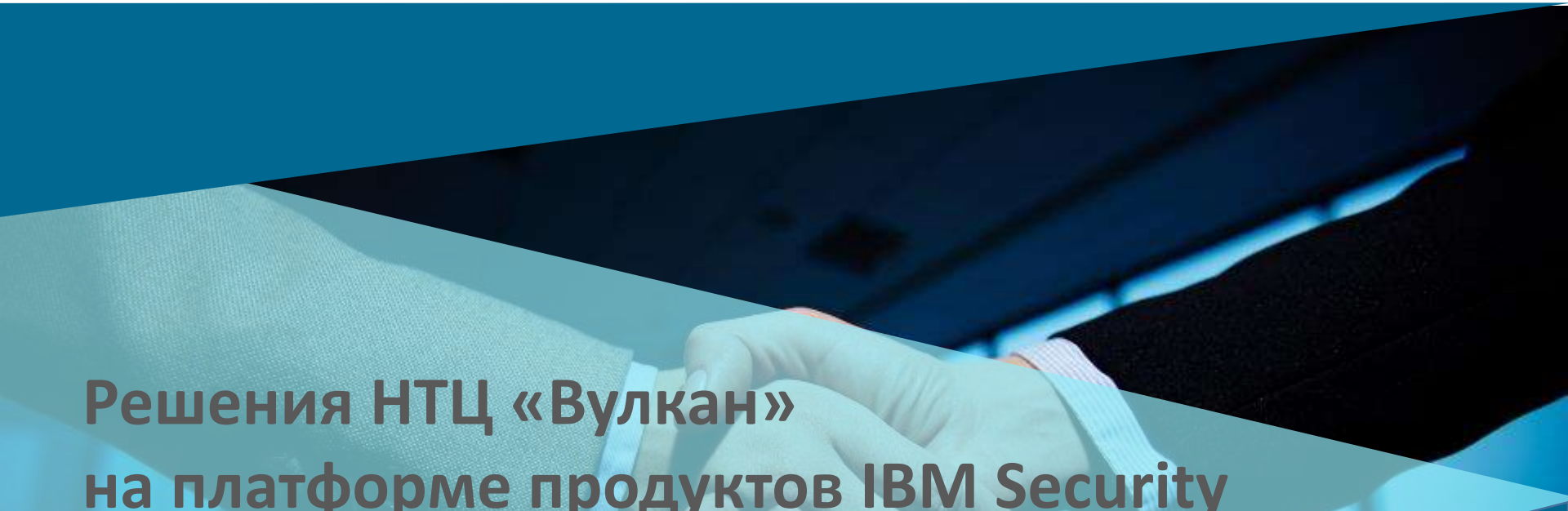
www.ntc-vulkan.ru



Решения НТЦ «Вулкан» на платформе продуктов IBM Security

Embedded Solution Agreement (ESA)

Елена Шакунова
Директор по развитию бизнеса

2017

СОДЕРЖАНИЕ

О КОМПАНИИ

НТЦ «Вулкан» является интегратором в области современных информационных технологий и обеспечения информационной безопасности

На рынке с 2010 года;

более 150 сотрудников

Входит в 30 крупнейших компаний России в сфере защиты информации*

Сертифицированная система менеджмента качества

Лицензиат:

- ФСТЭК России
- ФСБ России
- МО РФ
- Минпромторг

Комплексные решения в сфере экономической и информационный безопасности

* По версии *CNews Analytics, 2016*

QRV
АВТОМАТИЗИРОВАННАЯ КОРПОРАТИВНАЯ ИБ-ОТЧЕТНОСТЬ НА ПЛАТФОРМЕ IBM QRADAR (SIP)

Всё что есть в IBM QRadar SIEM

+

Автоматизатизированная корпоративная отчетность

АВТОМАТИЗАТИЗИРОВАННАЯ КОРПОРАТИВНАЯ ОТЧЕТНОСТЬ
ВОЗМОЖНОСТИ

Оформление отчетов по ИБ согласно корпоративному стилю

Dashboard'ы с функцией drilldown

Русифицированные отчеты и dashboard'ы

Приоритизация данных

Автоматическая рассылка отчетов по e-mail

50+ предустановленных наборов отчетов

ДЛЯ КОГО?
ЦЕЛЕВАЯ АУДИТОРИЯ

- ✓ Финансовые институты
- ✓ Телеком
- ✓ ТЭК и Нефтегазовый сектор
- ✓ Промышленность и транспорт
- ✓ Ритейл и оптовая торговля

ПОТРЕБИТЕЛИ ОТЧЕТА

- ✓ ТОП-менеджер
- ✓ Compliance-менеджер
- ✓ Risk-менеджер
- ✓ IT-менеджер
- ✓ IS-менеджер
- ✓ Владелец процесса (*Event Mgmt, Incident Mgmt, Access Mgmt и т.д.*)
- ✓ Технический специалист (*сетевик, системщик и т.д.*)
- ✓ Член SOC-команды

ПОЧЕМУ ?
ДЛЯ ЧЕГО?

- Необходима актуальная картина инцидентов ИБ
- Есть потребность в оценке эффективности работы ИБ-подразделений в ежедневном режиме
- Необходимо доносить важную информацию по ИБ до руководства
- Регулярная подготовка отчетов для смежных подразделений
- Требуется доступное обоснование (аргументация) для дальнейшего выделения бюджета на развитие ИБ

КАК ЭТО РАБОТАЕТ?
ПРИМЕРЫ ОТЧЕТОВ

ASA - VPN Session Closed

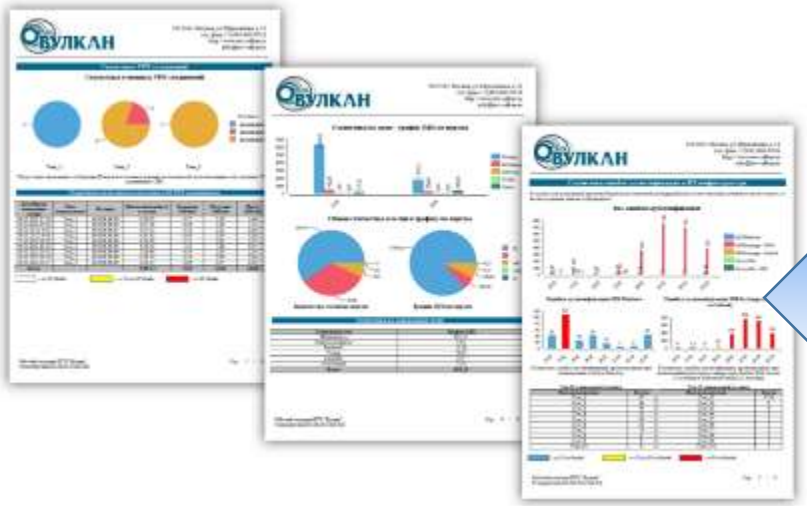
Generated: 11 May 2016, 00:41:58

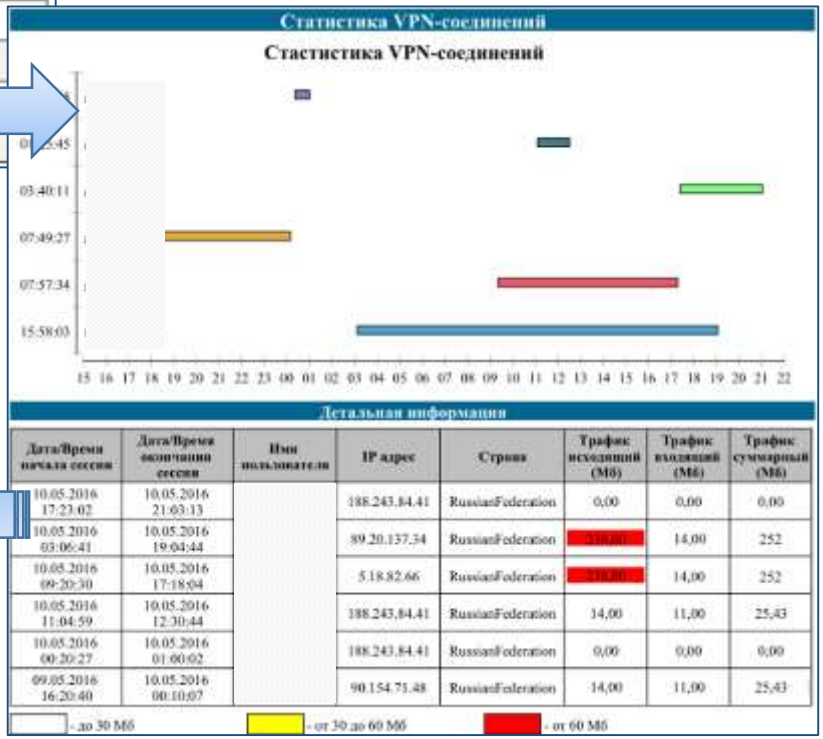
ASA - VPN Session Closed
ASA - VPN Session Closed
10 May 2016, 00:00:00 - 11 May 2016, 00:00:00

Start Time	Username	Source IP	Geographic Country/Region	BytesSent (custom)	BytesReceived (custom)	Duration_Hours (custom)	Duration_Minutes (custom)	Duration_Seconds (custom)
10 May 2016, 21:03:13		188.243.84.41	RussianFederation	179.488	191.461	3	40	11
10 May 2016, 19:04:44		89.20.137.34	RussianFederation	250.302.663	3,630.605.331	15	58	3
10 May 2016, 17:18:04		5.18.82.66	RussianFederation	302.173.578	2.546.320.604	7	57	34
10 May 2016, 12:30:44		188.243.84.41	RussianFederation	15.015.851	11.645.754	1	25	45
10 May 2016, 01:00:02		188.243.84.41	RussianFederation	171.064	86.238	0	39	3
10 May 2016, 00:10:07		90.154.71.48	RussianFederation	125.650.351	14.949.010	7	49	2

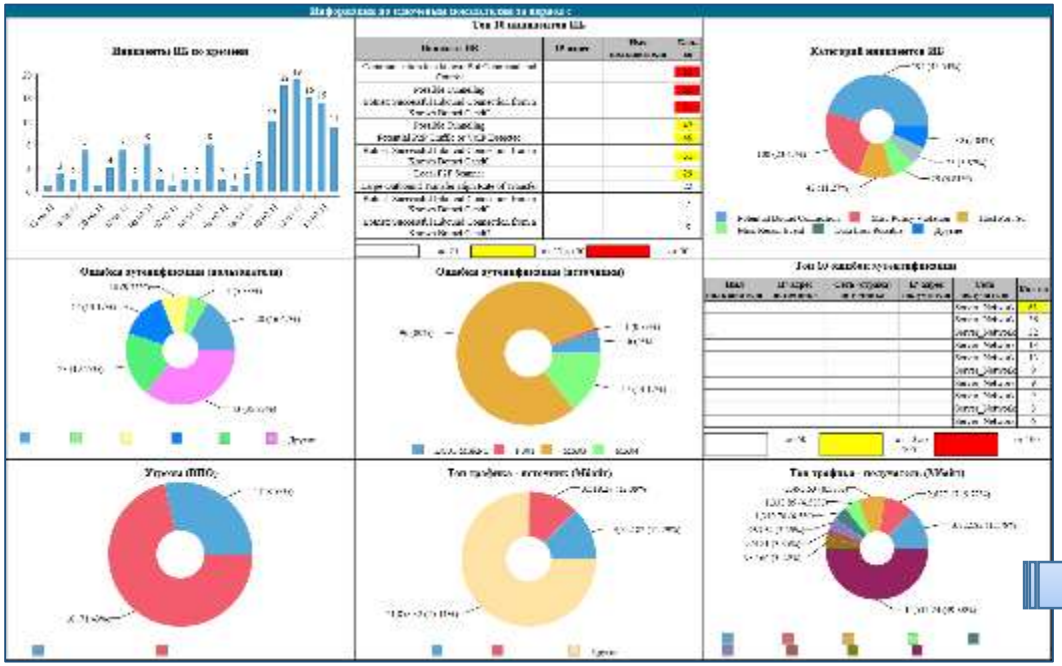
IBM QRadar

НТЦ «Вулкан»





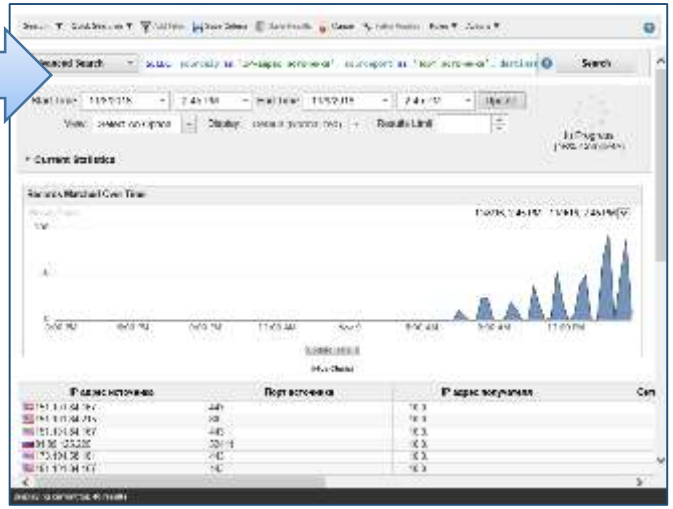
КАК ЭТО РАБОТАЕТ?
ПРИМЕРЫ ОТЧЕТОВ



НТЦ «Вулкан»

Drilldown

IBM QRadar



https://

КАК ИСПОЛЬЗОВАТЬ?

Как IBM QRadar SIEM

+

Как информационную панель для ситуационной осведомленности

Как инструмент для приоритизации ресурсов на возникающие инциденты ИБ

Как средство для выстраивания коммуникации внутри и за пределами ИБ-подразделения

РЫСЬ
АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПРОВЕРКИ КОНТРАГЕНТОВ НА ПЛАТФОРМЕ IBM I2

Программное решение на платформе IBM I2 для сбора и анализа данных:

- о связях (аффилированности) контрагентов с сотрудниками компании и их родственниками
- при поиске конечных бенефициаров

ВОЗМОЖНОСТИ

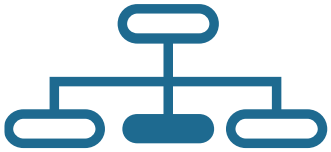
Комплексные проверки

- участников тендера на предмет взаимосвязи и возможного сговора
- контрагентов (учредителей, руководителей), связанных с сотрудниками компании
- по поиску конечного бенефициара

Автоматизированный процесс выявления аффилированности

Актуальная картина рисков Компании:

- финансовых
- налоговых (факт не предоставления отчетности в налоговую инспекцию)
- репутационных
- риска некачественного выполнения работ (черные списки, исполнительное производство)



Наглядные визуальные схемы

ДЛЯ КОГО?
ЦЕЛЕВАЯ АУДИТОРИЯ

- ✓ Госсектор
- ✓ Финансовые институты
- ✓ Нефтегазовый сектор
- ✓ ТЭК
- ✓ Промышленность
- ✓ Ритейл и оптовая торговля
- ✓ Медиа-холдинги
- ✓ Транспорт

Любая компания / организация с персоналом от 1 000 сотрудников

ЛИЦА, ПРИНИМАЮЩИЕ РЕШЕНИЯ:

- ✓ Руководство компании
- ✓ Экономическая безопасность
- ✓ Внутренний контроль
- ✓ Казначейство
- ✓ Управление рисками
- ✓ Управление комплаенс-процедур
- ✓ Тендерно-закупочные отделы
- ✓ Юридический департамент
- ✓ Руководители подразделений интеллектуальных систем защиты
- ✓ Маркетинговые и финансовые службы

ПОЧЕМУ?
ДЛЯ ЧЕГО?

- Необходима автоматизация аналитической обработки данных о контрагентах и сотрудниках из учетных систем компании и СПАРК-Шлюза
- Мониторинг изменения состояния контрагентов (реквизитов)
- Требуется информация о рисках, связанных с сотрудниками и кандидатами
- Оперативная проверка надежности контрагентов при проведении закупочных и тендерных процедур
- Потребность в наглядных визуально-аналитических отчетах для ТОПов

ИЗ ЧЕГО СОСТОИТ? И КАК ЭТО РАБОТАЕТ?

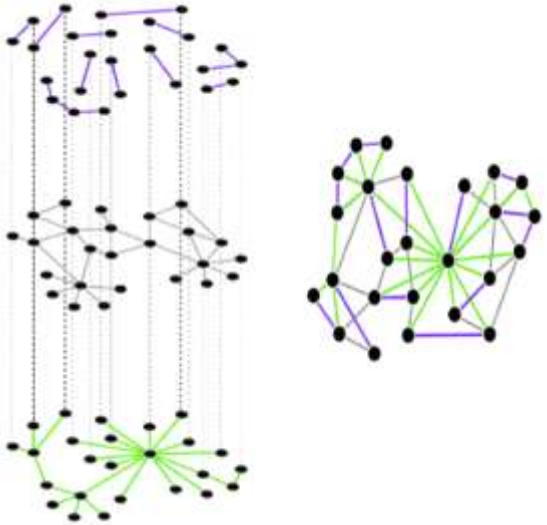
СИСТЕМА СОСТОИТ ИЗ 2 ЧАСТЕЙ:

1. Рабочее место аналитика

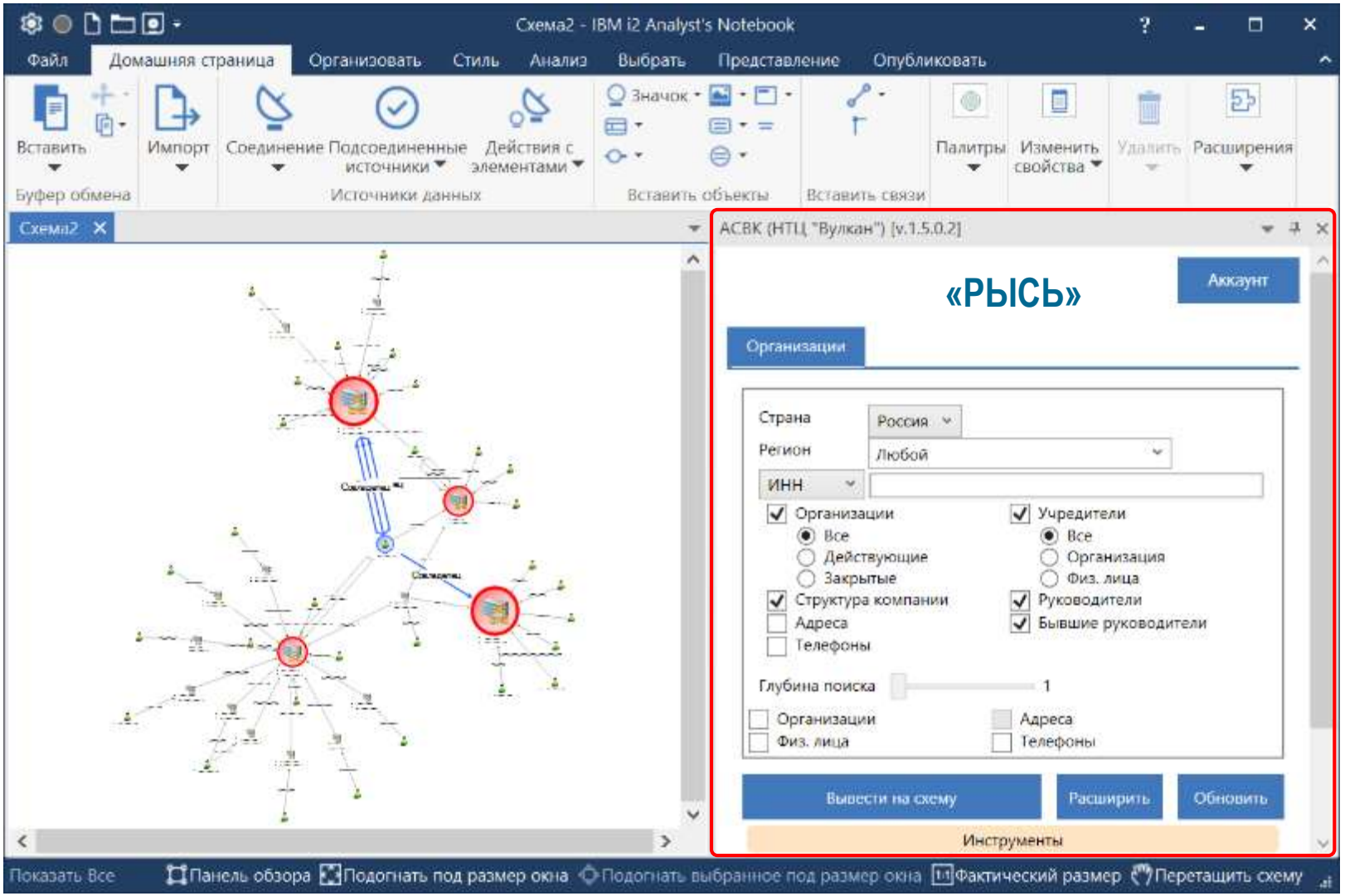
2. Хранилище данных

АРХИТЕКТУРА:

1. ИНФОРМАЦИЯ О КОНТРАГЕНТЕ
2. ИНФОРМАЦИЯ О СОТРУДНИКАХ И ИХ РОДСТВЕННИКАХ
3. ИНФОРМАЦИЯ ОБ УЧРЕДИТЕЛЯХ И РУКОВОДИТЕЛЯХ КОНТРАГЕНТОВ



КАК ЭТО РАБОТАЕТ?
ИНТЕРФЕЙС СИСТЕМЫ



С ЧЕМ РАБОТАЕТ?
ИСТОЧНИКИ ДАННЫХ

Внутренние

Файлы импорта (структурированные форматы данных)

Например:

- Бухгалтерские системы (1С, SAP R/3, Axapta, Microsoft Dynamics AX)
- Кадровые системы
- Реестры детализаций по предоставленным услугам сотовой связи
- Логи приема/отправки корпоративной почты
- GPS/ГЛОНАСС-контроль и учёт транспорта

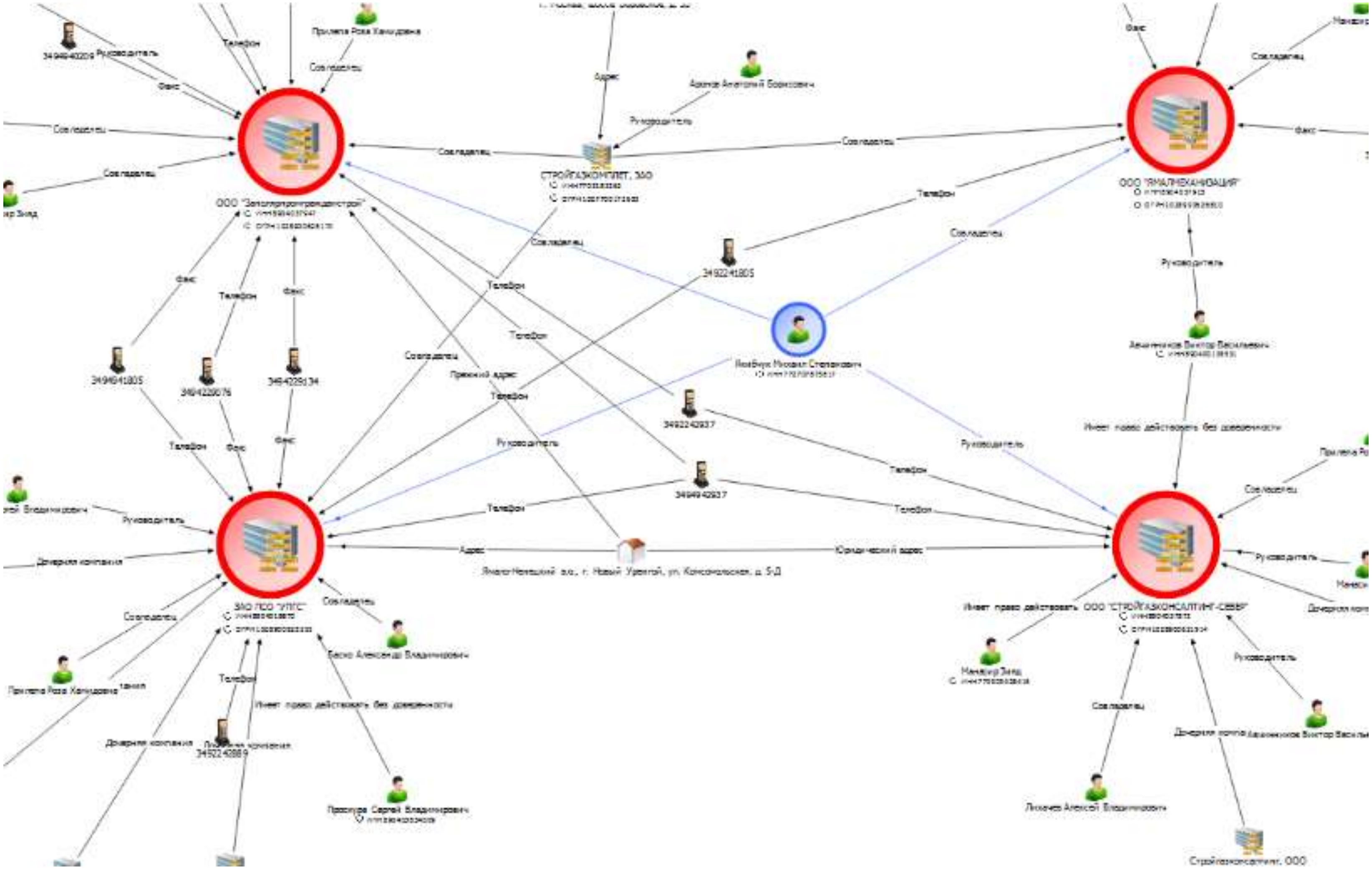
Внешние

Открытые источники данных (в т.ч. по подписке) - через коннекторы

Например:

- СПАРК. Шлюз, вкл. компании Казахстана и Украины
- Контур-Фокус
- Дельта Инком
- Базы данных налоговых органов
- Телефонные справочники
- СМЭВ (Система межведомственного электронного взаимодействия)

РЕЗУЛЬТАТ РАБОТЫ
ПРИМЕР СХЕМЫ АНАЛИЗА



КАК ИСПОЛЬЗОВАТЬ?

Проверка достоверности предоставляемых данных контрагента

- Номинальные директора, учредители
- Наличие офшорных компаний в структуре организации
- Ликвидированные компании или на стадии ликвидации

Выявление тендерных сговоров

- Поиск связей юридических и физических лиц, участвующих в тендере
- Соответствие 273-ФЗ (О противодействии коррупции) и 115-ФЗ (О противодействии отмыванию доходов / борьбе с финансированием терроризма)

Проверка при приеме на работу

- Наличие ИП
- Долевое участие в компаниях (конфликт интересов)

СПАСИБО ЗА ВНИМАНИЕ!

105318 г. Москва, ул. Ибрагимова, д. 31
тел. +7 (495) 663-95-16
info@ntc-vulkan.ru
www.ntc-vulkan.ru

Елена Шакунова
Директор по развитию бизнеса
e.shakunova@ntc-vulkan.ru