

OSINT

Современные подходы к автоматизации
поиска в открытых источниках



OSINT: наши продукты



Виток-OSINT – стек технологий для формирования запросов в открытые источники + приложение для поиска и анализа данных.



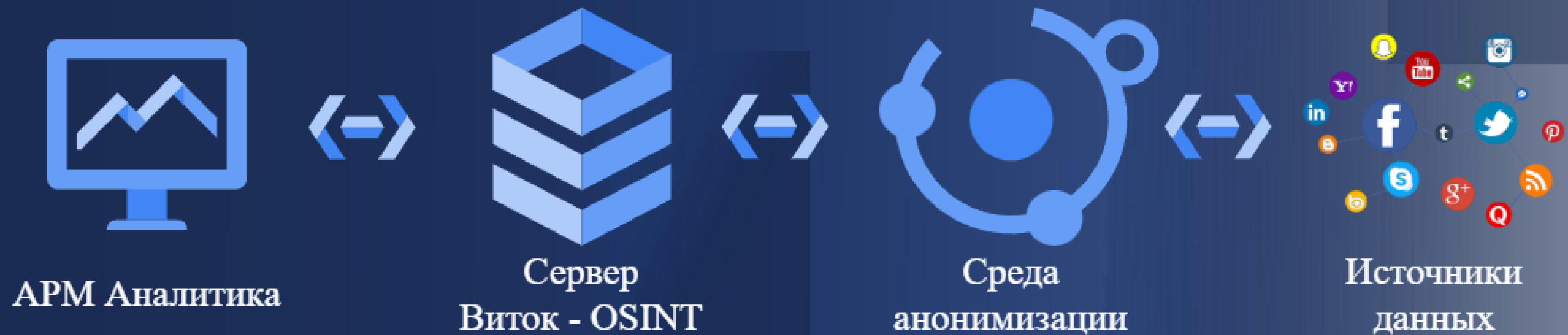
Виток-Портрет – веб-приложение для поиска информации в открытых источниках. Поиск осуществляется на стеке технологий Виток-OSINT.



Виток-М – информационно-аналитический веб-сервис мониторинга СМИ и блогосферы. Поиск также осуществляется на стеке технологий Виток-OSINT.



Схема взаимодействия



Серверная лицензия Виток-OSINT



Администрирование и распределение лимитов на запросы среди пользователей



Сохранение сделанных запросов в базе данных на сервере



Возможность работы с внутренними базами данных в едином интерфейсе



Паладин-X224:

- до 24xSFF дисков, +2xSFF диска
- 2x1 GbE, 1x1000Mbe BMC
- 2U, БП 1+1 (220В/48В)
- до 2 ЦПУ Xeon Scalable
- до 3 Тб ОЗУ (24xDDR4)



Сервер производства ЗАО «НОРСИ-ТРАНС»



Оборудование включено в реестр Минпромторга России

Взаимодействие с источниками



Пользователю не требуется задумываться над инфраструктурными вопросами: аккаунты, прокси-сервера, аргументы, очередь задач, поиск «из коробки»

Простой запуск

Номер телефона

Запуск запросов

Критерии

- ASN
- Crt.sh ID
- Domain
- Email
- Facebook ID
- Google ID
- Hashes
- Hybridanalysis job IDs
- IMEI
- Instagram ID
- IP address
- Latitude
- LinkedIn company ID
- LinkedIn ID
- Longitude
- Netblocks
- Odnoklassniki ID
- Offshore Leaks ID
- Organisation
- Password
- Serial Number
- Spotify User ID

Задачи

- Избранные
- Мессенджеры
 - Поиск ICQ по электронной почте
 - Поиск Skype по электронной почте
- Прочие сервисы
 - Goodreads account by email 1.0.0
 - Информация о получателе в Yahoo
 - Наличие аккаунта 7 Cups по электронной почте
 - Наличие аккаунта Adobe по электронной почте
 - Наличие аккаунта AliExpress по электронной почте
 - Наличие аккаунта Amazon по электронной почте
 - Наличие аккаунта Any.do по электронной почте
 - Наличие аккаунта Apple по электронной почте
 - Наличие аккаунта Archive.org по электронной почте
 - Наличие аккаунта Armurerie-Aux
 - Наличие аккаунта BlaBlaCar по электронной почте
 - Наличие аккаунта BLIP.fm по электронной почте
 - Наличие аккаунта Buy Me a Coffee
 - Наличие аккаунта Codecademy по электронной почте
 - Наличие аккаунта Elio по электронной почте

РЕДАКТИРОВАНИЕ ТЕМЫ

Введите детали темы для редактирования

Название темы

Телеканалы

Теги, ссылки на аккаунты и ключевые слова

<https://instagram.com/infomoscw24> <https://t.me/ntvnews> <https://tiktok.com/@tvrussia1> https://twitter.com/1tvru_news <https://youtube.com/channel/UC1me7og-uTpdRXRg...> Введите значение

Внести изменения

ГЛАВНАЯ НАВИГАЦИЯ

- Лента сообщений
- Источники
- Темы
- Добавить новую тему
- Избранное
- Twitter
- YouTube
- Instagram
- Telegram
- TikTok
- Телеканалы

ПОРТРЕТ ВИТОК

Добавить метку

Поиск по параметрам

Откройте меню выбора параметров

Все параметры 44

- Email
- Номер телефона
- Персона
- Автомобиль
- Домен

Выберите параметр слева

Для начала работы

Координаты

Введите координаты, адрес или выберите точку на карте

большой театр

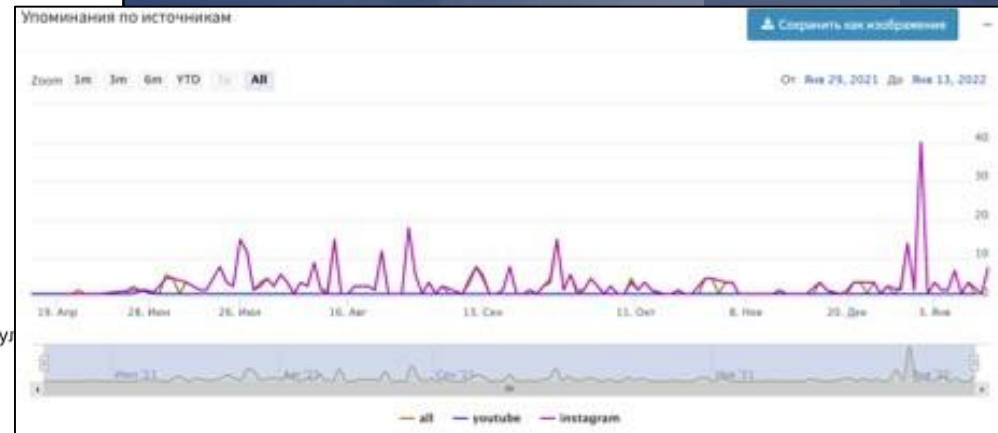
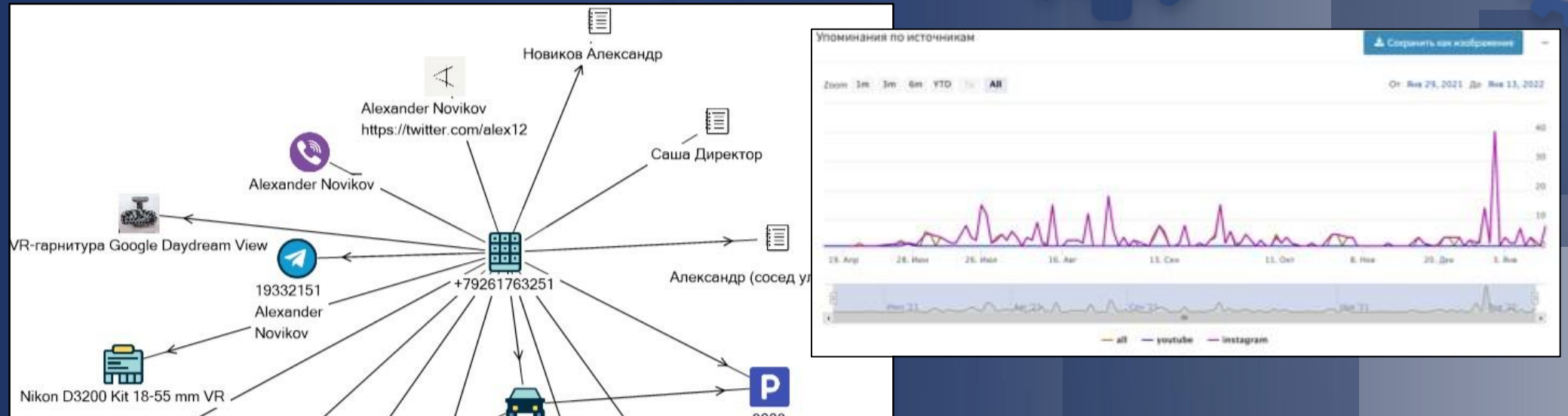
200 метров

Изображение

Выберите изображение ниже

Заменить

Различные формы представления данных под разные задачи



Просмотры: 0 Лайки: 0 Поделитесь: 0 Комментарии: 0 Рейтинги: 0.2371 Прочитано

Опубликована история

Распознанный текст изображения: @sergidetkov подпишитесь скорее г новый кусочек о...

Распознанная аудиодорожка видео: я никогда не понимал нахуя бабки бегут вот мой воз...

Алексей Щербаков www.instagram.com

Карта 154

#	Источник	Аватар	Имя
1	+5 Профиль Skype		Mayur Agrawal
2	+5 Профиль Skype	USPL	Urbrighter IT Services Pvt. Ltd.
3	+5 Профиль Skype		SAMBIO ACCOUNT THEGAMERPRO27.HACK
4	+5 Профиль Skype		Ankur Chauhan
5	+5 Профиль Skype		Srinivas Nagaraju
6	+5 Профиль Skype		Rafal
7	+4 Профиль Goodreads		Tester123
8	+5 Профиль Skype		Hanh Mai Do My
9	+9 Профиль Foursquare		
10	+4 Адрес		

Парковки

#	Госномер	Количество
1	X7770E777	47
2	O694CA777	3
3	H505HT152	2
	H860YX152	1
	C005AA52	1
	X005TK52	1
3	X7770E777	540

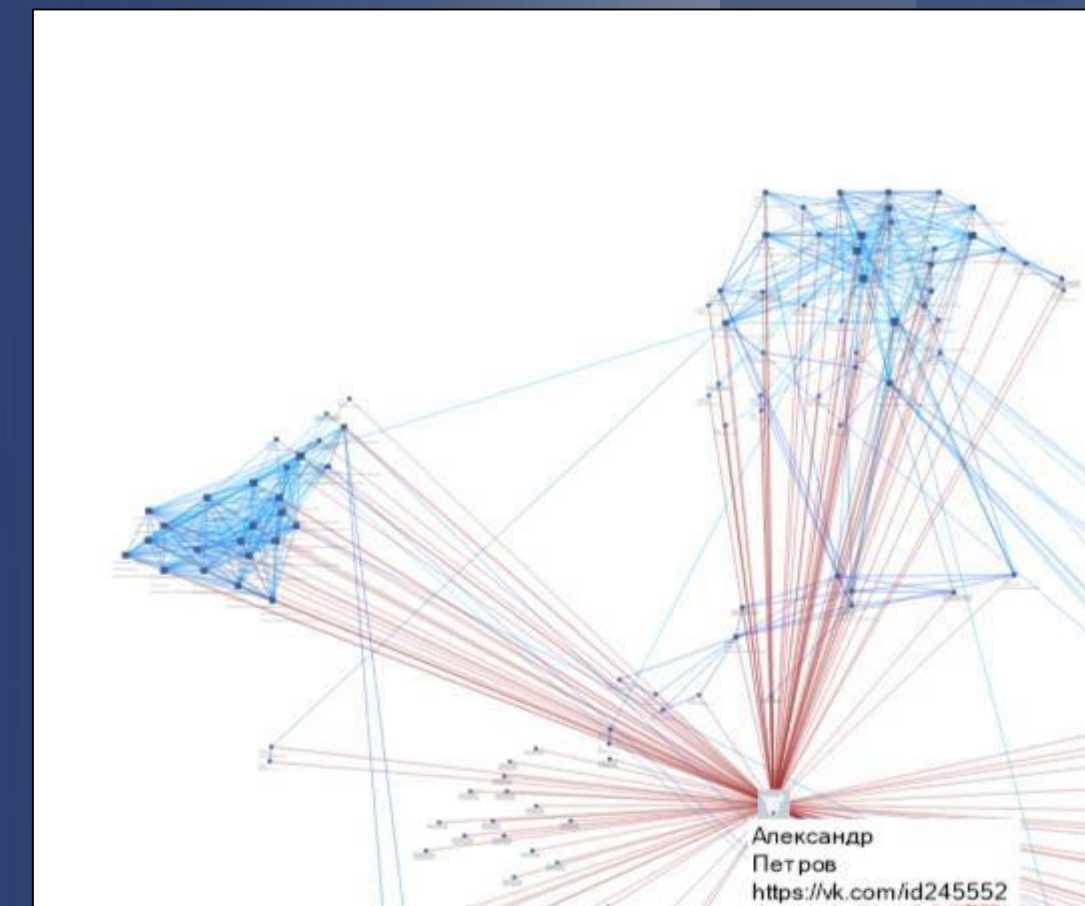
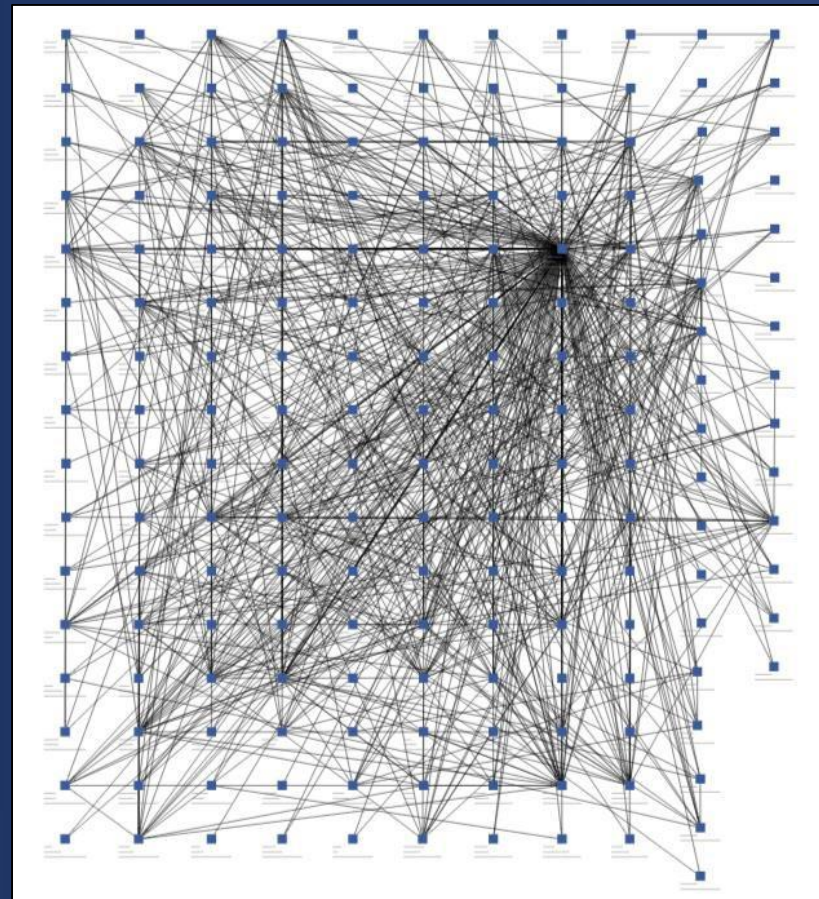
Обработка данных: кластерный анализ



Различные механизмы укладки графа



Поиск путей на графе,
выявление сообществ



Обработка данных: формирование единого досье



В финальном досье происходит анализ всех полученных данных



Единое досье формируется согласно общей онтологии данных и всей информации, полученной из разных источников




Досье разбивается на структурированные блоки, которые содержат разную информацию – контакты, интернет-активность, сферу профессионального и личного интереса и пр.

Поиск: Персона

Параметры запроса: natasha@gmail.com +7903152000 Иванова, Наталья, Александровна

Аватар



Общее

Имя
Иванова Наталья Александровна Иванова (Петрова) Наталья Наташа (работа поликлиника)

Дата рождения
20.9.1993

Возраст
30

Место рождения
Москва

Паспорт
45 06 494987 выдан паспортным столом 3 ОБД района Ясенево г.Москвы, 21.08.2003

ИНН
772838861715


СНИЛС
081-385-158 01

Номер телефона










IP-адрес
83.167.112.2

Социальные сети
skype://natasha-work?chat <https://my.mail.ru/mail/natasha> <https://vk.com/id24578779> <https://www.linkedin.com/in/наталья-иванова-петрова-3897a/> <http://my.nike.com/НатальяС2738785454>
<https://www.mapmyfitness.com/profile/685952> <https://ok.ru/profile/4889894191>

Наличие аккаунтов



Основные преимущества

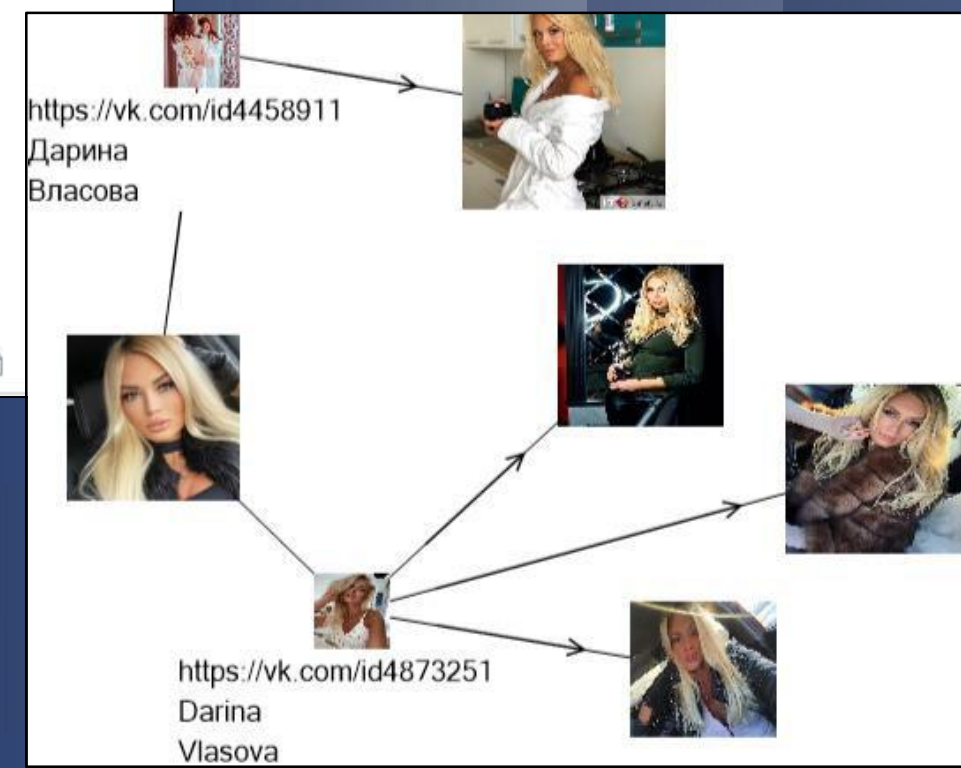
-  Эмуляция действий реального пользователя
-  Единая онтология выходных данных
-  Собственный API-интерфейс взаимодействия с источниками для задач автоматизации и интеграции с другими платформами
-  Непрерывный мониторинг работоспособности
-  Технология искусственного интеллекта: транскрибирование речи, распознавание лиц, распознавание текста с изображения
-  Возможность подключения собственных данных без программирования (No-Code)
-  Постоянное добавление новых источников, в т.ч. по заявкам заказчика
-  Функционирование вне зависимости от зарубежных санкций. Разработка и техподдержка на территории России.
-  Программное обеспечение включено в реестр Минцифры России

Пример работы поисковой методики с использованием ИИ

Распознанный текст изображения: на завтрак приготовила запеканку по рецепту...
[Показать полный текст](#)

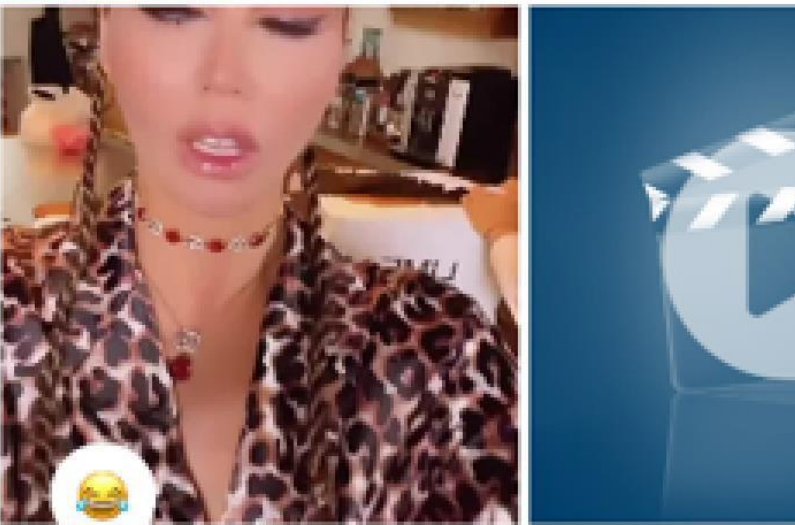


Константин Ивлев www.instagram.com [Перейти к профилю автора](#)

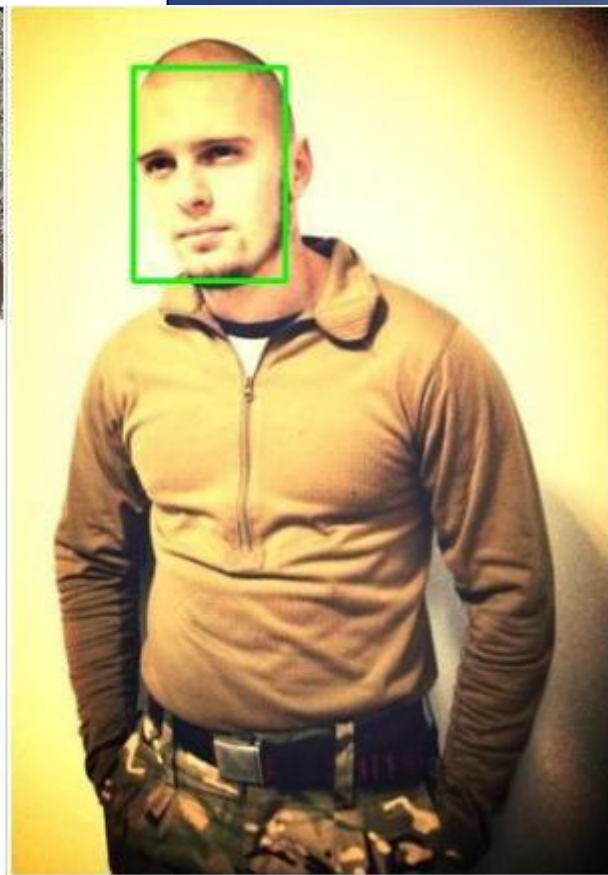


Распознанная аудиодорожка видео: Друзья, простите меня, пожалуйста, за сто и одну сториз, но этот тот редкий случай, когда девушка себе очень сильно нравится и хочет прям вот в своем аккаунте просто спамить своей очаровательной мосей




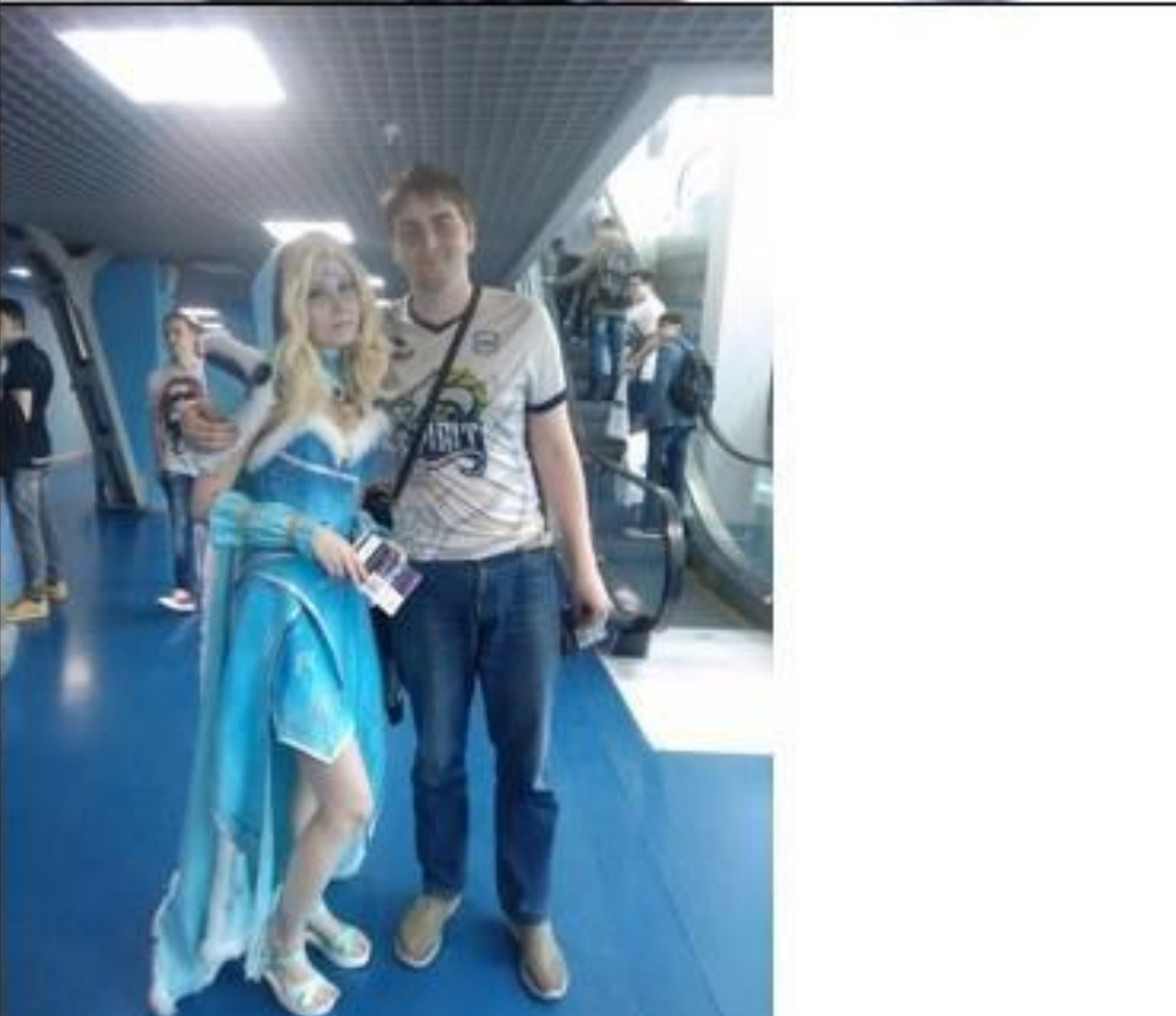
[Скрыть полный текст](#)





Ляйсан Утяшева www.instagram.com [Перейти к профилю](#)



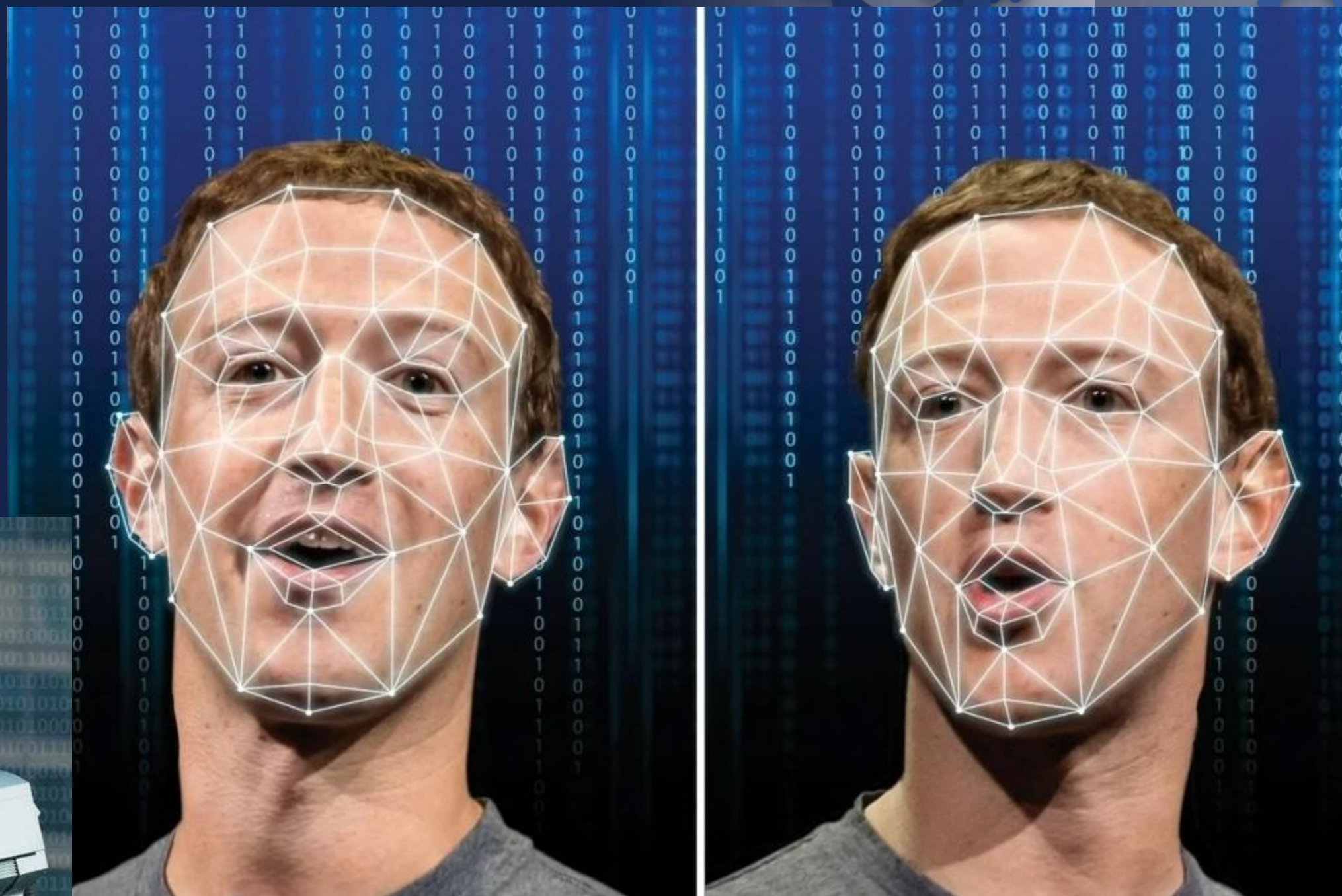
<https://nemez1da.ru/nacizistskie-podrazdeleniya/polk-azov/roq-aleksandrovich-romanov-oleg-oleksandrovich/>

Исходное изображение	Фотография	Совпадение	ID пользователя
		0,871	409572181
		0,871	409572181

Исходное изображение	Фотография	Совпадение	ID пользователя
		0,647	19195027
		0,656	19195027
		0,583	356269552



Распознавание лиц с камер видеонаблюдения



Обработка данных: алгоритмические задачи поиска

Пример: поиск родственников



Подбор СУБД с учетом необходимости быстрого поиска по большому объему разрозненных данных



Выявление объектов (адресов) в тексте



Нечёткий итерационный поиск

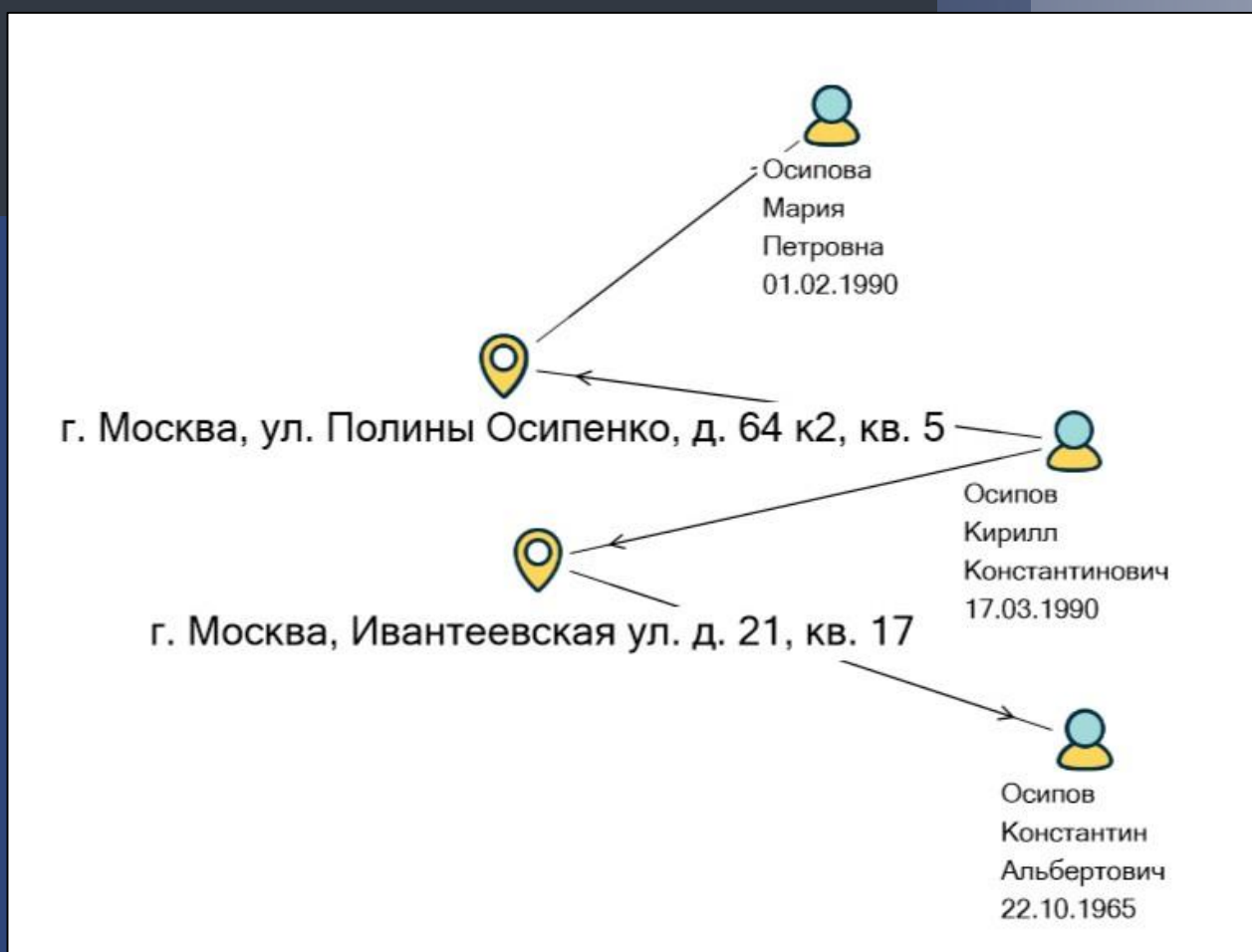


Микросервисная архитектура, позволяющая быстро адаптировать механизмы под нужную последовательность выполнения задач

Поступило сообщение о краже из квартиры по адресу Ивантеевская 21 17
Заявитель Описов Константин Альбертович, 22.10.1965 г.р.

Автомобиль: А643ВУ777
Владелец: Осипов Кирилл Константинович
Дата рождения: 17.03.1990
Адрес регистрации: г. Москва, Ивантеевская ул., д. 21, кв. 17
Адрес проживания: г. Москва, улица Полины Осипенко, дом 64, к. 2, кв. 5

Магазин: Sunlight
Номер бонусной карты: 34257238723
ФИО: Осипова Мария Петровна
Дата рождения: 01.02.1990
Город: Москва
Улица: Полины Осипенко
Дом: 64 корпус 2
Квартира: 5



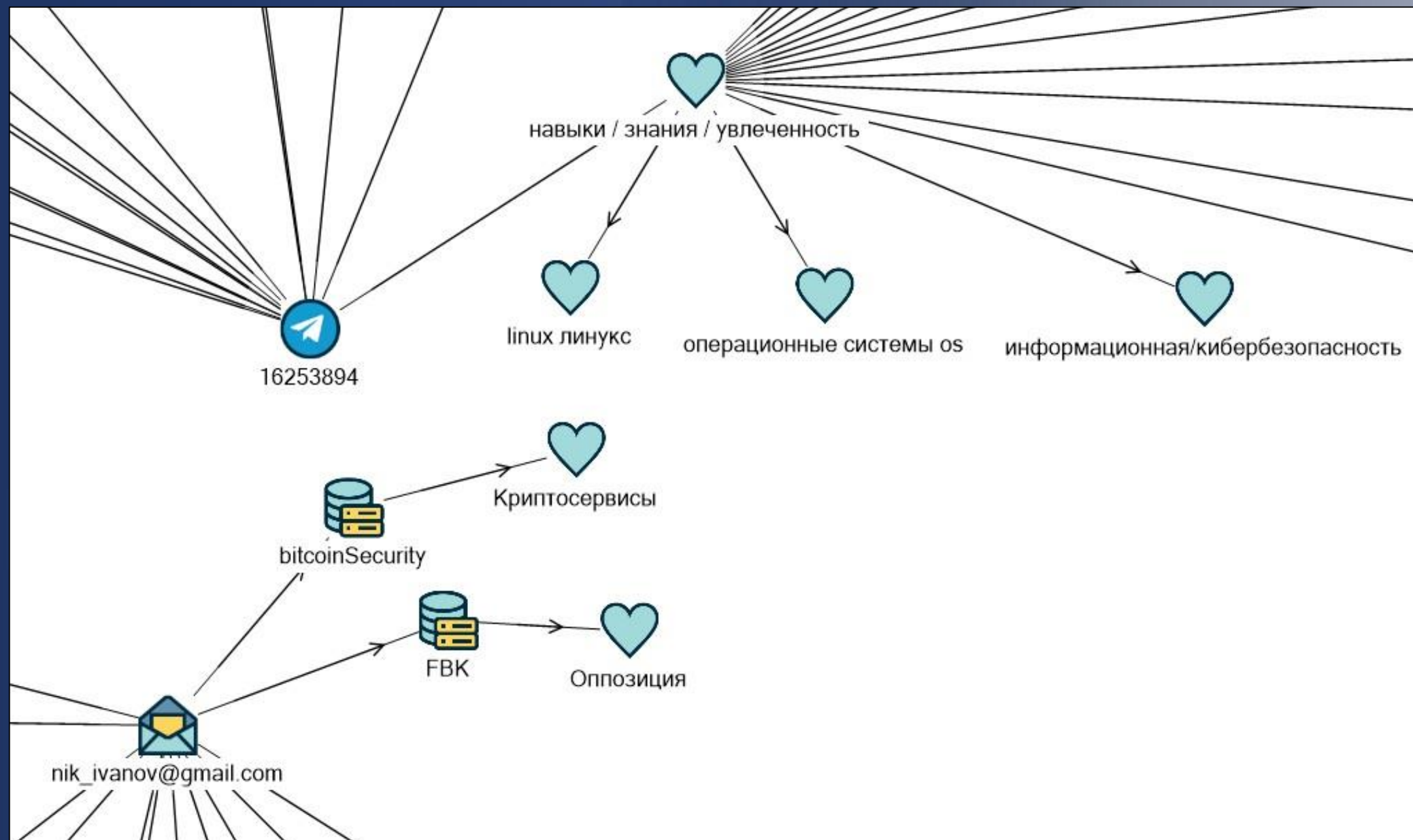
Обработка данных: классификация



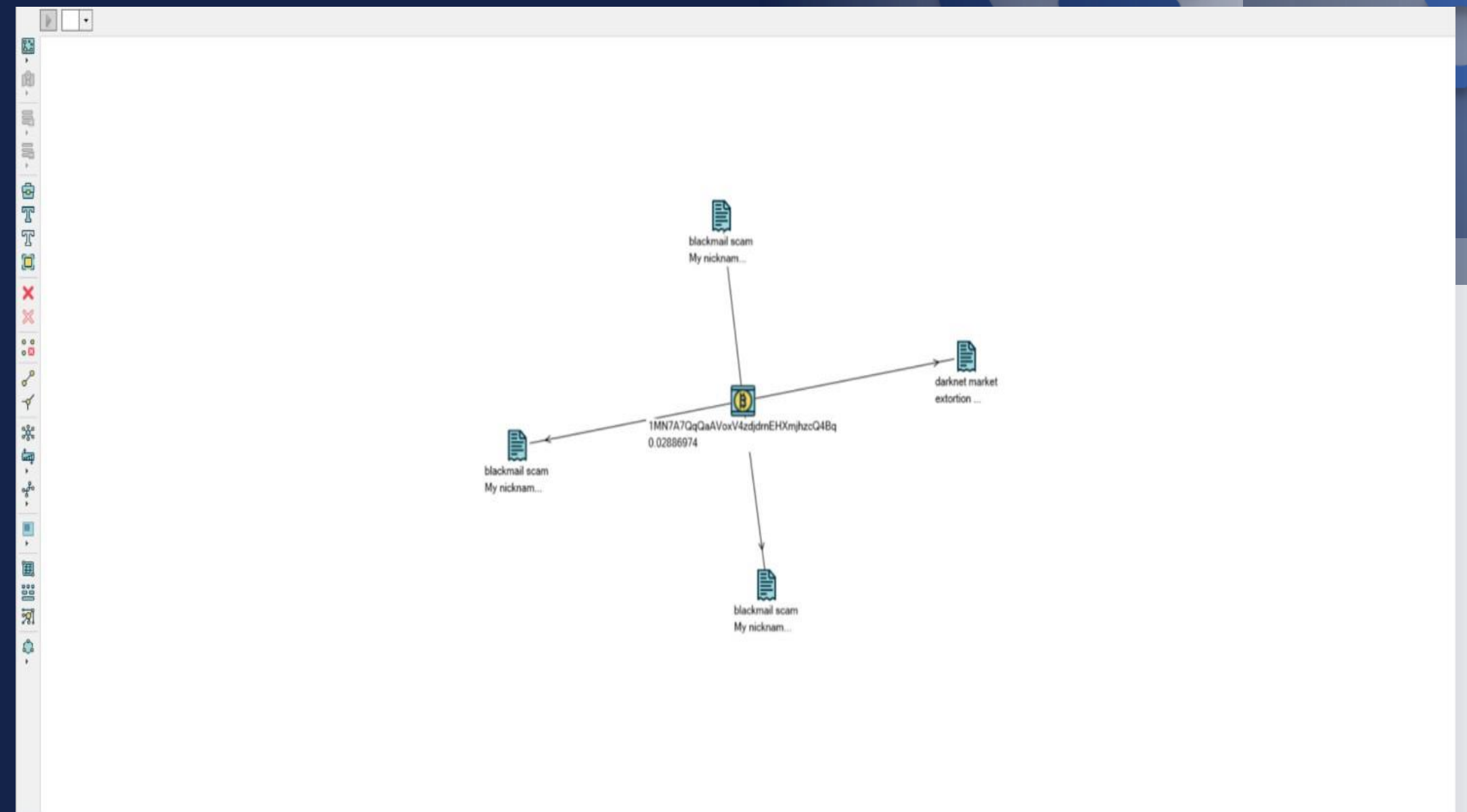
Классификация выявленных результатов



Интерпретация данных для обогащения портрета исследуемого объекта



Пример работы поисковой методики по идентификатору криптовалютного кошелька



Адрес Bitcoin-кошелька	Валюта Bitcoin-кошелька	Репутация Bitcoin-кошелька	Репутация Bitcoin-кошелька (текст)	Тэг Bitcoin-кошелька
я БС	я БС	=	я БС	
1MN7A7QqQaAVoxV4zdjdrnEHXmjhzCQ4Bq	BTC	84	Good	drug_trade
1MN7A7QqQaAVoxV4zdjdrnEHXmjhzCQ4Bq	BTC	84	Good	exchange
1MN7A7QqQaAVoxV4zdjdrnEHXmjhzCQ4Bq	BTC	84	Good	miner
1MN7A7QqQaAVoxV4zdjdrnEHXmjhzCQ4Bq	BTC	84	Good	verified_dient

Аппаратно-программный комплекс Виток-Л

- Предназначен для автоматизации процессов загрузки в хранилище данных информации, поступающей от внешних источников, с её последующей оперативной обработкой и анализом
- Включен в единый реестр российских программ для электронных вычислительных машин и баз данных
- Интеграция с серверной лицензией Виток-ОСИИТ
- Работа со сторонними источниками данных



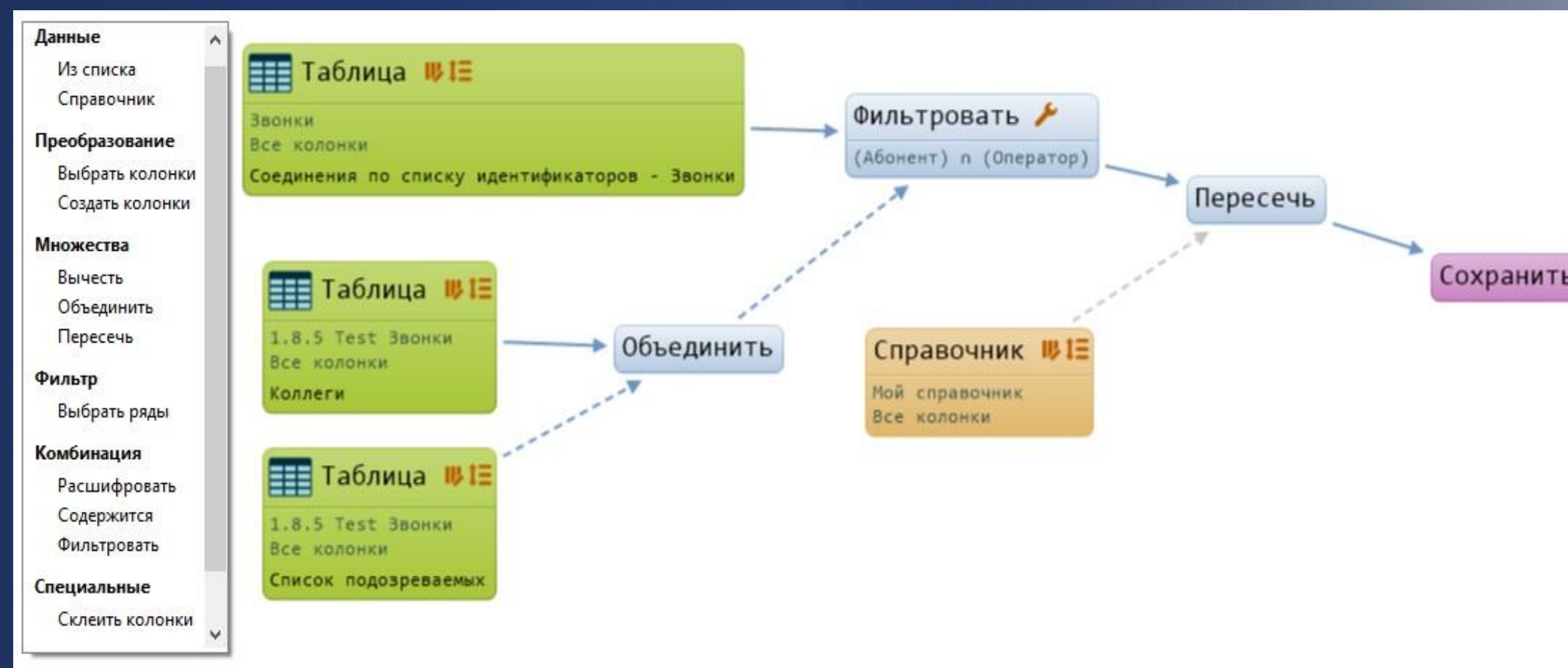
Работа с табличными данными



Источники данных: импортированные файлы, справочники, результаты работы аналитических методик



Функции: фильтрация, логические операции, расшифровка, автоматизация



Межрегиональное взаимодействие



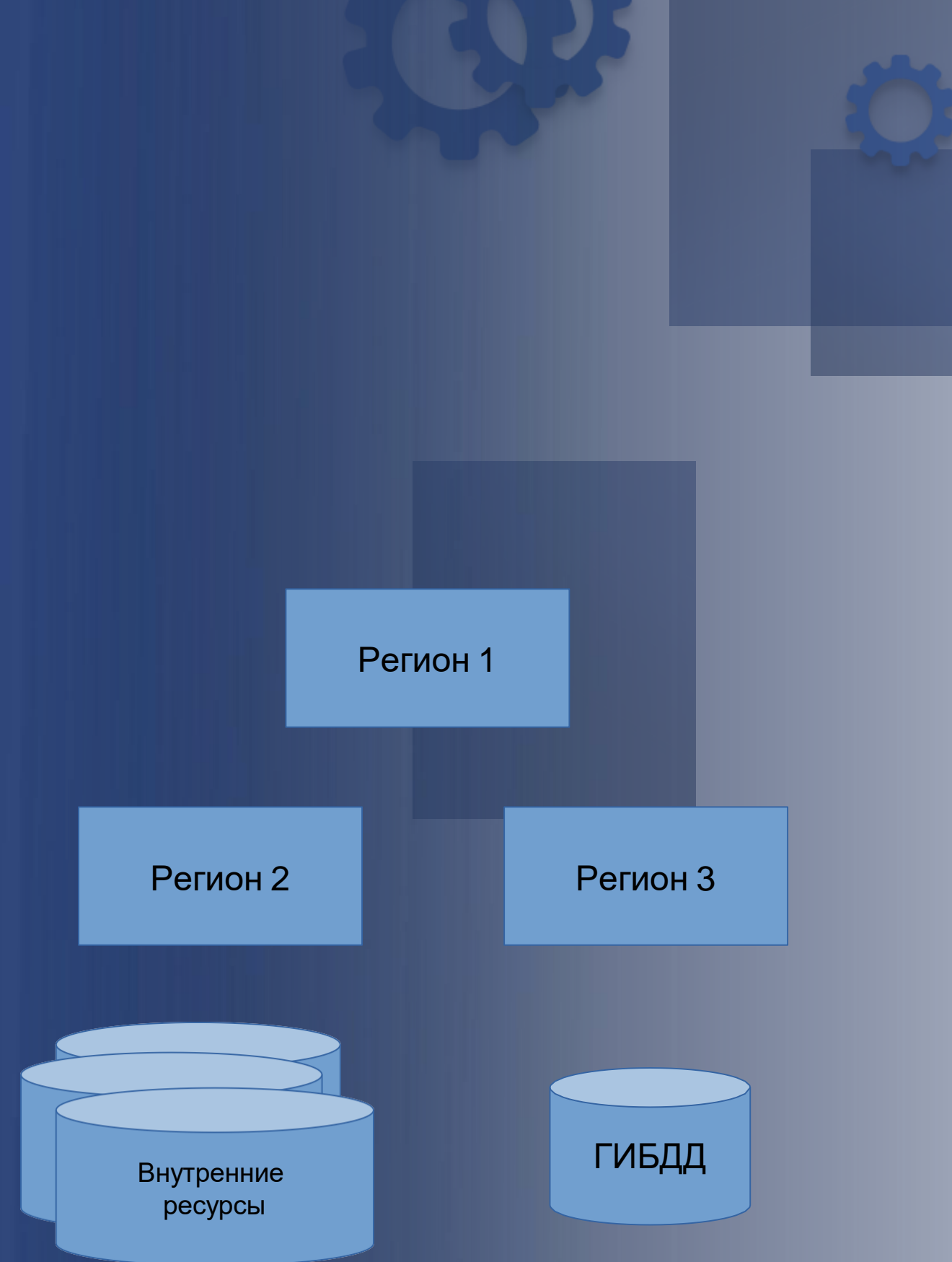
Средства взаимодействия:

- Пользовательские аналитические методики
- Системные аналитические методики



Потенциальные источники:

- Базы данных ГИБДД
- Внутренние ресурсы



Спасибо за внимание!

Адрес:
ул. Б. Новодмитровская,
12, стр. 15, Москва

По вопросам договорных
отношений:
osint@norsi-trans.ru

Техническая поддержка:
Телеграм: @nt_helpdesk
+7 (495) 995-88-82
+7 (495) 748-74-84
sd@norsi-trans.ru