подозревали кого-то из персонала, но доказать факт передачи коммерчески ценной информации не удалось. Поэтому решили сосредоточиться на том, чтобы ситуация больше не повторилась.

Кейс 4

falcongaze

Решение

Для решения этой и других проблем информационной безопасности приобрели SecureTower. Система перехватывала и анализировала данные в таких информационных каналах:

- электронная почта по протоколам POP3, SMTP, IMAP, MAPI и по их шифрованным аналогам;
- мессенджеры (Skype, Telegram, и еще 15 менее популярных)
- интернет (социальные сети, web-версии электронной почты, облачные хранилища);
- локальные и сетевые принтеры и проч.

Помимо этого, были проанализированы все информационные ресурсы организации. С коммерчески ценных документов были сняты цифровые отпечатки (далее — ЦО). На основе собранных отпечатков был сформирован банк и настроена блокировка отправки документов, которые на 30% и более соответствовали снятым ЦО.

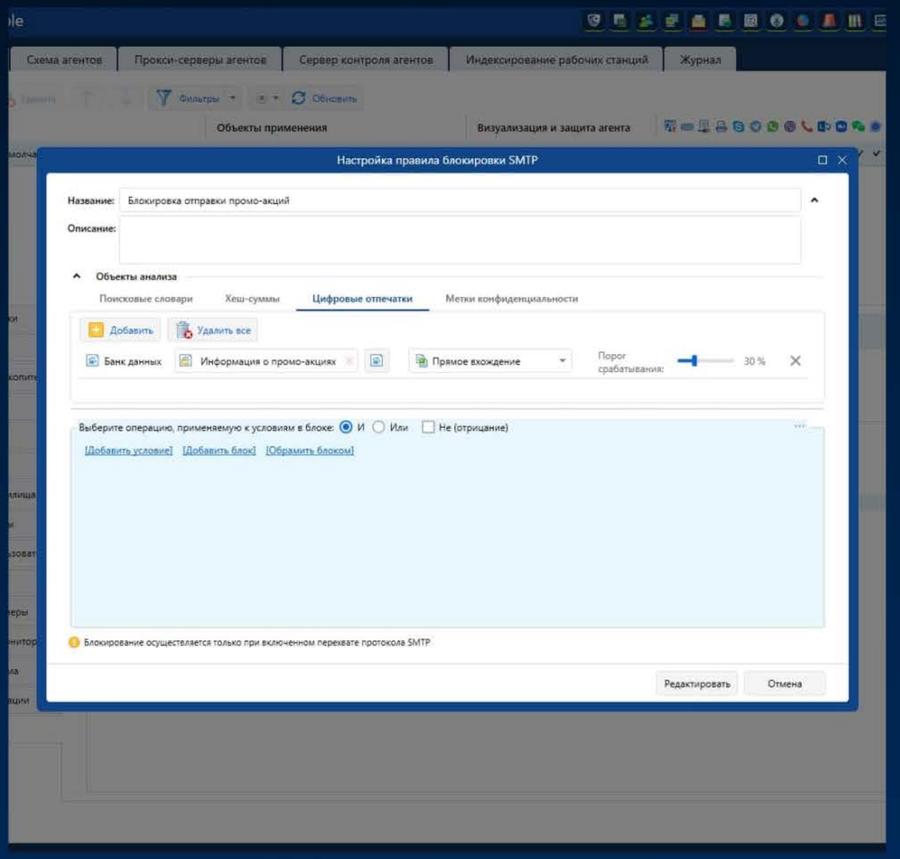
Результат

- Предотвращена утечка коммерчески ценных данных
- Выявлена недобросовестная сотрудница

Модули, которые были использованы:

Политики безопасности

Агенты (Консоль Администратора)

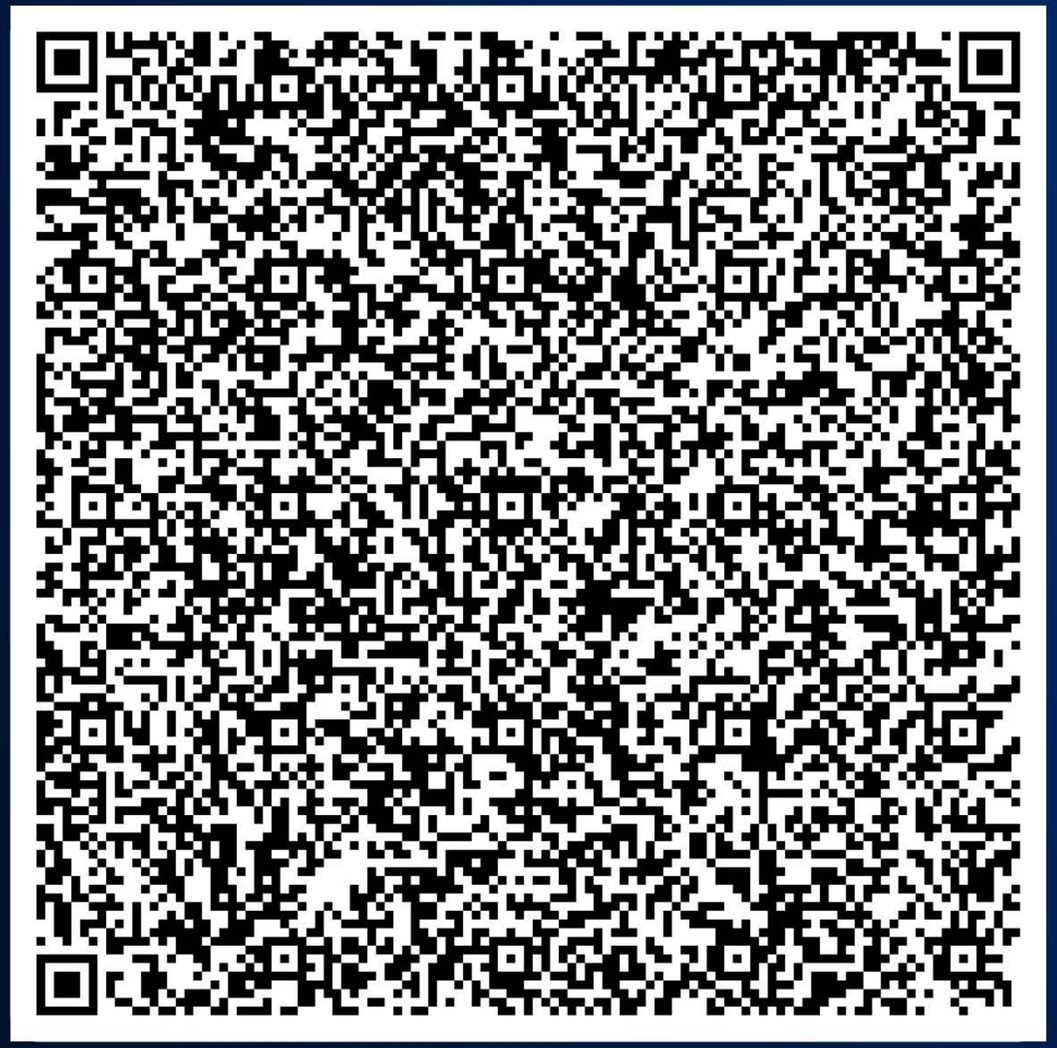


Консоль Администратора (Настройка правила блокировки по протоколу SMTP)

Рекомендации по сокращению рисков




TITANIUM
SecureTower
ЛУЧШЕ КОНТРОЛЬ, СИЛЬНЕЕ ЗАЩИТА



Роман Клименко

Руководитель
представительства Falcongaze

www.falcongaze.com