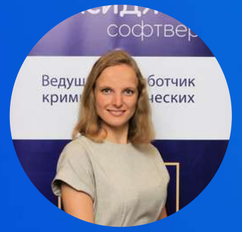
«Следуя трендам. Форензиковый продукт в расследовании инцидентов»

Оксиджен софтвер



Ольга Гутман

Генеральный директор

ИЗВЛЕЧЕНИЕ ИНФОРМАЦИИ ИЗ ЦИФРОВЫХ ИСТОЧНИКОВ

- Рабочие станции, внешние жесткие диски
- Мобильные гаджеты и мультимедийные устройства
- Облачные сервисы
- Дроны

НАШИ ПРОДУКТЫ

Мобильный Криминалист Эксперт

Для проведения комплексной цифровой экспертизы данных из мобильных устройств, облачных сервисов и персональных компьютеров

Мобильный Криминалист Enterprise

Для расследования корпоративных инцидентов и проведения аудита путем извлечения данных из рабочих станций, мобильных устройств и облачных сервисов

Мобильный Криминалист Десктоп

Для извлечения и анализа данных из рабочих станций на Windows, macOS, GNU/Linux или образов с файловой системой NTFS

Мобильный Криминалист Экспертный Центр

Разновидность лицензии продукта «МК Эксперт» для одновременной работы с программой нескольких сотен человек

КЕЙСЫ, КОТОРЫЕ ЧАЩЕ ВСЕГО РАССЛЕДУЮТ С ПРИМЕНЕНИЕМ ИНСТРУМЕНТОВ DFIR (DIGITAL FORENSICS & INCIDENT RESPONSE)

ФИШИНГ

ВРЕДОНОСНОЕ ПО

МОШЕННИЧЕСТВО

НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ АКТИВОВ КОМПАНИИ/НАРУШЕНИЕ ВНУТРЕННИХ ПОЛИТИК

УТЕЧКА ДАННЫХ

E-DISCOVERY

ПРОГРАММЫ-ВЫМОГАТЕЛИ

УВОЛЬНЕНИЕ СОТРУДНИКА С РАБОТЫ

ЗАПРЕЩЕННЫЕ ПРИЛОЖЕНИЯ

ХАРАССМЕНТ

ПРИЧИНЫ, ПО КОТОРЫМ НЕОБХОДИМО ИСПОЛЬЗОВАНИЕ DFIR-ИНСТРУМЕНТОВ

Рост количества источников информации и ее объема

Совершенствование атак в технологическом плане

Все более частое использование мобильных устройств в бизнес-процессах

Рост угрозы инсайдерства

Потребность в удаленном извлечении данных из цифровых источников

Рост влияния теневой IT-среды

ВЫПУСК «МК ENTERPRISE»

УНИКАЛЬНЫЙ ФУНКЦИОНАЛ

Удаленное извлечение данных из одной или группы рабочих станций (Windows, macOS, GNU/Linux)

Поддержка корпоративных облачных сервисов:

- Amazon EC2
- Google Admin
- Microsoft Teams
- Microsoft SharePoint
- Amazon S3
- и других

MK ENTERPRISE

КОНТРОЛИРУЯ БУДУЩЕЕ

МОБИЛЬНЫЙ КРИМИНАЛИСТ ДЕСКТОП

ДОБАВЛЕНО В ПОДДЕРЖКУ ЗА 2021:

- 700 МОДЕЛЕЙ МОБИЛЬНЫХ УСТРОЙСТВ
- 89 ПРИЛОЖЕНИЙ И 5 700 ИХ ВЕРСИЙ
- 38 ИСТОЧНИКОВ ДАННЫХ ИЗ РАБОЧИХ СТАНЦИЙ
- 12 ОБЛАЧНЫХ СЕРВИСОВ

РАБОТАЕМ В 8 СТРАНАХ!

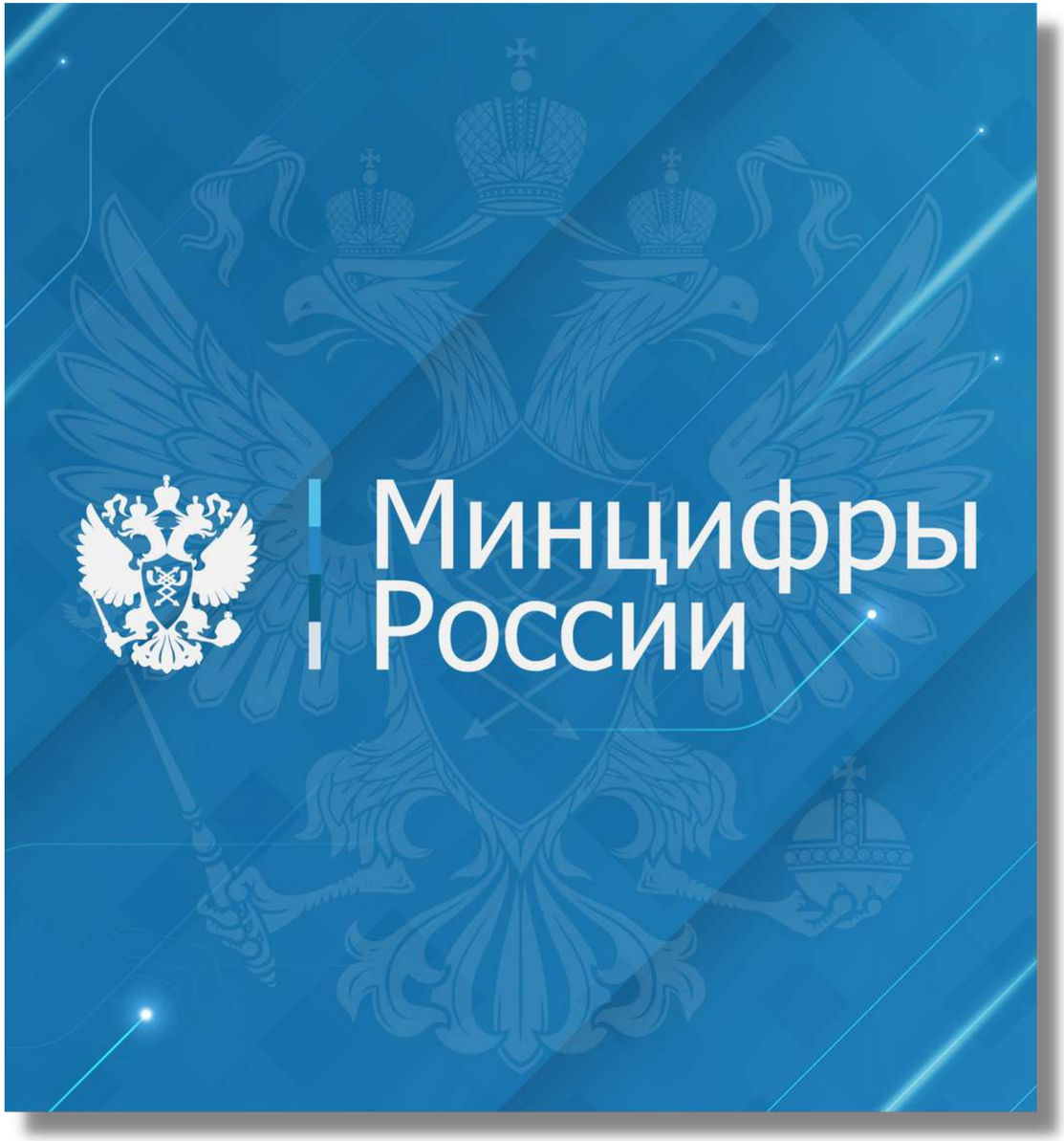
- РОССИЯ
- БЕЛАРУСЬ
- АРМЕНИЯ
- КАЗАХСТАН
- УЗБЕКИСТАН
- МОЛДАВИЯ
- ТАДЖИКИСТАН
- ЮЖНАЯ ОСЕТИЯ

ДОСТИЖЕНИЯ 2021 ГОДА

Все продукты бренда «Мобильный Криминалист» были добавлены в реестр отечественного ПО Минкомсвязи (Минцифры).

Развитие в новых направлениях компаний-клиентов:

- большая четверка (аудит и консалтинг)
- компании, проводящие расследования инцидентов
- крупные корпорации, представляющие группы компаний из разных сфер экономики



ОБУЧАЮЩИЙ КУРС

- В 2021 году прошло несколько потоков обучающих курсов
- Выдача удостоверения о повышении квалификации по итогам успешного окончания курса
- 5 дней (40 часов)
- Объёмная практическая и теоретическая части
- Аудитория курса: специалисты в области цифровой криминалистики, информационной безопасности

МЕРОПРИЯТИЯ 2021

MOBILE FORENSICS DAY 2021

- 5 юбилейная конференция
- 300 Участников

Семинары по всей России

Регулярные вебинары

30 Мероприятий

ФУНКЦИИ, РЕАЛИЗОВАННЫЕ В 2021 Г.

ИССЛЕДОВАНИЕ РАБОЧИХ СТАНЦИЙ

Извлечение данных из группы рабочих станций на Windows средствами Active Directory

Исследование данных внешнего диска ПК

Поддержка операционной системы Windows 11

Удаленное извлечение данных:

- из рабочих станций на macOS и GNU/Linux через SSH-протокол
- из ПК на Windows через протокол DCOM/RPC

Копирование содержимого оперативной памяти компьютера (RAM) на ОС Windows

Поддержка файловых систем FAT, EXT2/3/4, HFS/ HFS+

Поиск и анализ данных:

- по логическим образам L01
- по образам RAW: DD, BIN и IMG, а также по многотомным образам RAW
- по образам VDI, VHD, VMDK
- по образам DMG, ISO
- по логическим образам 7Z, RAR, TAR

ФУНКЦИИ, РЕАЛИЗОВАННЫЕ В 2021 Г.

ИССЛЕДОВАНИЕ РАБОЧИХ СТАНЦИЙ

Системные артефакты (Windows)

- списки пользовательских сессий
- информация об отложенных перемещениях файлов
- списки установленных обновлений Windows
- System Resource Usage Monitor
- списки индексируемых файлов
- списки исполняемых процессов

Системные артефакты (macOS)

- списки пользовательских сессий
- сохранение сведений о всех дисках и разделах системы
- данные об установленных приложениях
- история консольных команд, введенных в терминале
- System Resource Usage Monitor
- информация об автоматически запускаемых программах
- данные системных журналов
- системные пользовательские настройки
- журналы событий (Apple Unified Logs)

Системные артефакты (GNU/Linux)

- списки пользовательских сессий
- данные системных журналов

Новые приложения

- VIPole
- Element Messenger
- Instagram для браузера Google Chrome
- Discord (Windows, macOS)
- Chatwork (Windows, macOS)
- GroupMe (Windows)
- Zello (Windows)
- Your Phone (Windows)

MK Enterprise

- CA Flowdock
- Twist
- Microsoft Teams

ФУНКЦИИ, РЕАЛИЗОВАННЫЕ В 2021 Г.

ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ МОБИЛЬНЫХ УСТРОЙСТВ

Извлечение полной файловой системы и данных Keychain из Apple-устройств на iOS версии 12.5.2, 12.5.3, 14.4.1, 14.4.2, 14.5.1, 14.6 и 14.8

Поддержка Huawei-устройств на чипсетах Qualcomm

Извлечение данных из вторых пространств устройств брендов Huawei и Samsung

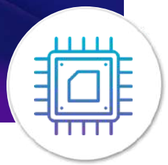
Поддержка Samsung Exynos-устройств на Android 9 - 11 версии

ФУНКЦИИ, РЕАЛИЗОВАННЫЕ В 2021 Г.

ИЗВЛЕЧЕНИЕ ДАННЫХ ИЗ МОБИЛЬНЫХ УСТРОЙСТВ

Поддержка Qualcomm-устройств бренда LG

Извлечение данных из MediaTek-устройств на чипсете MT6753



«МК Агент»: добавлена поддержка приложений Twitter, Line, Telegram, Viber, Wickr Me

Функция понижения версий приложений

ФУНКЦИИ, РЕАЛИЗОВАННЫЕ В 2021 Г.

ДОСТУП К ДАННЫМ ОБЛАЧНЫХ СЕРВИСОВ

- Grindr (iCloud/Google Backup)
- MEGA
- GroupMe
- Chatwork
- Google Admin
- Amazon EC2
- Amazon S3
- Microsoft Teams
- Microsoft SharePoint

ФУНКЦИИ, РЕАЛИЗОВАННЫЕ В 2021 Г.

АНАЛИТИЧЕСКИЙ ФУНКЦИОНАЛ

Объединение нескольких извлечений в одно на уровне данных или файловой системы

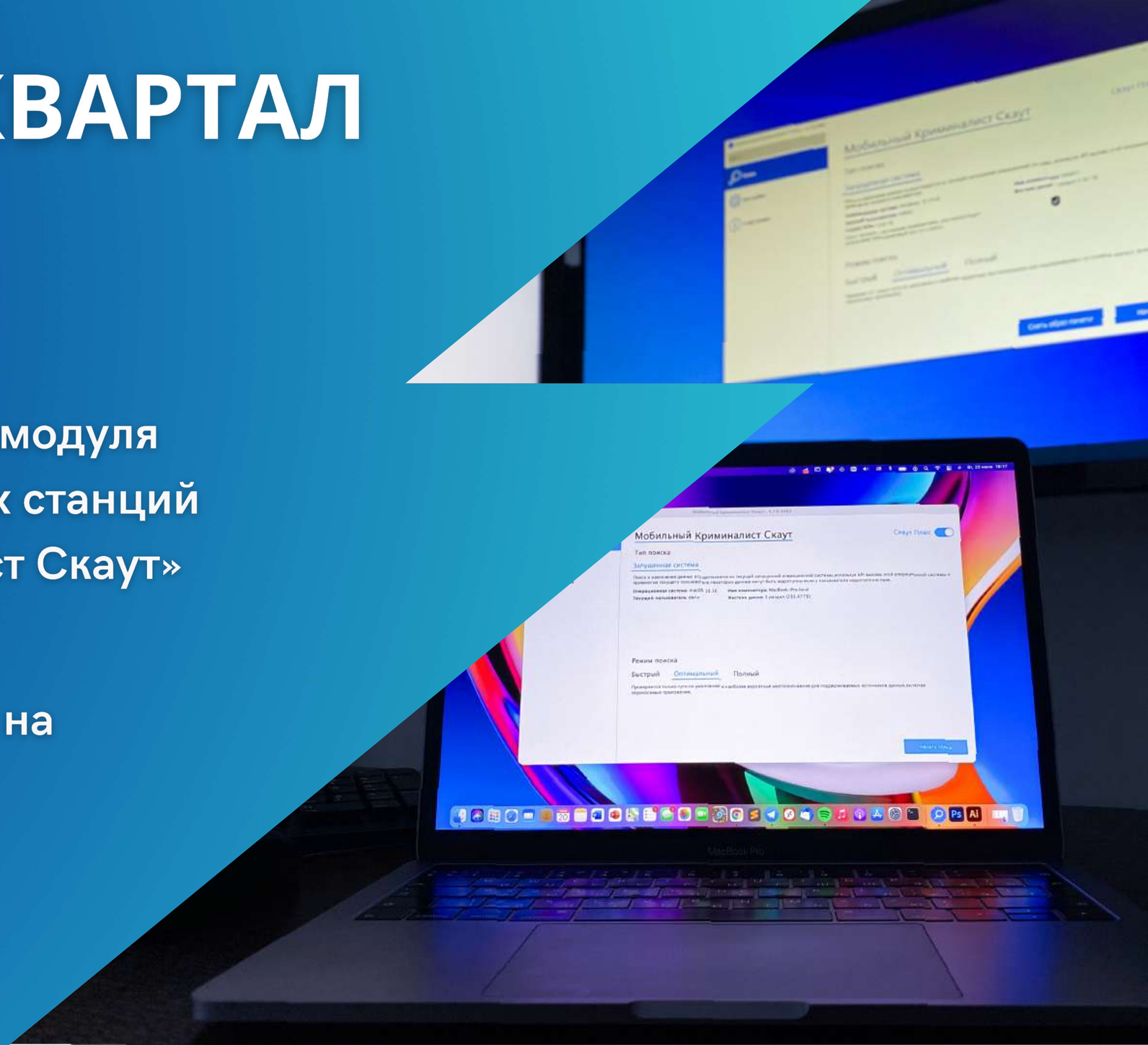
Добавлен менеджер паролей

Усовершенствован механизм восстановления удаленных данных приложений

Реализован новый механизм восстановления удаленных данных в SQLite-базах

ПЛАНЫ НА 1 КВАРТАЛ 2022 ГОДА

- Агентский режим работы модуля по исследованию рабочих станций «Мобильный Криминалист Скаут»
- Брутфорс пароля iPhone 7 и iPhone 7 Plus на iOS 14.0 и выше



Планы на 2022 год

Извлечение данных из рабочих станций

1. **Экспресс-триаж всех компьютеров сети по заданным критериям**
2. **Мониторинг переписки WhatsApp и Telegram в реальном времени при заданных условиях**
3. **Мониторинг действий пользователя в реальном времени при заданных условиях**

Планы на 2022 год

Извлечение данных из мобильных устройств

1. Агент для iOS-устройств
2. Подбор пароля на Samsung Exynos-устройствах на Android 9-11
3. Развитие поддержки Android Keystore
4. Извлечение данных из несмартфонных устройств
5. Расширение поддержки устройств на чипсетах MediaTek

Планы на 2022 год

Извлечение данных из облачных сервисов

FLOCK

FLOWDOCK

TWIST

Контакты

Ольга Гутман
Генеральный директор
olga.gutman@oxygensoftware.ru

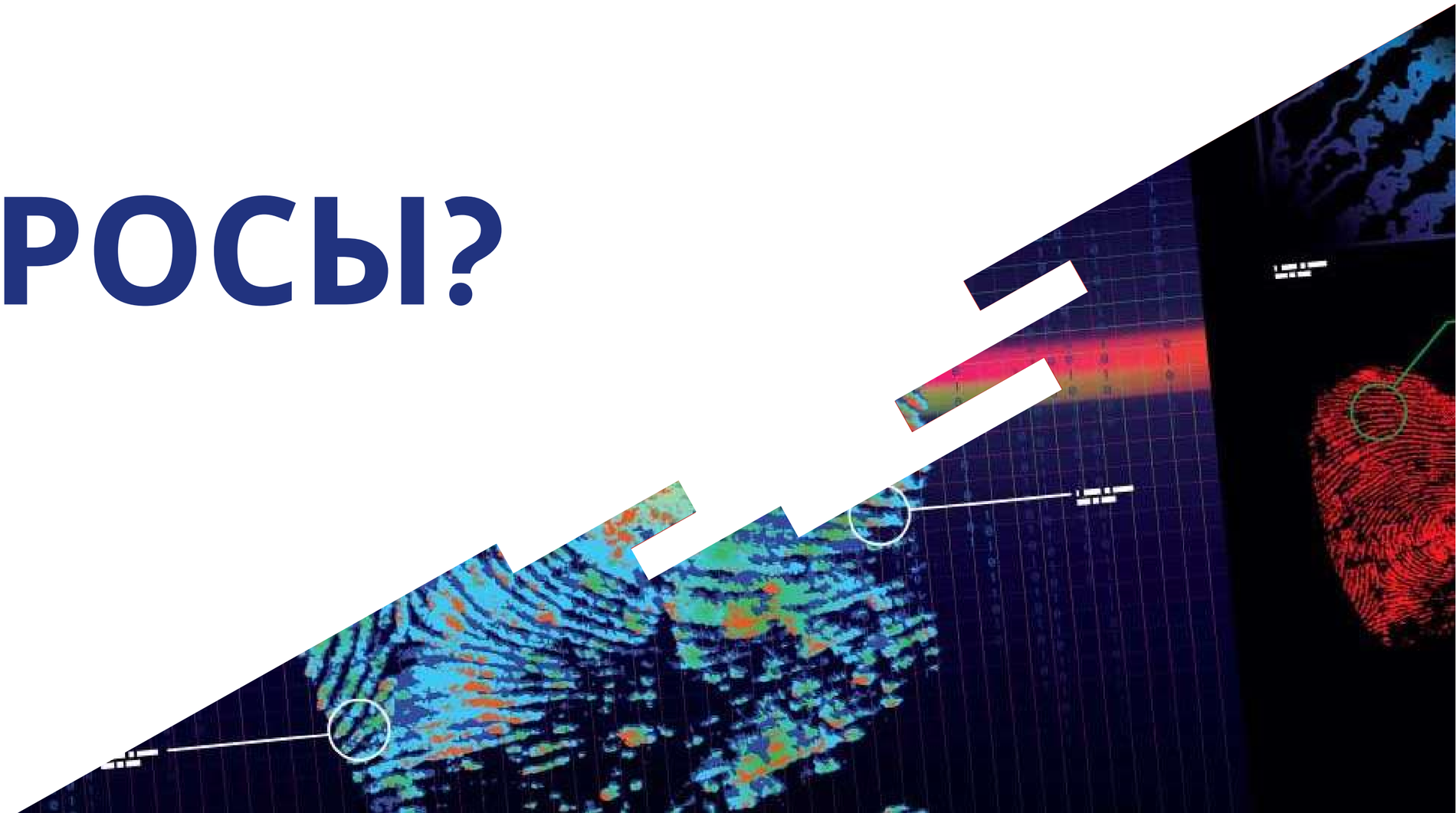
Как получить демоверсию?

ОТПРАВИТЬ ЗАПРОС В СЛУЖБУ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ:
SUPPORT@OXYGENSOFTWARE.RU

Социальные сети

Оксиджен
софтвер

ВОПРОСЫ?



Оксиджен
софтвер

СПАСИБО ЗА ВНИМАНИЕ!