Cross Solutions

СБОР ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ И ПРОВЕДЕНИЕ РАССЛЕДОВАНИЯ

Докладчик: Фальчевский Михаил
Заместитель руководителя департамента развития продуктов

ЧТО ТАКОЕ ЭЛЕКТРОННОЕ ДОКАЗАТЕЛЬСТВО?

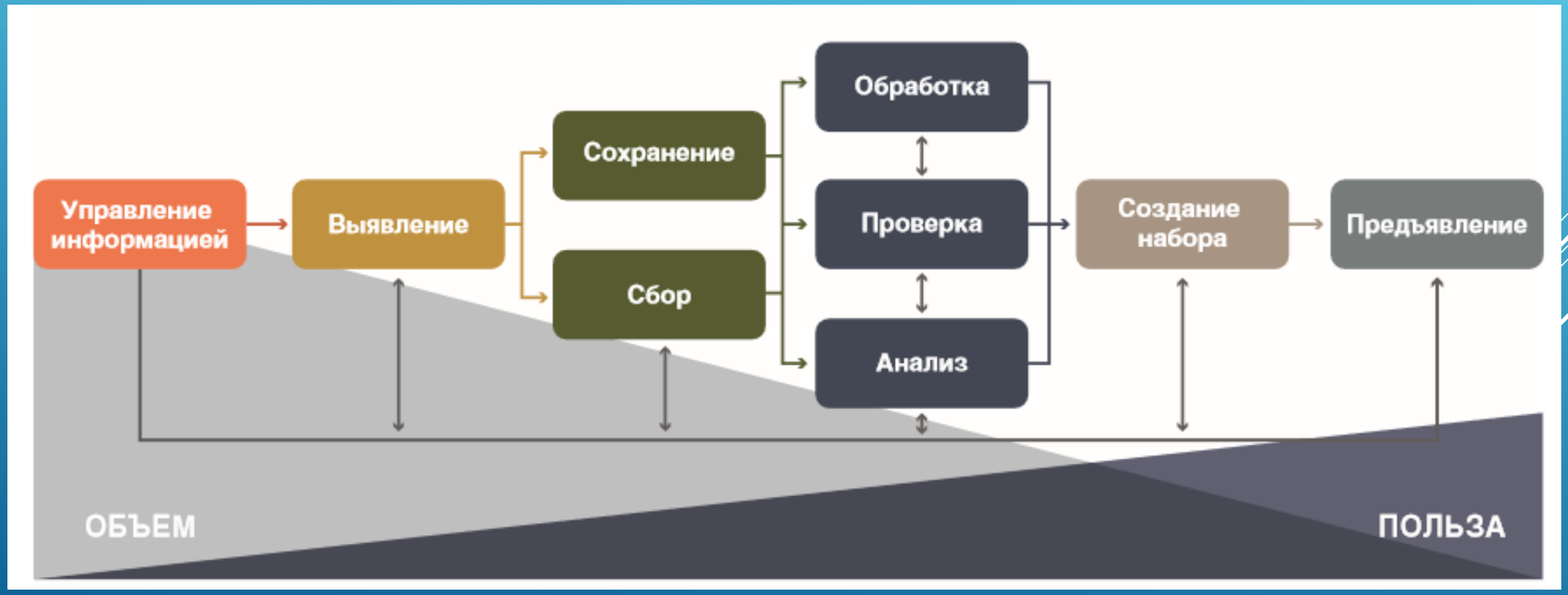
Свидетельства, представленные в цифровой форме: Информация или данные, хранящиеся или передаваемые в виде двоичного кода, которые можно использовать в качестве доказательства.

ЧТО ТАКОЕ СБОР ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В ЦЕЛЯХ РАССЛЕДОВАНИЯ?

Процессы по идентификации, сбору, получению и сохранению потенциальных свидетельств, представленных в цифровой форме, для проведения дальнейшего расследования.

Совокупность таких процессов представляет собой методику получения свидетельств, обеспечивающую их допустимость для правовых и/или дисциплинарных действий.

ОПЫТ ИНОСТРАННЫХ КОЛЛЕГ:
(EDRM) ELECTRONIC DISCOVERY REFERENCE MODEL
- МОДЕЛЬ, КОТОРАЯ АКТИВНО ИСПОЛЬЗУЕТСЯ ДЛЯ РАБОТЫ С ЭЛЕКТРОННОЙ ИНФОРМАЦИЕЙ В США, ВЕЛИКОБРИТАНИИ



АДАПТАЦИЯ ОПЫТА

ГОСТ Р ИСО/МЭК 27037-2014

Руководство по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме.
Описывает цикл обращения со свидетельствами, представленными в цифровой форме.

* слова «ИСО» и/или «МЭК», означают, что данный нормативный документ является переводом стандарта соответствующей международной организации

СРАВНЕНИЕ EDISCOVERY IN DIGITAL FORENSIC INVESTIGATIONS - ГОСТ Р ИСО/МЭК 27037-2014

Модель EDRM имеет своей конечной целью представление стандартизированного отчета, имеющего юридическую значимость, заинтересованным лицам в адекватные целям расследования сроки.

Поставленная цель достигается путем стандартизации процессов, формированием судебной практики* и использованием специализированного программного обеспечения (ПО). Использование ПО позволяет:

- Автоматизировать и стандартизировать процесс сбора электронных доказательств;
- Унифицировать форматы электронных доказательств (AD1, EO1);
- Распределить задачи в ходе расследования между специалистами, имеющими компетенции в разных сферах, необходимых для расследования;
- Подтвердить целостность собранных электронных доказательств (включая протоколирование процесса сбора);

*Особенность англо-американской правовой системы

СРАВНЕНИЕ EDISCOVERY IN DIGITAL FORENSIC INVESTIGATIONS - ГОСТ Р ИСО/МЭК 27037-2014

ГОСТ Р ИСО/МЭК 27037-2014 представляет собой описание процессов при обращении с потенциальными свидетельствами первой половины EDRM модели.

Положения ГОСТа выделяют две роли специалистов, имеющих компетенции в разных сферах:

Специалист "оперативного реагирования" по свидетельствам, представленным в цифровой форме; DEFR (digital evidence first responder): Физическое лицо, которое уполномочено, обучено и подготовлено действовать первым на месте инцидента, осуществляя сбор и получение свидетельств, представленных в цифровой форме, и которое **несет ответственность за обращение с этими свидетельствами**.

Специалист по свидетельствам, представленным в цифровой форме; DES (digital evidence specialist): Физическое лицо, которое может выполнять задачи специалиста "оперативного реагирования" по свидетельствам, представленным в цифровой форме, **и которое обладает специальными знаниями, навыками и способностями, чтобы разбираться в широком спектре технических вопросов.**

СРАВНЕНИЕ EDISCOVERY IN DIGITAL FORENSIC INVESTIGATIONS - ГОСТ Р ИСО/МЭК 27037-2014

ГОСТ допускает совмещение ролей.

Особенностью в нашей практики является совмещение этих ролей в одном лице.

Привычное название – Эксперт.

Совмещение ролей обеспечивает непрерывность процесса и единоличный контроль экспертом всех этапов работы, но персонифицирует экспертное заключение.

КАК ПОСТРОИТЬ ПРОЦЕССЫ РАССЛЕДОВАНИЯ? КАКИЕ ВОПРОСЫ НЕОБХОДИМО РЕШИТЬ, ОПИРАЯСЬ НА ПОЗИТИВНЫЙ ИНОСТРАННЫЙ ОПЫТ?

Синхронизируем цели:

Цель - представление заинтересованным лицам стандартизированного отчета в адекватные целям расследования сроки, с приданием отчету юридической значимости.

Для этого как минимум необходимо:

Обеспечить выполнение принципов значимости, достоверности и достаточности свидетельств, представленных в цифровой форме. (Зафиксированы в ГОСТ)

Стандартизировать процессы идентификации, сбора, получения и хранения свидетельств, представленных в цифровой форме (ГОСТ носит рекомендательный характер)

Обеспечить разделение ролей специалистов при проведении расследования (Экспертное заключение на ранее выданное заключение эксперта в ходе судебных заседаний – не редкость в наших реалиях.)

КАК ОБЕСПЕЧИТЬ ДОСТОВЕРНОСТЬ ПО ГОСТ?

- **Контролируемость –** обеспечивается документированием (протоколированием) всех предпринятых действий. Обоснованием процессов принятия решения, касающегося выбора определенного порядка действий. Доступность для независимой оценки.

- **Повторяемость**

Признается, если те же результаты теста получают при следующих условиях:

- использование такой же процедуры и метода измерений;

- использование таких же инструментальных средств и при таких же условиях;

- возможно повторение в любое время после первоначального тестирования.

- **Воспроизводимость**

Признается, если те же результаты получают при следующих условиях:

- использование такого же метода измерения;

- использование различных инструментальных средств и при различных условиях;

- возможно повторение в любое время после первоначального тестирования.

ПРИМЕРЫ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ СПЕЦИАЛИЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ACCESSDATA

FTK®

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

Поиск и идентификацию релевантных данных

Анализ данных

Протоколирование действий

Подготовку отчета для передачи

Обеспечивает принцип повторяемости

AD Enterprise

Расследования в сети пост-анализ инцидентов

Обеспечивает поиск и идентификацию релевантных данных

Обеспечивает первичный сбор доказательств (в том числе с удаленных рабочих станций)

Обеспечивает сохранение образов данных в стандартизированных форматах электронных копий

Обеспечивает принцип повторяемости

Обеспечивает принцип воспроизводимости

Обеспечивает разделение ролей специалистов при проведении расследования

Управление процессами удаленной операционной системы в реальном времени

QUIN-C

НОВОЕ ПОКОЛЕНИЕ КРИМИНАЛИСТИКИ

Обеспечивает возможность организации одновременного доступа специалистов с использованием Web - интерфейса

Ускоряет процессы расследования

ЗАКЛЮЧЕНИЕ

Анализ иностранного опыта позволяет сделать вывод:

Все первичные вопросы, которые нам необходимо решить, уже успешно решены путем использования специализированного программного обеспечения.

Придать юридическую значимость собранным свидетельствам в нашей правовой системе возможно в случае стандартизации процессов, унификации отчетов и формировании судебной практики.

Судебная практика может быть сформирована посредством многократных оценок Судом цифровых свидетельств, представленных в качестве доказательств в ходе судебных процессов.