

MOSCOW FORENSICS DAY '25

НИКИТА ПАВЛОВ

«РОЛЬ ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ В
ЦИФРОВОМ РАССЛЕДОВАНИИ: КАК
УДОБСТВО И ИНТУИТИВНОСТЬ UI
УСКОРЯЮТ ПРОЦЕССЫ АНАЛИЗА И ПОИСКА
ДАННЫХ?»

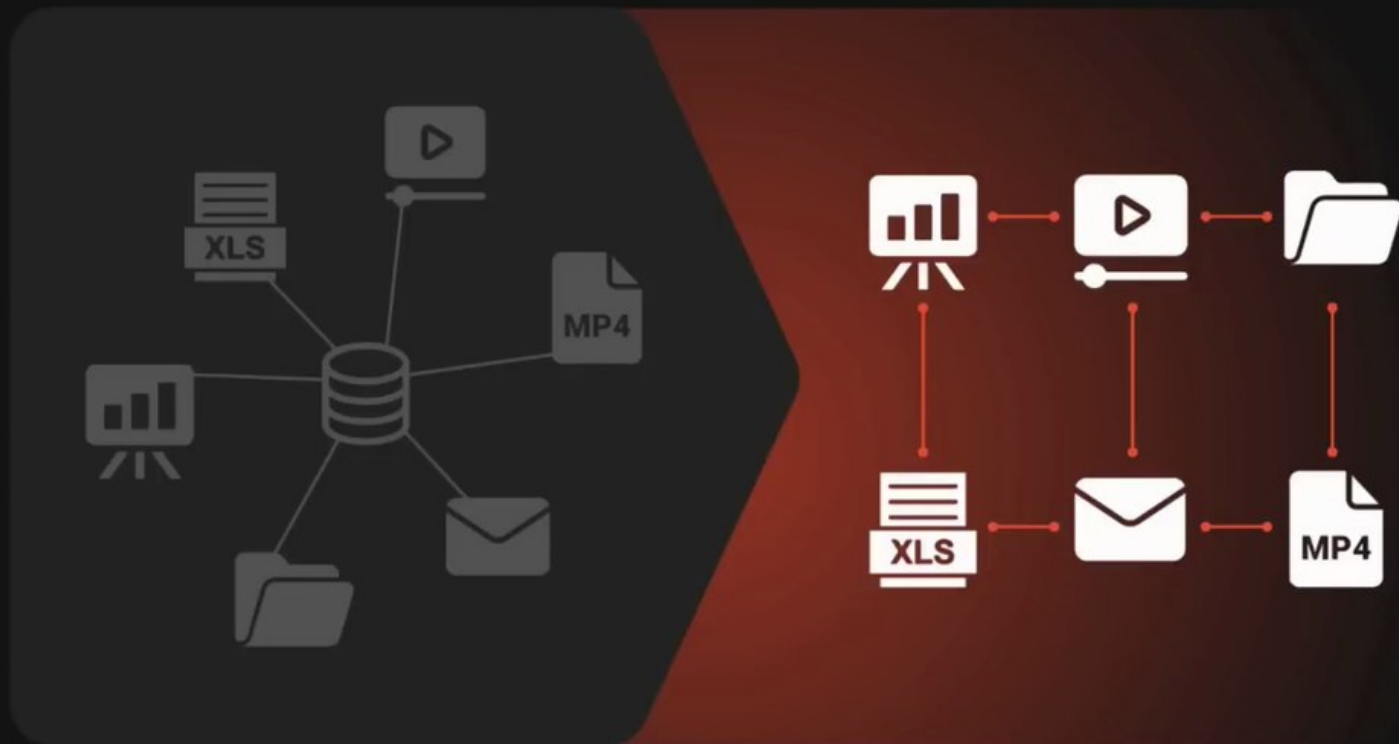
ООО «ЛАБОРАТОРИЯ
КРИМИНАЛИСТИЧЕСКОГО
АНАЛИЗА ДАННЫХ»



❌ Проблема: «Информационная перегрузка»

Закон Хика: «Чем больше выбор, тем дольше решение»

Время принятия решения растет с увеличением количества и вариантов выбора. сложности





UI/UX — это не про «красиво», а про «эффективно»

UI (User Interface) — это кнопки, меню, цвета, шрифты. Внешний слой.



UX (User Experience) — это ощущения, простота достижения цели, логика работы. Внутренняя суть.

Цель: Сделать так, чтобы инструмент помогал думать о расследовании, а не о том, *как* им пользоваться.



Ø Когнитивная нагрузка

Наш мозг имеет ограниченную «оперативную память»

Мы можем удерживать в голове 7 ± 2 элемента информации одновременно.

Сложный интерфейс «забивает» эту память рутиной («где эта кнопка?», «как тут фильтр применить?»).

Цель UI: Снизить нагрузку, взяв на себя рутинные задачи.
Свободные ресурсы мозга — для анализа и принятия решений.

Ø Визуальное восприятие (Гештальт-принципы): Глаз и мозг любят порядок

Принцип близости

Элементы, расположенные рядом, воспринимаются как связанные.

Принцип сходства

Элементы одного цвета, формы или размера воспринимаются как группа.

Принцип замкнутости

В инструментах визуализации (графах связей) группа взаимодействующих объектов обводится едва заметной полупрозрачной областью (контуром), даже если линия не сплошная.

Принцип общей судьбы

Элементы, которые движутся в одном направлении или появляются/исчезают одновременно, воспринимаются как связанные.

Принцип фигуры и фона

Всплывающее окно с предупреждением имеет затемнение фона под ним, четко отделяя себя как «фигуру». Строка в логах с высоким приоритетом имеет контрастный цвет фона, чтобы явно отделиться от остальных строк («фона»).

Применение

- Правильная группировка кнопок
- использование цвета для выделения аномалий (красный — угроза, зеленый — норма).

🚫 Кейс: Расследование инцидента с фишингом

UI как ускоритель реакции



Экономия 20-30 минут на каждом инциденте.

09:00: Поступление жалобы от пользователя.

09:02 (Плохой UI): Аналитик вручную ищет письмо в логах почтового сервера через сложный запрос. *Тратит 15-30 минут.*

09:02 (Хороший UI): Вводит email отправителя в единую строку поиска. Система за 10 сек. находит письмо и сразу показывает всех получателей и вложения.

09:10 (Хороший UI): Клик по хэшу вложения.

09:12 (Хороший UI): Кнопка «Заблокировать отправителя» + «Найти все вхождения». Система выполняет и показывает результат.

09:20: Инцидент локализован, письма удалены, пользователи предупреждены.



⚡ Что требовать от разработчиков? Практические советы

Единый поиск

Одно окно для всех типов данных

Горячие клавиши

Для частых действий

Шаблоны и дашборды

Возможность настраивать представления под задачи.

Ясность и однозначность

Никаких технических терминов в кнопках

Визуализация связей

Графы и карты, а не только таблицы.

Обратная связь

Система должна сообщать о действиях («Идет поиск...», «Готово»).

Формируйте и озвучивайте свои требования к интерфейсам инструментов, которые используете.

∅ Выгода для бизнеса

Удобный интерфейс — это не расходы, это инвестиции



Скорость: Более быстрая реакция → меньшие потери.

Точность: Меньше ошибок из-за человеческого фактора.

Эффективность: Один аналитик может обработать больше информации.

Удовлетворенность: Снижение выгорания, удержание ценных кадров.

Итоги



UI/UX — критически важный компонент инструментов для исследований.



Хороший интерфейс снижает когнитивную нагрузку и экономит время, основываясь на законах восприятия.



Ваша задача — не мириться с неудобными системами, а быть адвокатом удобства и эффективности.

Вопросы

Никита Павлов

inbox@zero-ediscovery.ru

zero-ediscovery.ru



zero-ediscovery.ru



@zero_ediscovery

