Cross Technologies

Александра Бялькина,
Руководитель направления развития продуктов


HOW TO CATCH THE BAD GUY:
1. Collect tons of data
2. Sort all the data
3. Analyze every last word
4. Find time to catch the bad guy

Предпосылки EDRM

Глобальная цифровизация, растущие объемы данных, множество форматов:

1996 – 10 MB

1999 – IBM the Microdrive 170 MB и 340 MB

2002 – 137 GB addressing space barrier broken

2005 – 500 GB hard drive

2007 – 1 terabyte hard drive

2009 – 2 terabyte hard drive

2011 – 4 terabyte hard drive

2013 – 5 terabyte hard drive

2015 – 10 terabyte hard drive

2018 - 16TB Samsung, 60 terabyte SSD Seagate

Предпосылки EDRM

Нехватка персонала и обучение персонала

Задержки по разбору инцидентов, криминалистическому анализу

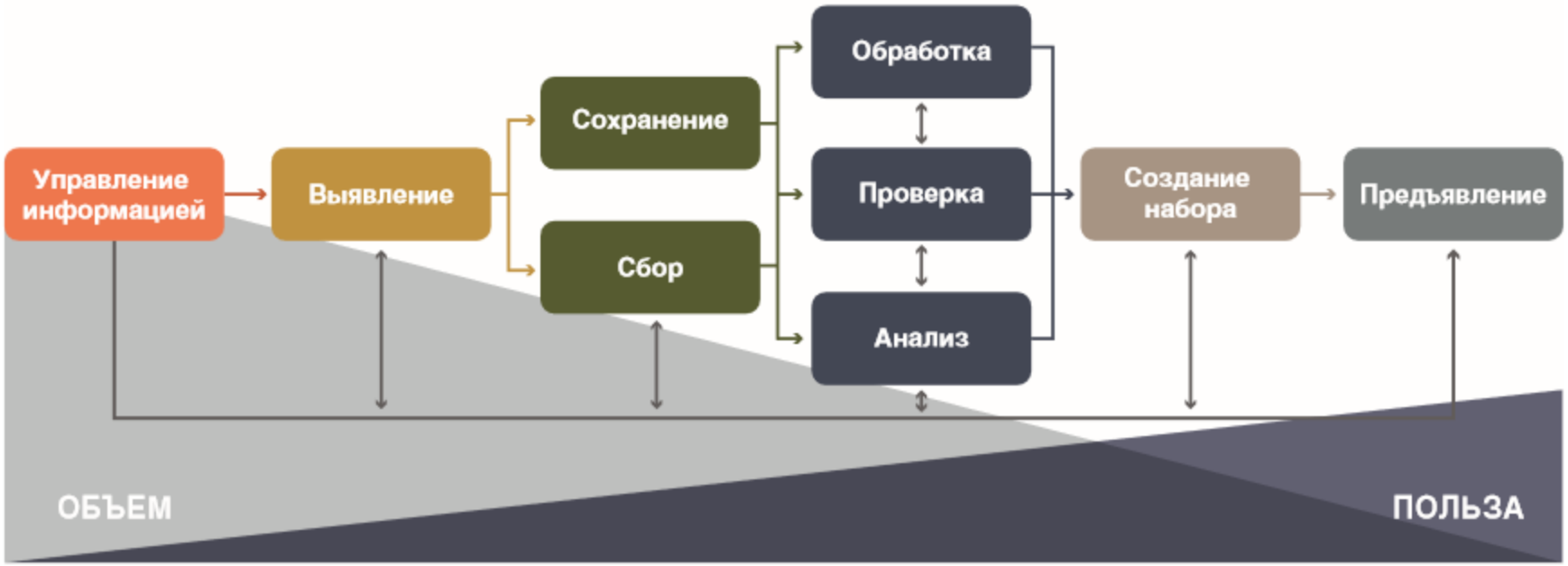
Необходимость оптимизации работы экспертов

Принципы сбора доказательств

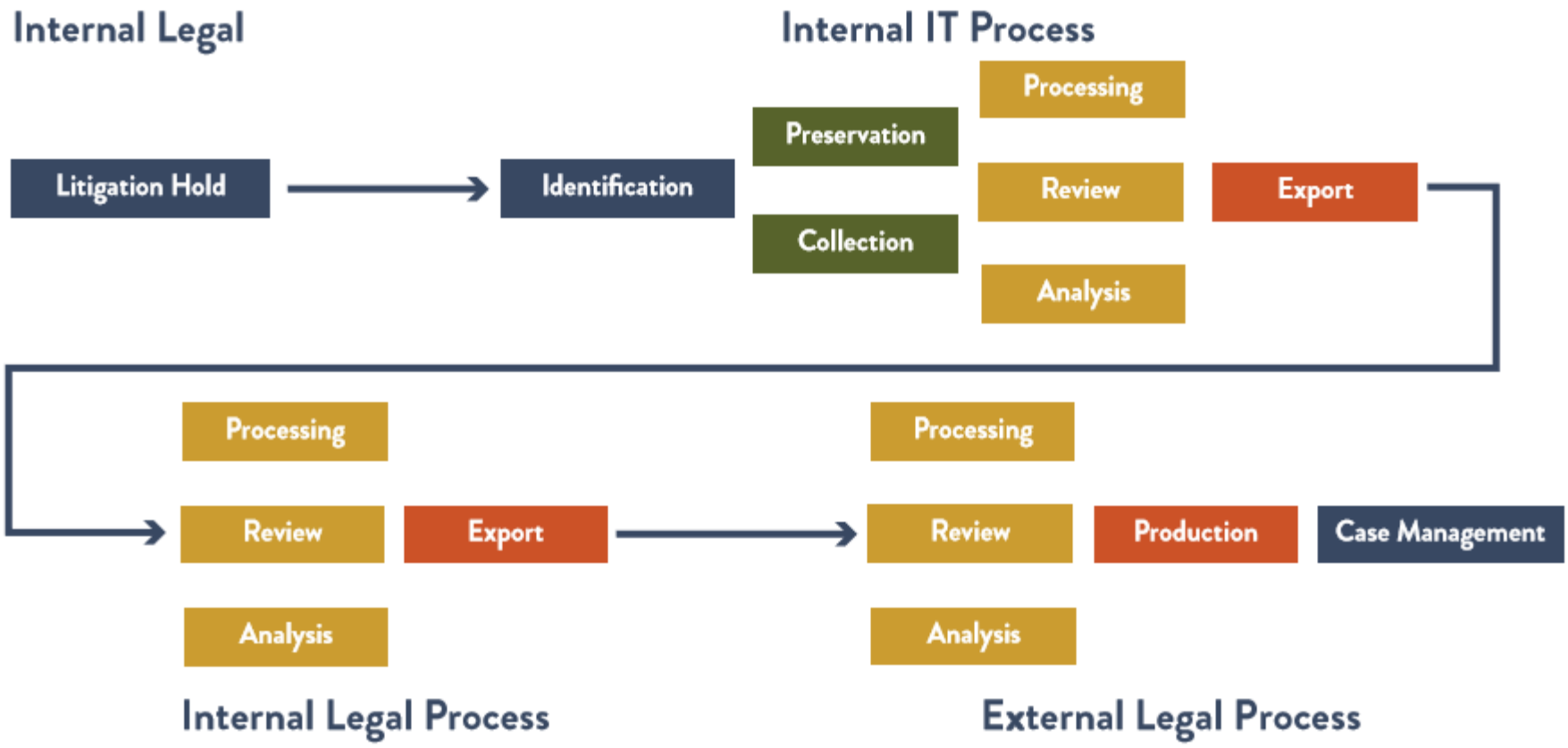
ACPO – Association of Chief Police Officers – 4 принципа:

1. Любое действие не должно изменять собираемую с электронных носителей информации (целостность)
2. Если необходимо обеспечить доступ к ESI, то специалист должен быть компетентным для сбора релевантных доказательств
3. Процесс сбора данных должен быть зафиксирован, чтобы третья сторона могла его повторить с получением того же результата (воспроизводимость, связана с п.1)
4. Соответствие (непротиворечивость) первых трех принципов законодательным актам.

Electronic Discovery Reference Model



EDRM


Internal Legal
Internal IT Process
Litigation Hold
Identification
Preservation
Collection
Processing
Review
Analysis
Export
Processing
Review
Analysis
Export
Processing
Review
Production
Case Management
Analysis
Internal Legal Process
External Legal Process

Что дает EDRM?

- Отсутствие влияния на бизнес-процессы (удаленный сбор, разделение задач: безопасности свое – аналитикам и юристам свое)
- Снижение рисков
- Снижение издержек на сбор и анализ доказательств

Best practice

- Автоматизация процесса сбора данных – скорость сбора, корректность, отсутствие зависимости от квалификации IT-специалиста
- Унификация форматов и процессов сбора, хранения и обработки данных
- Подтвержденная целостность собранных данных (включая трекинг процесса сбора)
- Придание юридической значимости собранным доказательствам
- Использование следственными органами инструментов, которые работают с форматами AD1, EO1

Как адаптировать EDRM для России

- Разработка единой методологии сбора и обработки информации
- Применение единых форматов данных (которые принимаются в судах) – например, AD1, EO1
- Отсутствие необходимости каждый раз в суде привлекать эксперта (для анализа достоверности собранной копии).
- Использование единых или интегрируемых платформ для работы с форматами данных
- Распространение методологии на дела уголовного характера

Документальная база

ГОСТ 27037-2014 и «eDiscovery in digital forensic investigations» (Centre for Applied Science and Technology)

Key similarities	Key differences	
	Digital investigation	eDiscovery
Working with large volumes of material	Broad range of content	Focus on text content
Trying to make best use of valuable resources	Also interested in how activities were conducted	Interested primarily in matters of record
Using case information to refine search	Key driver is locating evidence	Key driver is managing costs
Need to make material reviewable	Information is normally organised by source	Information is normally organised by owner
Need to share the workload	Relates to criminal proceedings	Primarily used in civil proceedings
Automation used where possible	Must maintain evidential chain	Attribution of documents and devices is not normally an issue


ACCESSDATA
Cross Technologies
Благодарим за внимание
bav@crossteh.su