

ОЛЬГА ГУТМАН

ГЕНЕРАЛЬНЫЙ ДИРЕКТОР

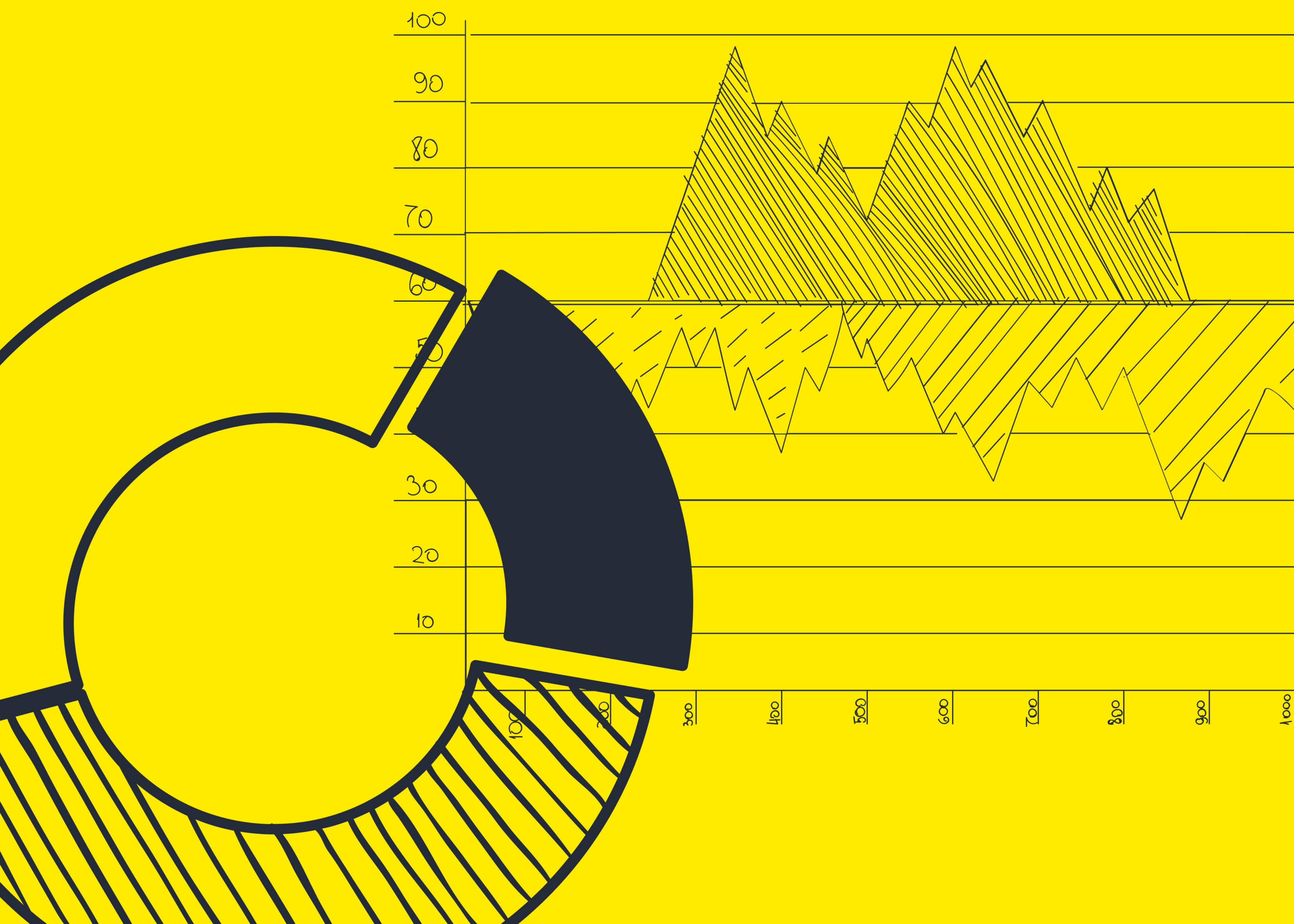


MIKO
SYSTEMS

ЦИФРОВАЯ КРИМИНАЛИСТИКА ДЛЯ КОРПОРАТИВНОГО СЕГМЕНТА



СТАТИСТИКА



ЗДЕСЬ МОГЛА БЫ БЫТЬ
СТАТИСТИКА...

НО!

УГРОЗЫ

- Штрафы от регуляторов и репутационные потери в связи с утечками данных
- Атаки с целью остановки деятельности предприятия
- Хищения коммерческой тайны и чувствительной информации, промышленный шпионаж
- Мошенничество и инсайдерство
- Атаки программ-вымогателей (ransomware) с целью хищения денежных средств
- Вымогательство с использованием вирусов-шифровальщиков
- Заражение промышленных сетей программами-майнерами

ВАРИАНТЫ

РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

- Быстрое восстановление работы компании
- Сбор информации и проведение расследования

КОМУ ВАЖНО РАССЛЕДОВАТЬ ИНЦИДЕНТЫ

- Предприятия гос. сектора
- Телекоммуникационные компании
- Компании финансового сектора
- Предприятия промышленности
- IT-компании

ЦЕЛИ

РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ

- Деньги-деньги-деньги!
- 152 ФЗ
- Штрафы для финансовых организаций
- Повышение уровня кибербезопасности
- Разработка регламентов для реагирования

ЧТО ТАКОЕ

DFIR

DFIR

Digital Forensics and Incident Response

**«ЦИФРОВАЯ КРИМИНАЛИСТИКА
И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ»** –
специализированная область, охватывающая
выявление, устранение и расследование
инцидентов кибербезопасности, в том числе
с применением криминалистических практик.

DFIR

НЕ ЗАЩИЩАЕТ

DFIR

НЕ КОНКУРЕНТ:

- Антивирусам
- DLP
- SIEM
- SOAR
- EDR
- Прочим системам защиты

4 ОСНОВНЫХ ЭТАПА

ПЕРВИЧНОЙ РАБОТЫ С ЦИФРОВЫМИ ДОКАЗАТЕЛЬСТВАМИ

- Идентификация
- Сбор
- Извлечение
- Хранение

ISO/IEC 27037:2012

ИДЕНТИФИКАЦИЯ

- Кто вовлечен в инцидент?
- Что случилось?
- Когда произошел инцидент?
- Где произошел инцидент?
- Как произошел инцидент?

СБОР

Изолирование «места преступления», идентификация и документация устройств и источников данных:

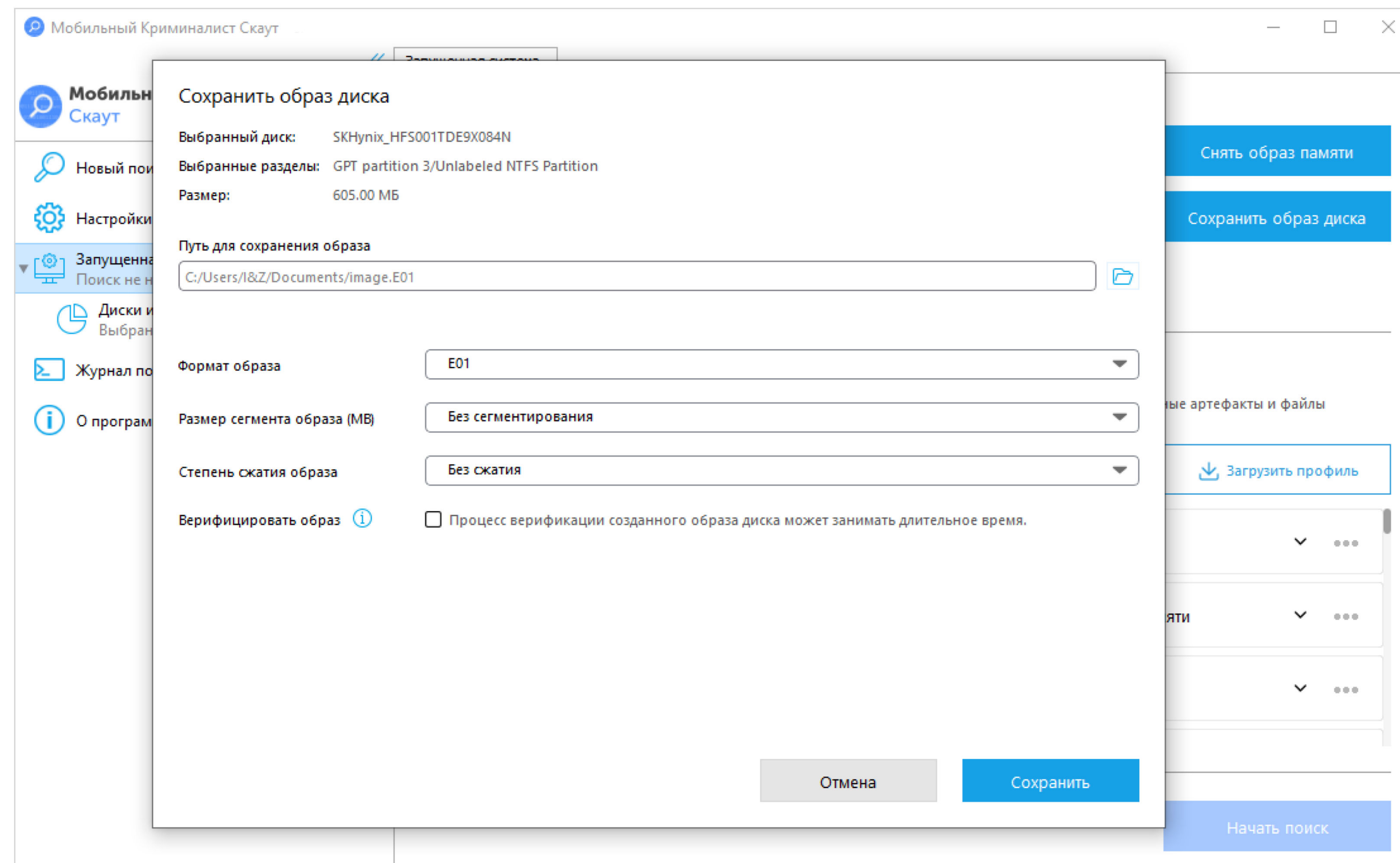
- Техническое состояние (включено/выключено/режим ожидания)
- Физическое состояние (царапины, следы вскрытия и т.д.)
- Серийные номера
- Модели
- Сетевые соединения
- Другое

ИЗВЛЕЧЕНИЕ ДАННЫХ

Если нет витальных предпосылок к обратному, этот этап должен проводиться не «на месте», а в специально оборудованной лаборатории.

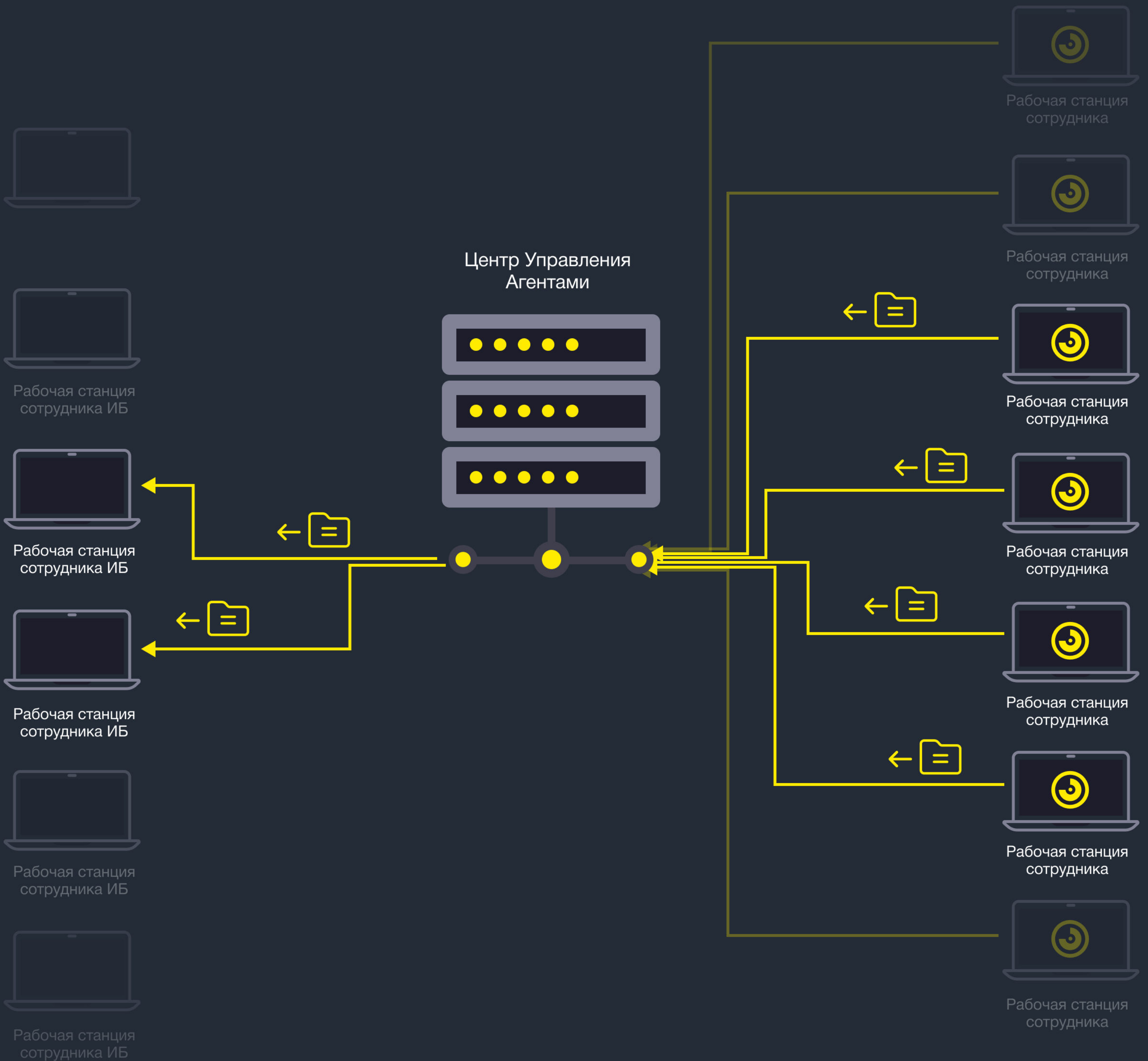
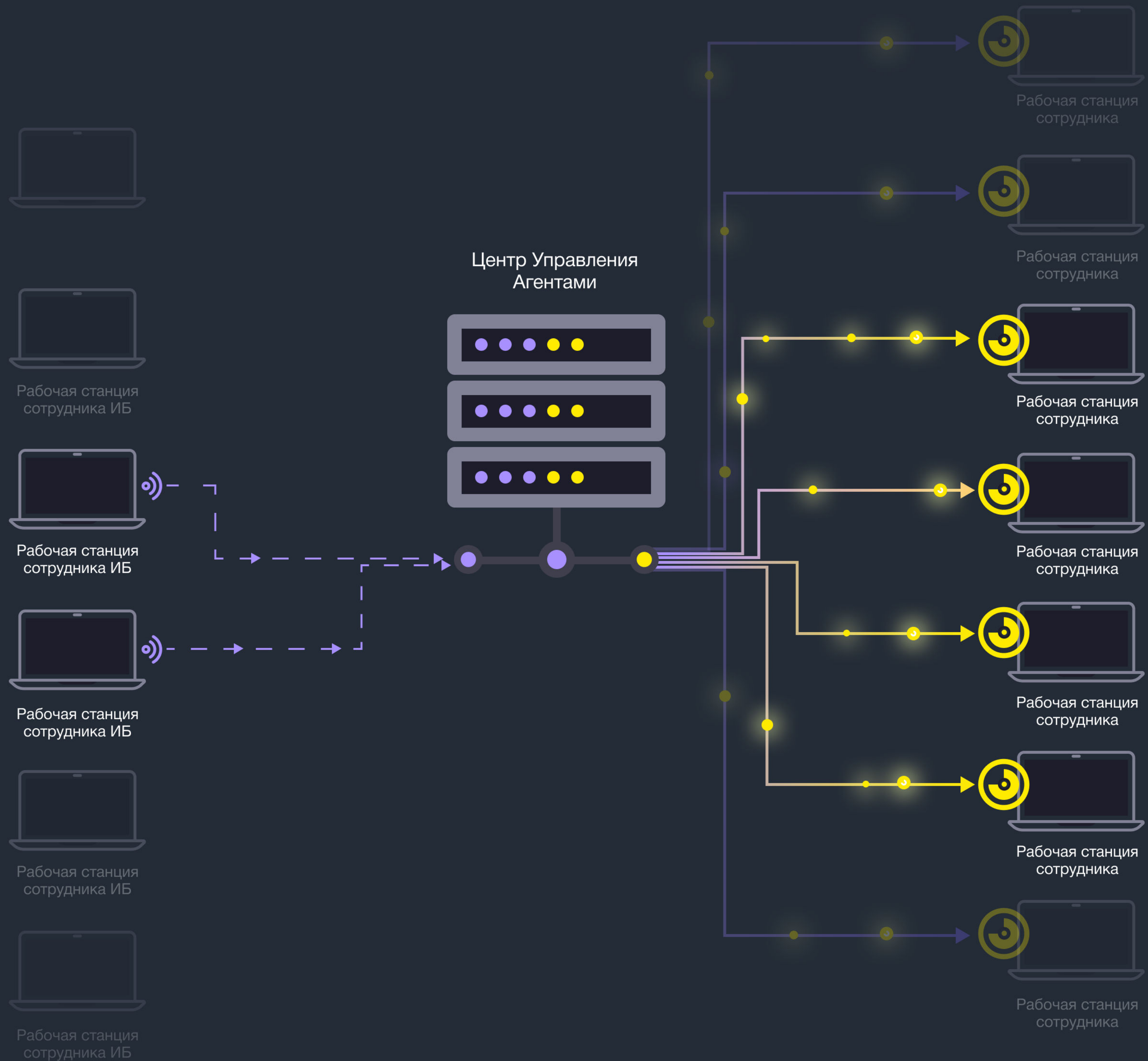
- Серверы
- Рабочие станции (ПК сотрудников)
- Оперативная память
- Мобильные устройства
- Облачные сервисы
- Внешние носители данных

ИЗВЛЕЧЕНИЕ ДАННЫХ



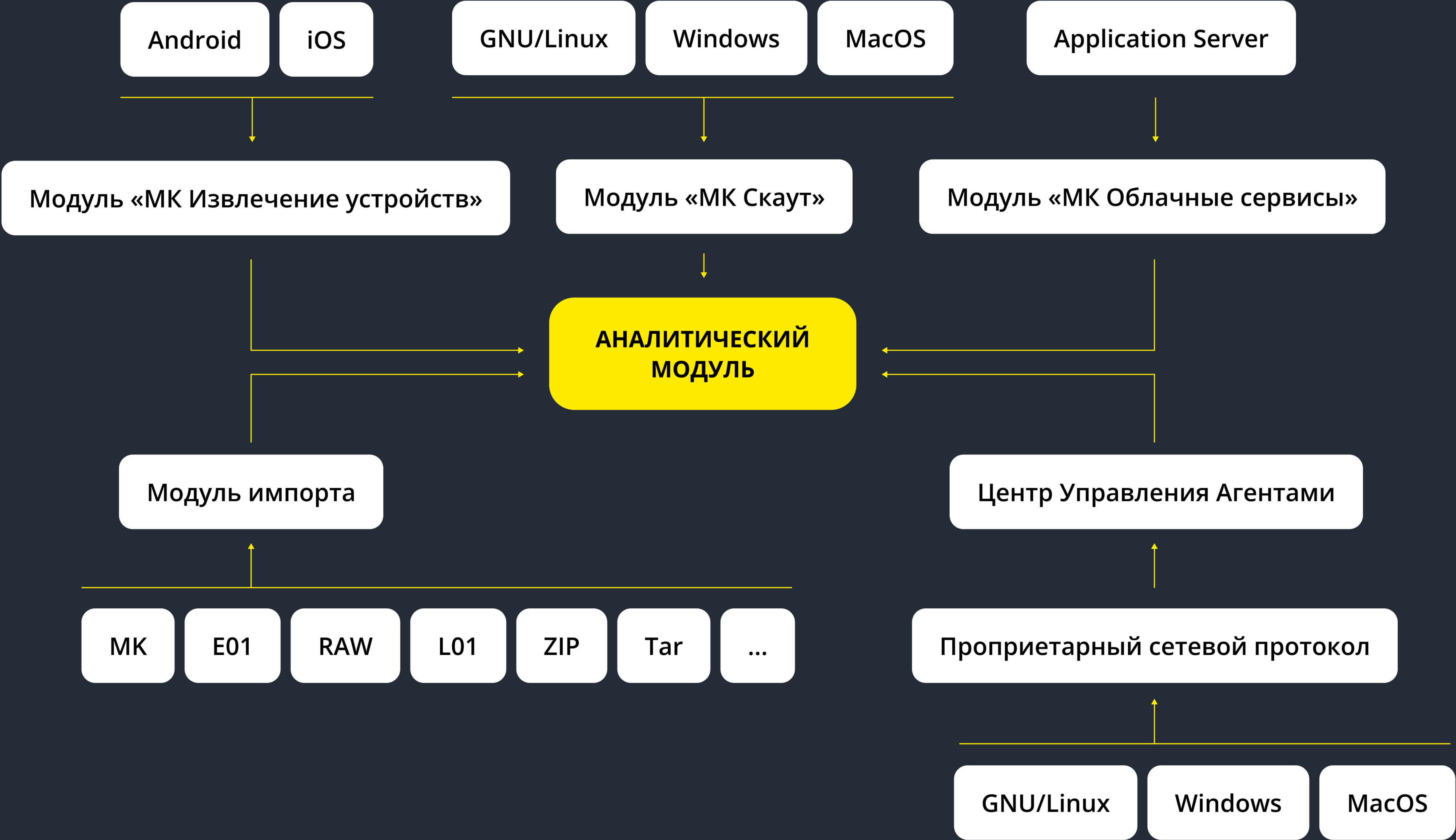
ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ РАБОЧИХ СТАНЦИЙ

АГЕНТСКИЙ РЕЖИМ



ИЗВЛЕЧЕНИЕ ДАННЫХ

АРХИТЕКТУРА ВЗАИМОДЕЙСТВИЯ МОДУЛЕЙ «МК ENTERPRISE»:



ХРАНЕНИЕ ДАННЫХ

- Предотвращение модификации данных
- Обеспечение их целостности

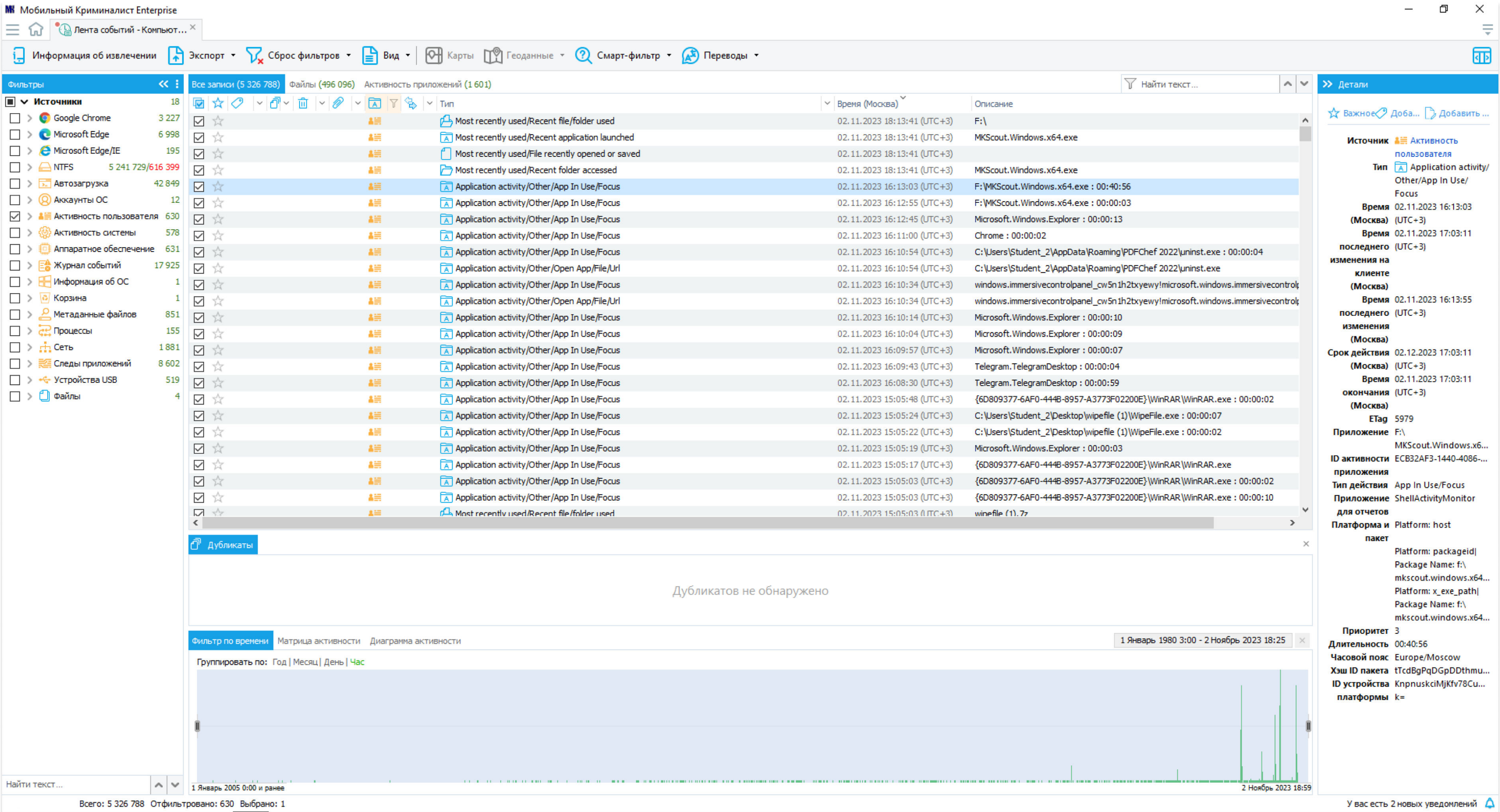
АНАЛИЗ

(ИЗУЧЕНИЕ
И ИНТЕРПРЕТАЦИЯ
ДАННЫХ)

- Все данные, аспекты и доступная информация переданы эксперту
- Поставлены и разъяснены все цели и задачи расследования
- Воссоздается хронология событий инцидента

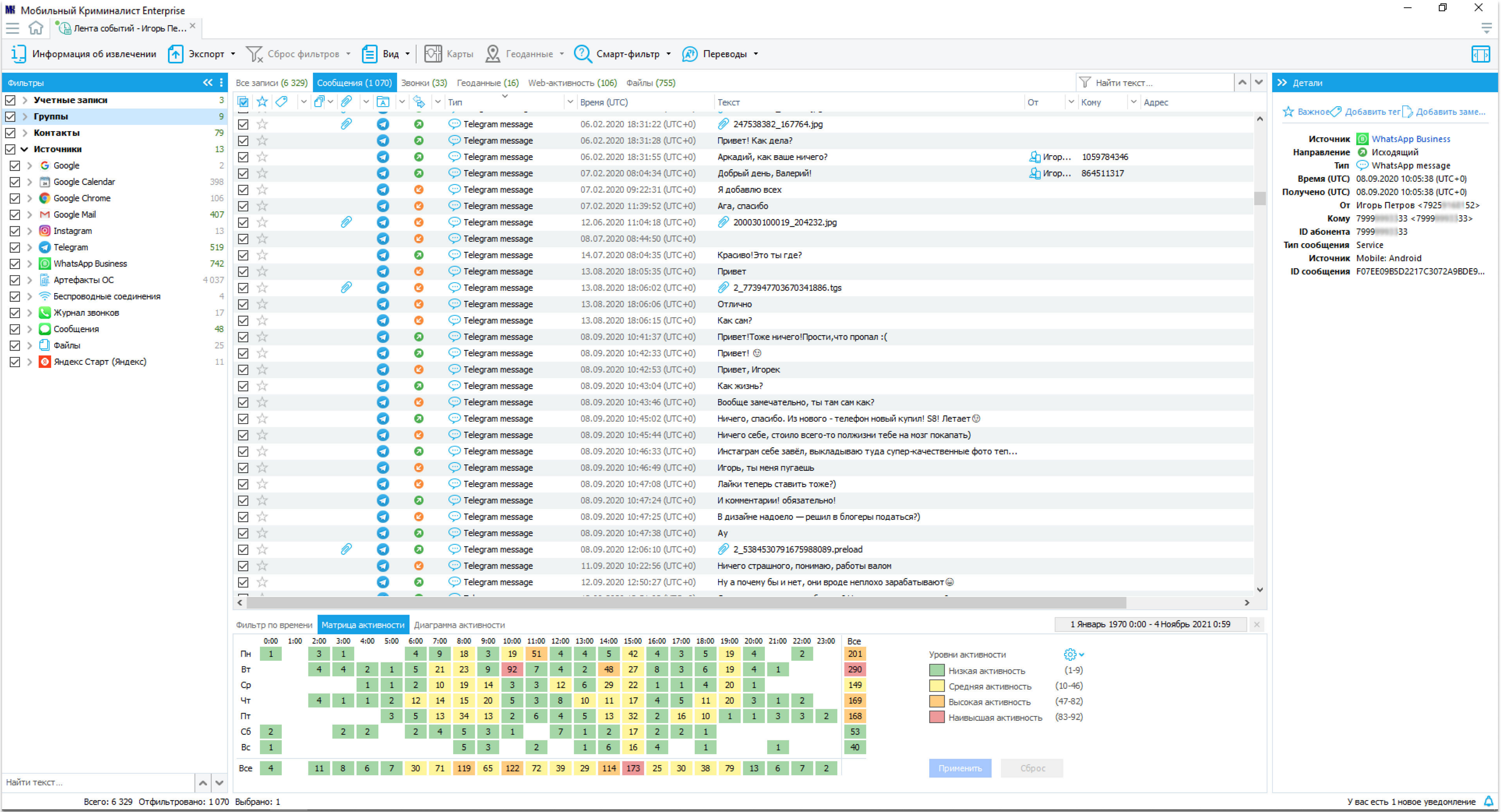
АНАЛИЗ

ЛЕНТА СОБЫТИЙ



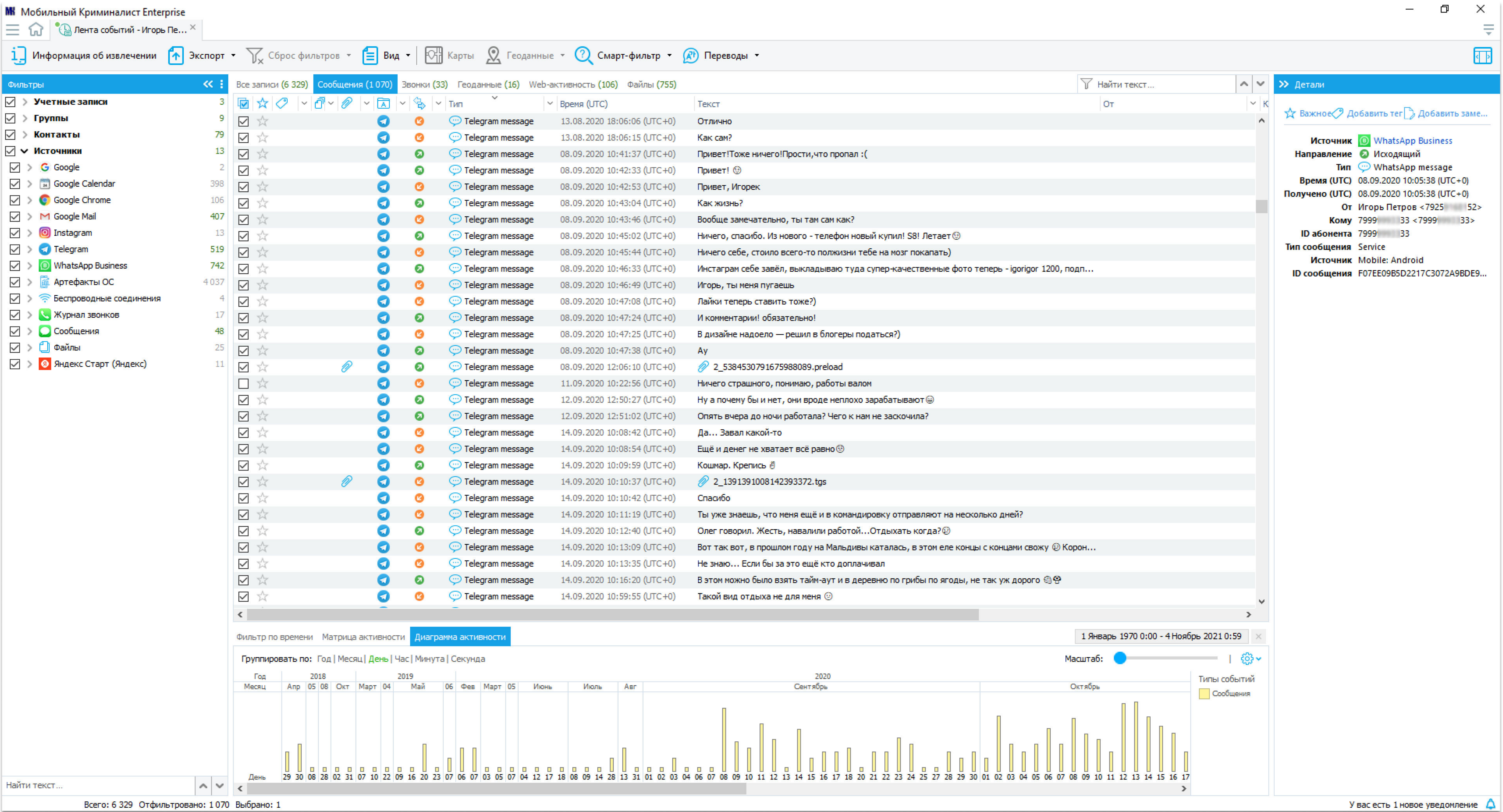
АНАЛИЗ

МАТРИЦА АКТИВНОСТИ



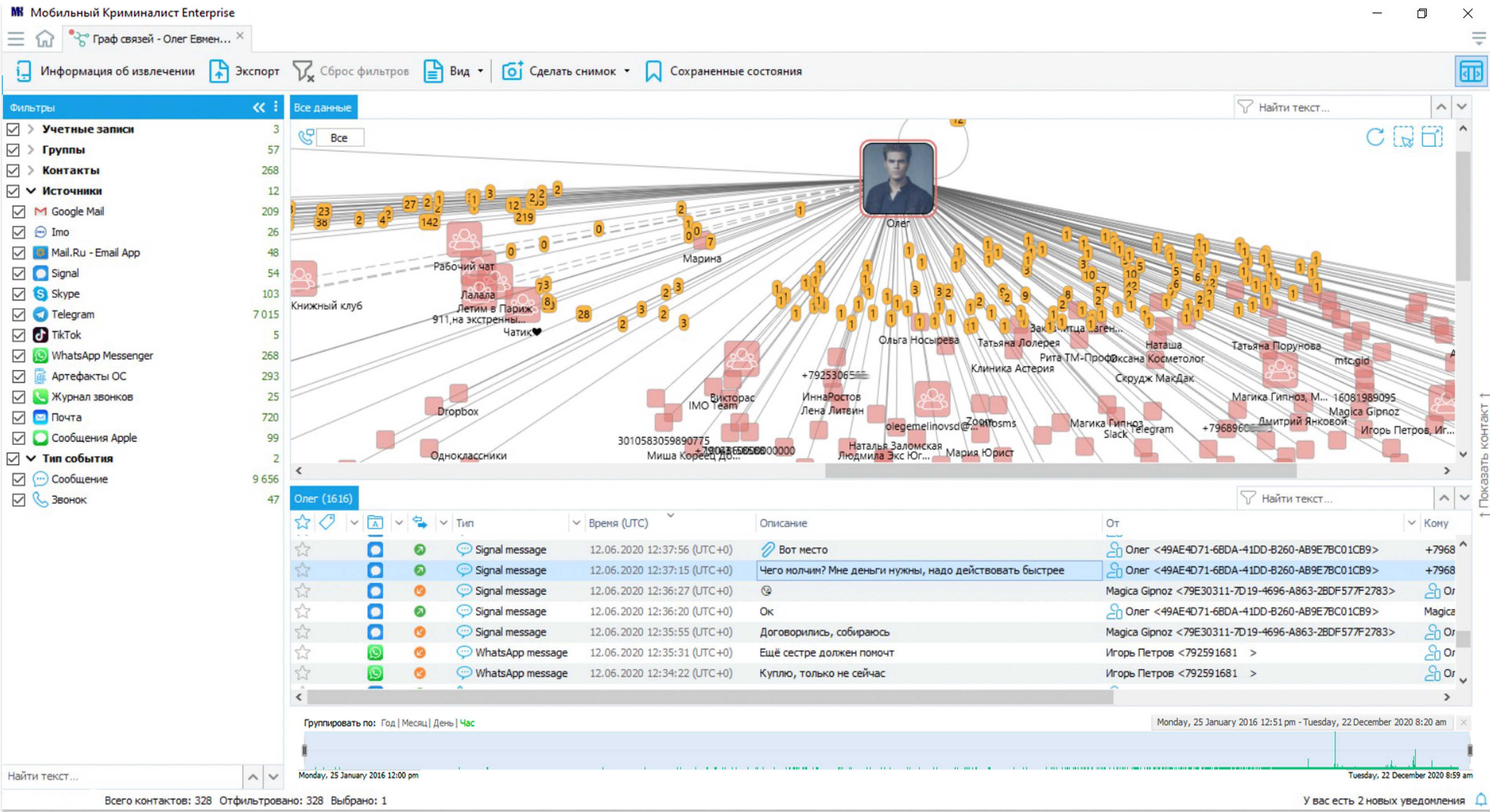
АНАЛИЗ

ДИАГРАММА АКТИВНОСТИ



АНАЛИЗ

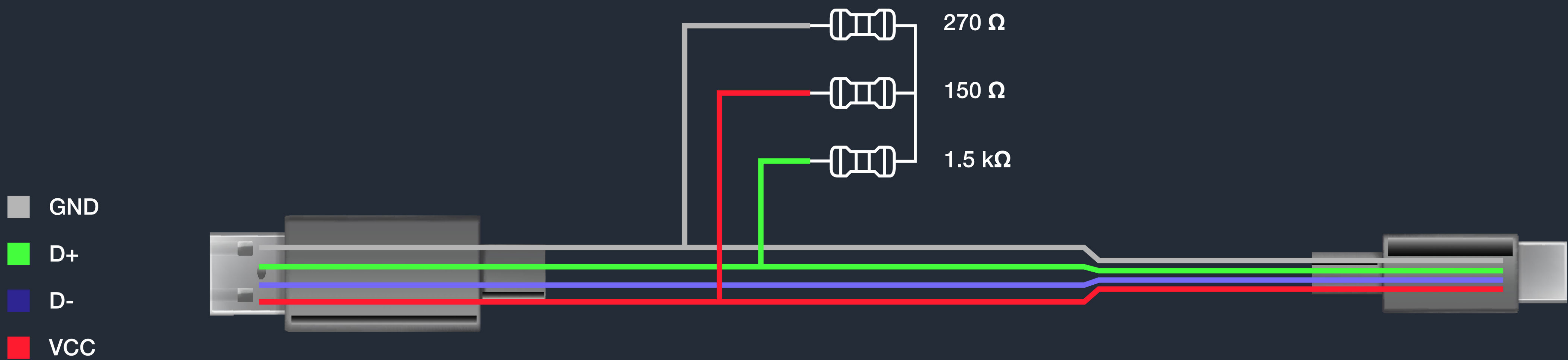
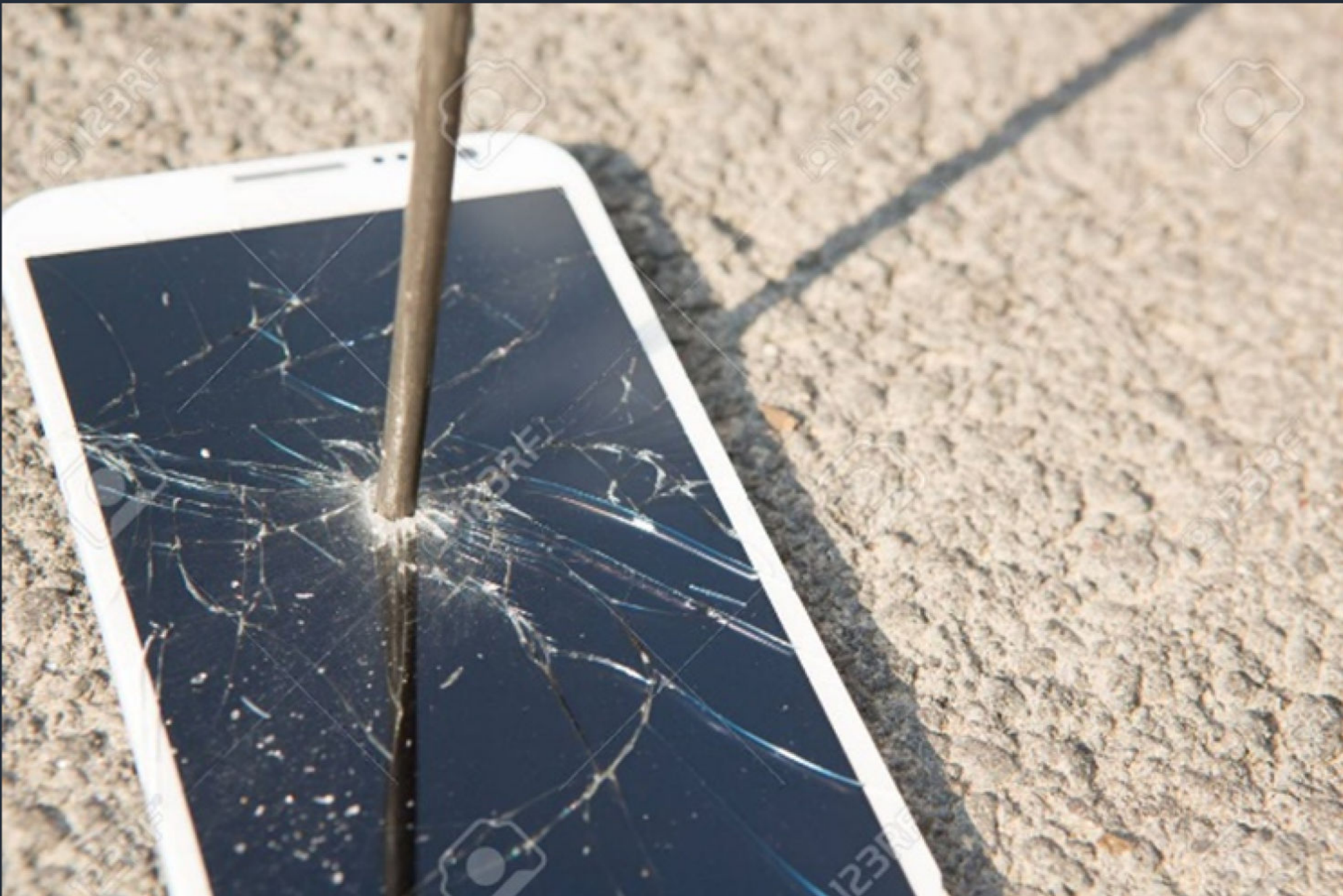
ГРАФ СВЯЗЕЙ



ОТЧЕТ

- Описывает все действия на каждом этапе расследования
- Описывает все результаты каждого из этапов
- Понятен и прозрачен
- На базе отчета будет написан регламент (обновлен Playbook)

ЦЕННОСТЬ ПЕРСОНАЛА



СПАСИБО

КОНТАКТЫ:

 +7 (495) 909-92-78

 clients@mko-systems.ru

 mko-security.ru