Наша компания использует систему РОИ (разведки по открытым источникам) нового поколения. В настоящее время данную систему используют более 500 корпоративных и частных клиентов по всему миру. Используя возможности данной системы в совокупности с ручными методами обработки информации, наша компания может предложить своим клиентам следующие области применения сервиса:

Минимизация риска утечки информации.

Поиск потенциальных путей утечки информации путем установления аффилированности сотрудников компании и подрядчиков с группой потенциально заинтересованных лиц и конкурентов.

В рамках данного направления производится выявление и составления перечней явно и потенциально опасных персон и компаний. Перечни составляются на основе анализа деятельности заказчика, с учетом ее специфики, существующей модели угроз и стандартов, принятых на предприятии.

Проверка проводится по следующим атрибутам:

- Прямая аффилированность человек-человек.
- Аффилированность человек – юр.лицо
- Аффилированность через общие места работы и учебы
- Через часто посещаемы локации

Минимизация риска коррупционной составляющей

В рамках данного направления производится выявление и составления модели явно и потенциально опасных или неблагонадежных субъектов и их признаков, взаимодействие с которыми нежелательно или требует особого внимания со стороны руководства заказчика.

Анализ контрагентов

- Составление профиля подрядчика
  - Учредители и руководство компании
  - Ближний круг общения руководства компании
  - Семейные связи и родство
  - Места проживания, учебы, работы
  - Аффилированность через руководство с другими юр.лицами
- Проверка аффилированности подрядчиков с неблагонадежными субъектами
- Проверка аффилированности подрядчиков с чиновниками и органами правопорядка

- Проверка открытых и закрытых судебных делопроизводств на юр.лице

Скрининг кадрового состава

Проверка может производиться как по текущим сотрудникам заказчика, так и в процессе найма новых. Данная проверка поможет на ранних стадиях выявить неблагонадежных персоналий, не лояльных организации, аффилированных с компаниями и сотрудниками из перечней коррупционного профиля и профиля субъектов с повышенными рисками утечки информации.

В рамках данного направления производится составление профиля сотрудника, который может содержать следующие атрибуты:

- Действительность паспорта
- Статус банкрота
- Наличие ИП и ОКВЭДы
- Наличие арбитражных практик
- Правонарушения
- Родственники
- Ближний круг общения
- Учебные заведения и места работ
- Локации
- Политические взгляды
- Неблагоприятные тематики в контенте (посты, фото, видео, комментарии)

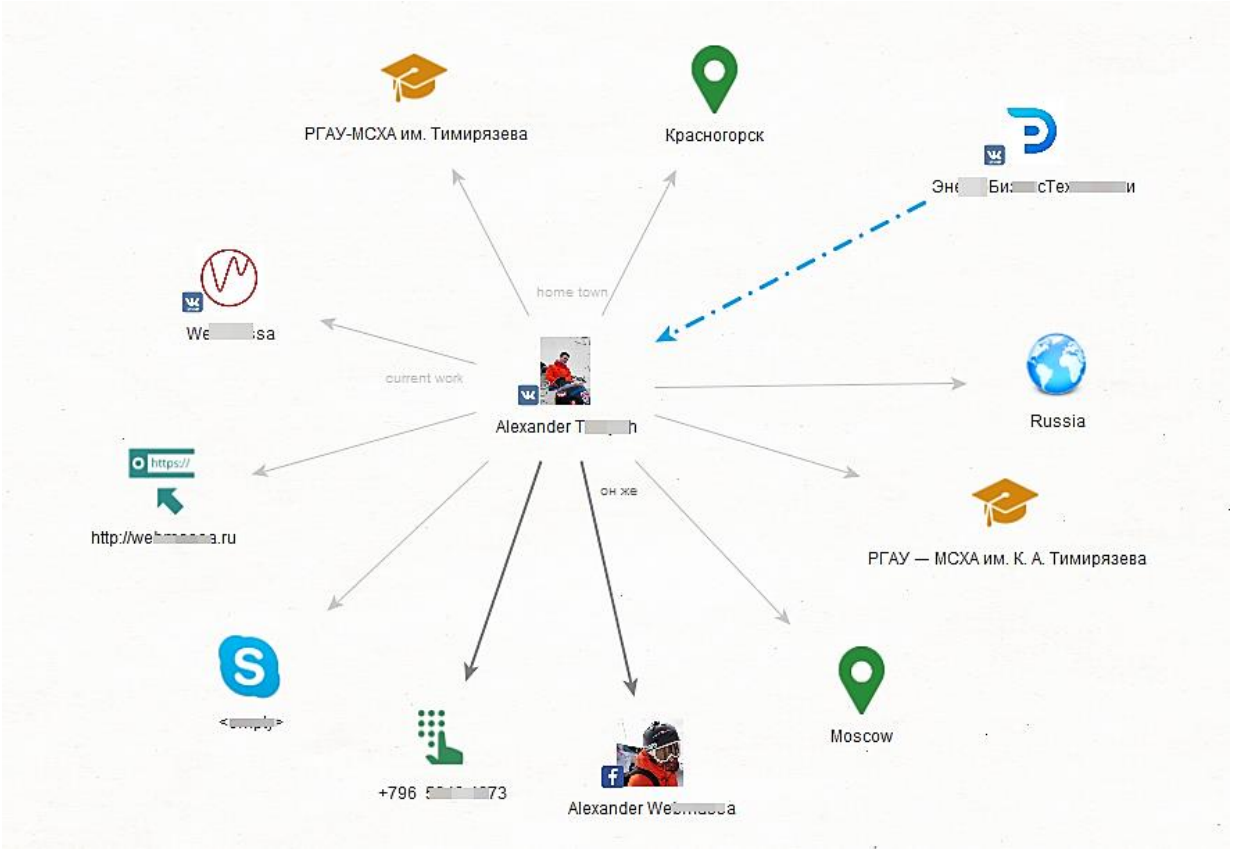
Для всех трех видов деятельности возможно несколько видов работ:

1. Единовременный анализ или скрининг. Когда проверка осуществляется один раз и актуализация производится по запросу заказчика.
2. Регулярная актуализация данных по выбранным объектам, производимая на периодической основе.

По каждому объекту предоставляется отчет, содержащий всю информацию со ссылками на источники. Формат отчета определяется на основе составленных моделей, профилей и особых требований заказчика.

РАССЛЕДОВАНИЯ ПО ОТКРЫТЫМ ИСТОЧНИКАМ ДАННЫХ

- Проверка аффилированости между людьми и компаниями.
- Выявление потенциального местоположения по данным из открытых источников
- Составление полного профиля человека или компании по открытым источникам.
- Поиск родственников человека.



HR/БЕЗОПАСНОСТЬ

- Составление полного профиля с информацией из всех основных социальных сетей, включая весь доступный контент (посты, видео, фото, комментарии, посты, группы).
- Выявление аффилированости с неблагонадежными элементами.
- Составление списка параметров для мониторинга персонала и регулярный скрининг персонала и кандидата по ним.
- Мониторинга профилей топ-менеджмента и их семей на предмет выявления репутационных рисков.
- Анализ фото и видео.
- Распознавание лиц.

СКУД

Система контроля и управления доступом (англ. Physical Access Control System, PACS)

- Выявление объектов.
- Можно использовать для анализа изображения с камер видео наблюдения для автоматического мониторинга нарушений правил техники безопасности, санитарных и прочих норм, предписывающих ношение определенных элементов одежды или защитных средств, принятых на предприятии.
  Например: определение человека в каске (халат, очки, респиратор итп.) или без.

Основные примеры применения используемой нами системы:

- **Пример №1**

Поиск данных о деятельности конкретного лица в социальных сетях.

Фотографии и имени достаточно для обнаружения всех аккаунтов личности в социальных сетях путем нажатия одной кнопки.

- **Пример №2**

Определение структуры и связей преступной группировки.

Возможность анализа внутренних и внешних связей между людьми, событиями и компаниями. Визуализация помогает в определении ключевых элементов внутри группировки. Возможность проводить анализ при использовании любого количества данных.

- **Пример №3**

Поиск на основных форумах и торговых площадках сети Dark Web.

Возможность поиска и мониторинга сайтов сети Dark Web без необходимости авторизации или создания учетной записи.

- **Пример №4**

Поиск содержимого социальных сетей по географическим координатам.

Поиск свидетелей или мониторинг обстановки в пределах конкретной локации. Система «Social Links» предоставляет возможности для поиска фото- или видео-содержимого, страниц социальных сетей и местоположения в сетях Facebook, Instagram, Snapchat и Twitter путем использования географических координат.

- **Пример №5**

Определение личности по цифровым данным.

Обширная комбинация источников и ссылок на базы данных, таких как PIPL, обеспечивает успешное решение задач по дополнению имеющихся данных и определению личности.

- **Пример №6**

Анализ крипто валюты.

Система позволяет осуществлять исследовательскую деятельность в режиме реального времени на платформе распределенного хранения достоверных данных (блокчейн) Ethereum, обеспечивает наличие взаимосвязей между адресами, операциями, средствами и контактами на базе данной платформы.