СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

Киберпреступность **4**

ВВЕДЕНИЕ В ЦИФРОВУЮ КРИМИНАЛИСТИКУ

UNODC
Дохинская декларация:
ПООЩРЕНИЕ КУЛЬТУРЫ СОБЛЮДЕНИЯ ЗАКОННОСТИ

образование для правосудия

Управление Организации Объединенных Наций по наркотикам и преступности

ОБРАЗОВАНИЕ ВО ИМЯ ПРАВОСУДИЯ
СЕРИЯ УНИВЕРСИТЕТСКИХ МОДУЛЕЙ

КИБЕРПРЕСТУПНОСТЬ

Модуль 4

ВВЕДЕНИЕ В ЦИФРОВУЮ КРИМИНАЛИСТИКУ

Организация Объединенных Наций
Вéна, 2019

Этот модуль является ресурсом для преподавателей.

Этот модуль, разработанный в рамках инициативы «Образование для Правосудия»(E4J), являющейся компонентом Глобальной программы по осуществлению Дохинской декларации, Управления Организации Объединенных Наций по наркотикам и преступности (УНП ООН) и является частью серии учебных модулей «Образование для правосудия» (E4J) по Киберпреступности и сопровождается учебным пособием. Полный спектр материалов «Образование для правосудия» E4J включает в себя университетские модули по вопросам честности и этики, предупреждения преступности и уголовного правосудия, борьбы с коррупцией, организованной преступности, торговли людьми / незаконного ввоза мигрантов, огнестрельного оружия, охраны дикой природы, лесных и рыболовных преступлений, борьбы с терроризмом, а также киберпреступность.

Все модули в серии модулей университета «Образование для правосудия» E4J содержат предложения для выполнения в классе упражнений, оценки учащихся, слайды и другие учебные пособия, которые преподаватели могут адаптировать к своему контексту и интегрировать в существующую учебную программу. Модуль предоставляет план для трехчасового занятия, но может использоваться для более коротких или более длительных занятий.

Все университетские модули «Образование для правосудия» E4J участвуют в действующих научных исследованиях и дебатах и могут содержать информацию, мнения и заявления из различных источников, включая сообщения прессы и независимых экспертов. Ссылки на внешние ресурсы были проверены на момент публикации. Однако, поскольку сторонние веб-сайты могут измениться, пожалуйста *contact us*, если вы столкнулись с неработающей ссылкой или перенаправлены на неприемлемый контент. Также сообщите нам, если вы заметили, что публикация связана с неофициальной версией или веб-сайтом.

Несмотря на то, что были приложены все усилия для обеспечения точного перевода модуля, обратите внимание, что модуль на английском языке является утвержденной версией. Поэтому в случае сомнений, пожалуйста, обратитесь к первоисточнику в английской версии.

Ознакомиться с условиями использования Модуля можно на *веб-сайте E4J*.

Используемые обозначения и представление материалов в этой публикации не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединенных Наций относительно правового статуса какой-либо страны, территории, города или района или ее органов власти, или относительно разграничения его границ.

Данная публикация не была официально редактирована.

Оглавле́ние

Введение

Криминалистика применяет «естественные, физические и социальные науки к вопросам права» (Maras and Miranda, 2014, p. 1). Одной из многочисленных отраслей криминалистики является цифровая судебная экспертиза (больше известная как *цифровая криминалистика*). Цифровая криминалистика является «одной из отраслей криминалистики, которая сосредоточена на уголовно-процессуальном праве и доказательствах применительно к компьютерам и связанным с ними устройствам» (Maras, 2014, p. 29), таким как мобильные устройства (например, телефоны и смартфоны), игровые приставки и прочие устройства, функционирующие через Интернет (например, устройства для здоровья и фитнеса и медицинские приборы). Цифровая криминалистика, в частности, имеет отношение к процессу сбора, получения, сохранения, анализа и представления электронных доказательств (также известных как *цифровые доказательства*) в целях получения оперативно-розыскных сведений и/или осуществления расследования и уголовного преследования в отношении различных видов преступлений, включая киберпреступления.

> *Примечание:*
>
> Хотя в данном модуле основное внимание уделяется цифровой криминалистике при проведении расследований правоохранительными органами и судебном преследовании в отношении киберпреступлений, многие мероприятия, связанные с цифровой криминалисткой, осуществляются субъектами, находящимися вне системы уголовного правосудия, такими как частные компании и организации (для получения информации о мероприятиях, связанных с цифровой криминалисткой, которые осуществляют частные компании и организации, см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики»). Более того, большое количество различных учреждений, организаций, коммерческих предприятий и физических лиц могут участвовать в мероприятиях, относящихся к цифровой криминалистике и расследованиям киберпреступлений (см. модуль 5 серии модулей по киберпреступности: «Расследование киберпреступлений» для получения информации о лицах, участвующих в таких расследованиях).

В данном модуле представлен обзор цифровой криминалистики и цифровых доказательств, рассматриваются, в частности, процесс проведения судебной цифровой

экспертизы, общие практические методы цифровой криминалистики, стандарты цифровой криминалистики и цифровых доказательств, а также передовая практика в области цифровой криминалистики.

Результаты обучения

- Обсудить данные и определить источники данных
- Описать и обсудить цифровые доказательства
- Сравнить и сопоставить цифровые доказательства и традиционные доказательства для установления различий между ними
- Обсудить способы аутентификации цифровых доказательств
- Описать и критически проанализировать модели процесса цифровой криминалистики
- Критически оценить стандарты и передовые практические методы, касающиеся цифровых доказательств и цифровой криминалистики

Основные вопросы

Процедуры и методы, используемые для идентификации, сбора, получения, сохранения, анализа и, наконец, представления цифровых доказательств в суде, должны соответствовать действующему уголовно-процессуальному законодательству (этот вопрос рассматривается в модуле 3 серии модулей по киберпреступности: «Правовая база и права человека»). В этом законодательстве прописываются нормы доказательственного права и правила уголовного судопроизводства, которые необходимо соблюдать для обеспечения допустимости доказательств в суде. Информационно-коммуникационные технологии (ИКТ) могут содержать доказательства совершения преступления. Данные, извлеченные из средств ИКТ, которые могут быть использованы в суде, именуются электронными доказательствами (также известными как *цифровые доказательства*), а процесс идентификации, получения, сохранения, анализа и представления таких доказательств именуется *цифровой криминалистикой*. В данном модуле подробно рассматриваются вопросы, связанные с цифровыми доказательствами и цифровой криминалистикой.

Цифровые доказательства

Цифровая криминалистика «основывается на [принципах криминалистики, таких как] принцип обмена [Эдмона] Локара» (Albert and Venter, 2017, p. 24), который утверждает, что «когда объекты и поверхности вступают в контакт друг с другом, происходит перекрестный перенос материалов» (Maras and Miranda, 2014, pp. 2-3). В контексте цифровой криминалистики люди, после использования информационно-коммуникационных технологий (ИКТ), оставляют цифровые следы (Albert and Venter, 2017). В частности, лицо, использующее ИКТ, может оставить *цифровые отпечатки*, т.е. данные, оставленные пользователями ИКТ, которые могут раскрыть сведения о них, включая информацию о возрасте, половой, расовой и этнической принадлежности, гражданстве, сексуальной ориентации, мыслях, предпочтениях, привычках, хобби, истории болезни и проблемах здоровья, психологических расстройствах, статусе занятости, принадлежности к какому-либо сообществу, отношениях, геолокации, распорядке дня и прочей активности. Такие цифровые отпечатки могут быть активными или пассивными. *Активный цифровой отпечаток* создается данными, предоставляемыми пользователем, такими как персональные данные, видео, изображения и комментарии, размещаемые в приложениях, на вебсайтах, электронных досках объявлений, в социальных сетях и других онлайн-форумах. *Пассивный цифровой отпечаток* – это данные, которые непреднамеренно оставляют люди, пользующиеся Интернетом и цифровыми технологиями (например, история просмотров в браузере). Данные, которые являются частью активных и пассивных цифровых отпечатков, могут использоваться в качестве доказательства совершения преступления, в том числе киберпреступления (т.е. в качестве *цифровых доказательств*). Такие данные могут также использоваться для доказательства или опровержения утверждения о факте; подтверждения или опровержения показаний потерпевшего, свидетеля и подозреваемого; и/или определения причастности или непричастности подозреваемого к совершению преступления.

Данные хранятся в цифровых устройствах (например, компьютерах, смартфонах, планшетах, телефонах, принтерах, «умных» телевизорах (Smart TV) и любых других устройствах, которые имеют цифровую память), внешних запоминающих устройствах (например, внешних жестких дисках и *USB-флеш-накопителях), сетевых компонентах и устройствах (например, маршрутизаторах), серверах и облачном хранилище данных (где данные хранятся «в нескольких центрах данных в различных географических точках»; УНП ООН*, 2013, стр. xxvi). Извлекаемые данные могут представлять собой данные, относящиеся к контенту (т.е. слова в письменных сообщениях или произнесенные слова в аудиофайлах; например, видео, текст электронных писем, текстовые сообщения, мгновенные сообщения и содержание социальных сетей), и данные, *не относящиеся к контенту*, или *мета-данные* (т.е. данные о содержании;

например, личность и местоположение пользователей и данные об операциях, такие как информация об отправителях и получателях телекоммуникационных и электронных сообщений).

Данные, получаемые в режиме онлайн и/или извлекаемые из цифровых устройств, могут содержать большое количество информации о пользователях и событиях. Например, игровые приставки, которые работают как персональные компьютеры, хранят личную информацию о пользователях устройств (например, имена и адреса электронной почты), финансовую информацию (например, данные кредитной карты), информацию об истории посещений Интернета (например, о посещенных вебсайтах), изображения, видео и другие данные. Данные, извлеченные из игровых приставок, использовались при расследовании дел, связанных с сексуальной эксплуатацией детей и размещением в Интернете материалов со сценами сексуального насилия над детьми (Read et al., 2016; Conrad, Dorn, and Craiger, 2010) (эти киберпреступления дополнительно рассматриваются в модуле 12 серии модулей по киберпреступности: «Киберпреступления против личности»). Еще одним цифровым устройством, которое накапливает значительный объем данных о его пользователях, является Amazon Echo (с голосовым помощником Alexa). Данные, накапливаемые этим устройством, могут содержать ценные сведения о пользователях/владельцах, такие как информация об их интересах, предпочтениях, запросах, покупках и прочих видах активности, а также об их местонахождении (чтобы, например, определить, находятся ли они дома или вне дома, путем просмотра меток времени и аудиозаписи взаимодействий с речевым помощником Alexa). Данные, извлеченные из Amazon Echo, использовались в Соединенных Штатах Америки при расследовании дела об убийстве. Хотя обвинения против подозреваемого были в конечном итоге сняты, это дело наглядно продемонстрировало, что данные, собираемые с использованием новых цифровых технологий, неизбежно будут представлены в суде в качестве доказательства (Maras and Wandt, 2018).

Данные могут добываться и использоваться в целях получения оперативно-розыскных сведений (для получения дополнительной информации см. UNODC 2011 Criminal Intelligence Manual for Analysts (УНП ООН, 2011 год, «Оперативная информация о преступной деятельности: пособие для аналитиков»)) и/или могут представляться в суде в качестве цифровых доказательств. В последнем случае цифровые доказательства могут служить *прямыми доказательствами* путем «установления факта» либо *косвенными доказательствами* путем «выведения заключения об истинности данного факта» (Maras, 2014, pp. 40-41). Рассмотрим следующий гипотетический случай: материал расистского содержания был опубликован от имени учетной записи в Twitter (Учетная запись А). *Прямым доказательством* является тот факт, что Учетная запись А была использована для публикации расистского материала. *Косвенным доказательством* является тот факт, что материал был размещен владельцем учетной записи. Для того чтобы доказать, что владелец учетной записи опубликовал этот материал, необходимо

получить дополнительные подкрепляющие доказательства (как показано в модуле 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики», установление личности исполнителя киберпреступления является нелегкой задачей).

Прежде чем цифровые доказательства могут быть представлены в суде в качестве прямых или косвенных доказательств, их необходимо аутентифицировать (т.е. необходимо показать, что доказательства соответствуют предполагаемой цели). Для наглядной демонстрации практики аутентификации рассмотрим следующие общие категории цифровых доказательств: контент, генерируемый одним или несколькими лицами (например, текст, электронное письмо или мгновенное сообщение и документы текстового редактора, такого как Microsoft Word); контент, генерируемый компьютером или цифровым устройством без участия пользователя (например, журналы регистрации данных), который считается одной из форм *вещественного доказательства*, например, в Соединенном Королевстве (см. дело *Regina (O) v. Coventry Magistrates Court*, 2004); и контент, генерируемый одновременно пользователем и устройством (например, динамические таблицы в таких программах, как Microsoft Excel, которые включают в себя данные, вводимые пользователем, и расчеты, осуществляемые программой). Контент, генерируемый пользователем, может считаться допустимым доказательством, если он является достоверным и правдоподобным (т.е. можно установить его принадлежность к какому-либо лицу). Контент, генерируемый устройством, может считаться допустимым доказательством, если можно доказать, что устройство функционировало должным образом в момент генерирования данных, и если можно показать, что в момент генерирования данных действовали механизмы обеспечения защиты для предотвращения изменения данных. В случаях, когда контент генерируется одновременно устройством и пользователем, необходимо установить достоверность и правдоподобность каждого из них.

По сравнению с *традиционными доказательствами* (например, бумажными документами, оружием, контролируемыми веществами и т.д.), цифровые доказательства создают уникальные сложности при аутентификации из-за объема доступных данных, их скорости (т.е. скорости, с которой они создаются и передаются), неустойчивости (т.е. они могут быстро исчезнуть при перезаписи или удалении) и уязвимости (т.е. их легко можно обработать, изменить или повредить). В то время как одни страны внедрили нормы доказательственного права, включающие в себя требования в отношении аутентификации, которые конкретно относятся к цифровым доказательствам, другие страны для *аутентификации* традиционных доказательств и цифровых доказательств используют схожие требования. Во Франции, например, как бумажные, так и электронные документы должны аутентифицироваться путем проверки личности создателя документов и целостности документов (Bazin, 2008). Проверка целостности документов означает не только проверку их точности, но и способности сохранять

точность (т.е. *непротиворечивость*) с течением времени. Более того, для того чтобы унифицировать режимы обращения с нецифровыми и цифровыми доказательствами, Сингапур внес поправки в нормы доказательственного права, приняв Закон о доказательствах (с поправками) 2012 года, чтобы обеспечить одинаковую практику аутентификации для нецифровых и цифровых доказательств.

В дополнение к определению подлинности цифровых доказательств, многие страны также проводят оценку того, является ли полученное доказательство *наилучшим доказательством* (т.е. подлинным доказательством или точной копией подлинного доказательства), и/или может ли оно быть допустимым в соответствии с исключениями из требований соблюдения запрета на показания *с чужих слов* (т.е. заявлений, сделанных вне суда) (Biasiottie et al., 2018; Kasper and Laurits, 2016; Alba, 2014; Duranti and Rogers, 2012; Goode, 2009). В качестве примера можно привести Танзанию (Закон о доказательствах 1967 года, Закон о письменных законах (с различными поправками) 2007 года и Закон об электронных операциях 2015 года); Белиз (Закон об электронных доказательствах 2011 года); Индонезию (Закон №.11 от 2008 года об электронной информации и операциях и Постановление правительства №.82 от 2012 года); Малайзию (Закон о доказательствах 1950 года); Индию (Закон об информационных технологиях 2000 года); Сингапур (Закон о доказательствах (с поправками) 2012 года) и другие страны.

Кроме того, оценка подлинности цифровых доказательств также предполагает изучение процессов, методов и инструментов, использованных для сбора, получения, сохранения и анализа цифровых доказательств, чтобы убедиться в том, что данные не были изменены каким-либо образом. Эти процессы, методы и средства рассматриваются в следующих разделах данного модуля.

Цифровая криминалистика

Процесс цифровой судебной экспертизы включает в себя: поиск, получение, сохранение и хранение цифровых доказательств; описание, объяснение цифровых доказательств и установление их происхождения и значимости; анализ доказательств и их убедительности, достоверности и относимости к делу; и представление доказательств, имеющих отношение к делу (Maras, 2014).

Были разработаны и приняты различные методологии цифровой криминалистики. В 2001 году «Digital Forensic Research Workshop», «некоммерческая добровольная организация,… [специализирующаяся] на финансировании деятельности технических рабочих групп, проведении ежегодных конференций и решении комплекса задач с целью оказания помощи в определении направления исследований и разработок»,

разработала модель, основанную на протоколе Федерального бюро расследований Соединенных Штатов Америки для производства обыска на физическом месте преступления, который включает в себя семь этапов: идентификация, сохранение, сбор, исследование, анализ, представление доказательств и принятие решения (Palmer, 2001, p. 14) (см. рисунок 1).

Идентификация	Сохранение	Сбор	Исследование	Анализ	Представление	Решение
Выявление события/ преступления	Ведение дела	Сохранение	Сохранение	Сохранение	Документирование	
Разрешение сигнатуры	Технологии обработки изображений	Одобренные методы	Прослеживаемость	Прослеживаемость	Показания эксперта	
Определение профиля	Система охраны вещественных доказательств	Одобренное программное обеспечение	Методы валидации	Статистика	Разъяснение	
Выявление аномалий	Синхронизация времени	Одобренное аппаратное обеспечение	Методы фильтрации	Протоколы	Заявление о воздействии на задание	
Жалобы		Правомочие	Сравнение на соответствие шаблону	Извлечение данных	Рекомендуемая контрмера	
Мониторинг системы		Сжатие без потерь	Обнаружение скрытых данных	Временная шкала/сроки	Статистическая интерпретация	
Контрольный анализ		Выборка	Извлечение скрытых данных	Связь		
И т.д.		Редукция данных		Пространство		
		Методы восстановления				

Рисунок 1. Palmer, Gary. (2001). Технический отчет DFRWS: План действий для цифровых криминалистических исследований. Семинар по цифровым криминалистическим исследованиям. Ютика, штат Нью-Йорк.

В 2002 году была предложена еще одна модель цифровой криминалистики, которая была основана на модели «Digital Forensic Research Workshop» 2001 года и протоколе Федерального бюро расследований Соединенных Штатов Америки для производства обыска на месте преступления (для физических мест преступления) (Reith, Carr and Gunsch, 2002). Эта модель («Абстрактная модель цифровой криминалистики») состояла из девяти этапов (Baryamureeba and Tushabe, 2004, 3):

1. *Идентификация* (т.е. «распознание инцидента по признакам и определение его типа»);

2. *Подготовка* (т.е. «подготовка средств, методов, ордеров на обыск и мониторинг процесса получения разрешений и поддержки руководства»);
3. *Стратегия подхода* (т.е. «разработка процедуры, которая будет использоваться с целью сбора максимального объема безупречных доказательств при минимизации воздействия на потерпевшего»);
4. *Сохранение* (т.е. «изолирование, защита и сохранение состояния вещественных и цифровых доказательств»);
5. *Сбор* (т.е. «составление протокола осмотра физического места преступления и дублирование цифровых доказательств с использованием стандартизированных и утвержденных процедур»);
6. *Исследование* (т.е. «углубленный систематический поиск доказательств, относящихся к предполагаемому преступлению»);
7. *Анализ* (т.е. «определение значимости, восстановление фрагментов данных и выведение заключения на основе обнаруженных доказательств»);
8. *Представление* (т.е. «краткое изложение и объяснение выводов»); и
9. *Возвращение доказательств* (т.е. возвращение физического и цифрового имущества законному владельцу»).

В 2003 году была предложена Интегрированная модель цифрового расследования (см. рисунок 2), которая представляет собой более целостный подход к расследованию, состоящий из пяти основных этапов, каждый из которых, в свою очередь, состоит из отдельных фаз (Carrier and Spafford, 2003): *готовность* (т.е. оценка способности оперативных служб и инфраструктуры оказывать поддержу проведению расследования); *развертывание* (т.е. инцидент выявлен, соответствующий персонал уведомлен, и получено разрешение на проведение расследования, например, судебный ордер на производство расследования правоохранительными органами, разрешение руководителя для проведения частных расследований); *расследование на физическом месте преступления* (т. е. ограждение места преступления, идентификация относящихся к делу вещественных доказательств, документирование места преступления, сбор вещественных доказательств на месте преступления, исследование этих доказательств, реконструкция событий на месте преступления и представление результатов в суде); *цифровое расследование на месте преступления* (т.е. сбор и идентификация имеющих отношение к делу цифровых доказательств, документирование доказательств, извлечение и анализ доказательств, реконструкция событий и представление результатов в суде); и *рассмотрение* (т. е. после завершения расследования проводится оценка с целью анализа извлеченных уроков).

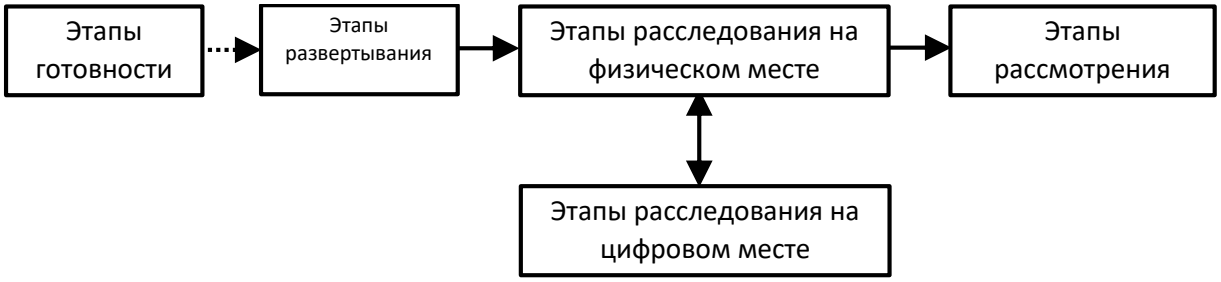

Рисунок 2. Этапы интегрированного процесса цифрового расследования: Carrier, Brian D. and Eugene H. Spafford. (2003). Getting physical with the digital investigation process. International Journal of Digital Evidence, Vol. 2(2), 1-20.

В 2006 году Национальный институт стандартов и технологий США в своем Руководстве по интеграции криминалистических методов в планы реагирования на инциденты (Guide to Integrating Forensic Techniques into Incident Response)(SP 800-86) (Kent et al., 2006, 3-1) предложил модель цифровой криминалистики, состоящую из четырех этапов (см. рисунок 3): этап *сбора* доказательств, который включает в себя идентификацию доказательств на месте преступления, маркировку, документирование и, наконец, собирание доказательств; этап *исследования*, на котором определяются соответствующие криминалистические средства и методы, которые будут использоваться для извлечения соответствующих цифровых доказательств и сохранения их целостности; этап *анализа*, на котором извлекаемые доказательства оцениваются для определения их практической пригодности и применимости к делу; и этап *отчетности*, который включает в себя описание действий, выполненных в процессе цифровой криминалистики, и представление результатов.

Рисунок 3. Национальный институт стандартов и технологий: четырёхфазовая модель цифрового расследования, предложенная в руководстве SP 800-86: Kent, Karen et al. (2006). Guide to Integrating Forensic Techniques into Incident Response, National Institute of Standards and Technology, 121.

Еще одна модель расследования была предложена Национальным институтом правосудия (NIJ) Министерства юстиции США в 2001 году и пересмотрена в 2008 году. В частности, в пособии NIJ «Расследование на электронном месте совершения

преступления: руководство для служб быстрого реагирования» (Electronic Crime Scene Investigation: A Guide for First Responders) основное внимание уделено действиям на физическом месте преступления, таким как ограждение и оценка места преступления (например, для определения имеющих отношение к делу устройств с потенциальными цифровыми доказательствами), документирование места преступления, выемка соответствующих устройств, упаковка, транспортировка и, наконец, обеспечение сохранности этих устройств.

Вышеупомянутые модели основаны на предположениях о том, что при расследовании каждого преступления и киберпреступления все этапы должны быть пройдены в полном объеме (Rogers et al., 2006). Однако на практике это происходит не всегда. Поскольку объемы данных и количество цифровых устройств, накапливающих, хранящих и передающих данные, растут в геометрической прогрессии, что ведет к увеличению числа уголовных дел, связанных с цифровыми устройствами того или иного типа, все чаще признается практически нецелесообразным проводить доскональные проверки каждого цифрового устройства. Как отметили Кейси, Феррaро и Нгуен (Casey, Ferraro, Nguyen) (2009), «немногие [лаборатории цифровой криминалистики] все еще могут позволить себе создавать дубликат каждого носителя информации и проводить углубленную судебную экспертизу всех данных на этих носителях… Не имеет особого смысла ждать завершения анализа каждого отдельного носителя информации, если лишь некоторые из них позволят получить данные, имеющие доказательную ценность» (стр. 1353).

В этой связи были разработаны модели процессов цифровой криминалистики, учитывающие эту проблему. Например, в публикации Rogers et. al (2006) была предложена модель процесса киберкриминалистической сортировки данных на местах (CFFTPM), основанная на проведении цифровой судебной экспертизы «на месте» с целью «обеспечения идентификации, анализа и интерпретации цифровых доказательств в короткие сроки без необходимости транспортировки систем(ы)/носителей информации в лабораторию для углубленного исследования или создания полного образа для судебно-экспертного анализа» (p.19). На основе этой модели Кейси, Феррaро и Нгуен (Casey, Ferraro, Nguyen) (2009) предложили «три уровня судебной экспертизы», которые можно использовать на местах или в лаборатории:

1. *Судебно-экспертный осмотр на основе обследования/сортировки*. Такой осмотр проводится с целью быстрого изучения потенциальных источников доказательств и определения приоритетных источников для дальнейшего исследования на основе значимости доказательств, которые они могут содержать, и изменчивости этих доказательств (Casey, Ferraro, and Nguyen, 2009, p. 1353 and 1356).

2. *Предварительная судебная экспертиза*. Для ускорения процесса цифровой судебной экспертизы проводится *предварительная судебная экспертиза*

источников, выбранных на этапе *судебно-экспертного осмотра на основе обследования/сортировки*, чтобы обнаружить информацию, которая может быть использована в расследовании для получения прямых, косвенных или других подкрепляющих доказательств предполагаемого преступления (Casey, Ferraro, and Nguyen, 2009, pp. 1353 and 1356-1359). Неспособность обнаружить артефакты для судебно-экспертного анализа (т.е. данных, которые могут иметь значение для цифровой судебной экспертизы) во время этого осмотра, что может произойти в результате упущения их из виду, не означает автоматически, что углубленная судебная экспертиза проводиться не будет (это зависит от конкретного дела и от политики и процедур лиц, проводящих экспертизу).

3. *Углубленная судебная экспертиза*. Исследуются все источники доказательств. Экспертиза такого типа зачастую проводится в случаях, «когда есть подозрение на уничтожение доказательств, когда возникают дополнительные вопросы, и когда дело близится к судебному разбирательству» (Casey, Ferraro, and Nguyen, 2009, p. 1359).

В настоящее время продолжаются дебаты относительно жизнеспособности и актуальности каждой модели и ее компонентов (Valjarevic and Venter, 2015; Du, Le-Khac, and Scanlon, 2017). Реальность такова, что каждая страна следует своим собственным стандартам, протоколам и процедурам в области цифровой криминалистики. Однако различия в этих процессах служат препятствием для осуществления международного сотрудничества в проведении расследований правоохранительными органами (см. модуль 7 серии модулей по киберпреступности: «Международное сотрудничество в борьбе с киберпреступностью»).

Стандарты и передовые практические методы в области цифровой криминалистики

Международная организация по стандартизации (ИСО), международная неправительственная организация, и Международная электротехническая комиссия (МЭК), международная некоммерческая организация, разрабатывают и публикуют международные стандарты для унификации практики, используемой в разных странах. В 2012 году Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) опубликовали международные стандарты, касающиеся обращения с цифровыми доказательствами (ISO/IEC 27037 Руководство по

идентификации, сбору, получению и сохранению свидетельств, представленных в цифровой форме). Это руководство охватывает только начальный процесс обращения с цифровыми доказательствами. Предлагаются следующие четыре этапа обращения с цифровыми доказательствами:

Идентификация. Этот этап включает в себя поиск и распознавание соответствующих доказательств, а также их документирование. На этом этапе приоритетные задачи сбора доказательств определяются на основе ценности и изменчивости доказательств (см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» для получения дополнительной информации).

Сбор. Этот этап предполагает сбор всех цифровых устройств, которые могут содержать данные, имеющие доказательную ценность. Эти устройства затем транспортируются в лабораторию судебной экспертизы или другое учреждение для сбора и анализа цифровых доказательств. Этот процесс именуется *сбором данных в статическом режиме*. Однако бывают случаи, когда сбор данных в статическом режиме является практически неосуществимым. В таких ситуациях осуществляется *сбор данных в реальном времени*. Рассмотрим, к примеру, системы критически важных объектов инфраструктуры (например, системы управления производственными процессами). Эти системы не могут быть отключены от питания, поскольку они предоставляют критически важные услуги. Поэтому в этих случаях осуществляется сбор данных в реальном времени, когда изменчивые и неизменчивые данные извлекаются из систем, работающих в реальном времени. Однако такой сбор данных в реальном времени может мешать нормальному функционированию систем управления производственными процессами (например, замедлять их работу) (см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» для получения дополнительной информации).

> *Примечание:*
>
> Прежде чем приступить к сбору данных в реальном времени, следует определить приоритеты сбора данных с точки зрения их доступности, а также их ценности и изменчивости.

Получение. Цифровые доказательства необходимо получать без ущерба для целостности данных. Национальный совет начальников полиции Соединенного Королевства (NPCC), ранее известный как Ассоциация руководителей полицейских служб Соединенного Королевства, придает этому требованию большое значение и выделяет его в качестве важного принципа в практике цифровой криминалистики (принцип №.1: «Никакие

действия, предпринимаемые правоохранительными органами, лицами, работающими в этих органах, или их представителями, не должны приводить к изменению данных, которые впоследствии могут использоваться в суде») (UK Association of Chief Police Officers, 2012, p. 6). Такое получение данных без их изменения осуществляется путем создания копии содержимого цифрового устройства (процесс, известный как *создание неискаженного образа*) с использованием устройства (*блокировщика записи*), которое предназначено для предотвращения изменения данных в процессе копирования. Для того чтобы определить, является ли дубликат точной копией оригинала, значение хэш-функции рассчитывается с использованием математических вычислений; здесь для получения значения хэш-функции используется криптографическая хэш-функция. Если значения хэш-функции для оригинала и копии совпадают, то содержимое копии является точно таким же, что и в оригинале. Признавая возможность существования определенных «обстоятельств, при которых какое-либо лицо считает необходимым получить доступ к исходным данным [т.е. осуществить сбор данных в реальном времени]», Национальный совет начальников полиции Соединенного Королевства отмечает, что «лицо, [получающее доступ к этим данным], должно быть компетентным для таких действий и быть в состоянии представить доказательства, объясняющие целесообразность своих действий и их последствия» (Принцип №.2) (UK Association of Chief Police Officers, 2012, p. 6) (см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» для получения дополнительной информации).

Примечание:

Некоторые криптографические хэш-функции имеют недостатки.

Хотите знать больше?

- Thompson, Eric. (2005). MD5 collisions and the impact on computer forensics. *Digital Investigation* 2, 36-40. http://msn.iecs.fcu.edu.tw/report/data/ori_paper/2005-9-15/MD5%20collisions%20and%20the%20impact%20on%20computer%20forensics.pdf.
- Vijayan, Jaikumar. (2017). Researchers from Google, CTI Break SHA-1 Hash Encryption Function. *eWeek*, 23 February 2017. http://www.eweek.com/security/researchers-from-google-cti-break-sha-1-hash-encryption-function .

Сохранение. Целостность цифровых устройств и цифровых доказательств может быть обеспечена с использованием *системы охраны доказательств* (рассматривается в

модуле 3 серии модулей по киберпреступности: «Правовая база и права человека»), которая определяется как «процесс, при помощи которого следователи обеспечивают охрану места преступления (или происшествия) и сохранность доказательств на протяжении всего периода производства по делу. В журнал регистрации записывают информацию о том, кто осуществлял сбор доказательств, где и каким образом они были собраны, какие лица получили эти доказательства, и когда они их получили» (Maras, 2014, p. 377). Тщательное документирование процесса цифровой судебной экспертизы на каждом этапе имеет важное значение для обеспечения допустимости доказательств в суде (см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» для получения дополнительной информации).

Остальные этапы процесса цифровой судебной экспертизы (анализ и отчетность) не включены в руководство ISO/IEC 27037. Этап *анализа* (или исследования) требует использования надлежащих инструментов и методов цифровой криминалистики для обнаружения цифровых данных. На рынке доступно большое количество инструментов самого разного качества для проведения цифровой судебной экспертизы. Примеры инструментов для цифровой криминалистической экспертизы включают в себя программы EnCase, FTK, и X-Ways Forensics. Выбор типа инструмента зависит от типа проводимой цифровой судебной экспертизы (например, для криминалистической экспертизы мобильных устройств и облачных сервисов на мобильных устройствах можно использовать программу Oxygen Forensics Suite; для сетевой криминалистики, которая предполагает «использование научно-обоснованных методов расследования [преступлений, совершенных в отношении и с использованием] компьютерных сетей» (Maras, 2014, p. 305), в качестве инструмента можно использовать программу Wireshark). Существующие инструменты цифровой криминалистики (например, EnCase, FTK и NUIX) предназначены для работы с традиционными вычислительными устройствами. Специализированные инструменты цифровой криминалистики необходимы, например, для экспертизы сетей, интерфейсов и операционных систем критически важных объектов инфраструктуры (рассматривается в модуле 2 серии модулей по киберпреступности: «Основные виды киберпреступности»).

Национальный институт стандартов и технологий США имеет доступную для поиска базу данных инструментов цифровой криминалистики, которая содержит информацию об инструментах с различными функциями (например, инструменты для проведения криминалистической экспертизы баз данных, облачных хранилищ, беспилотных летательных аппаратов, транспортных средств и т.п.). Национальные правоохранительные органы разных стран имеют разные предпочтения в отношении использования инструментов для цифровой криминалистической экспертизы.

Криминалистическая экспертиза «умных» транспортных средств

Криминалистическая экспертиза «умных» транспортных средств является малоизученной, но важной областью цифровой криминалистики (Parkinson and McKay, 2016). Массовое использование интеллектуальных транспортных средств с функциями выхода в Интернет (и разработка автономных транспортных средств) придали дополнительный импульс усилиям по созданию процедур, стандартов и инструментов проведения криминалистической экспертизы интеллектуальных транспортных средств, которые могли бы обеспечить возможность проведения надежной с точки зрения криминалистики цифровой экспертизы таких средств (Le-Khac et al., 2018). Эти транспортные средства могут обеспечить получение большого количества информации (например, о маршрутах поездок и часто посещаемых местах, домашних и рабочих адресах, набранных номерах телефонов, принятых звонках и т.д.), которая может использоваться при расследовании преступлений, совершенных в отношении интеллектуальных или автономных транспортных средств (например, взлома), или других преступлений, когда информация, полученная из этих транспортных средств, может быть использована в качестве доказательства совершения преступления (De La Torre, Rad, and Choo, 2018).

Хотите знать больше?

De La Torre, Gonzalo, Paul Rad, and Kim-Kwang Raymond Choo. (2018). Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems*, available online 11 January 2018.

Le-Khac, Nhien-An, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang, and Raymond Choo. (2018). Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems*, available online 7 June 2018.

Используемые инструменты должны быть *надежными с точки зрения криминалистики*. При этом процесс «сбора и последующего анализа… [цифровых] данных» с помощью этих инструментов должен быть в состоянии сохранить «данные в том состоянии, в котором они были впервые обнаружены», и «никоим образом не уменьшать доказательную ценность электронных данных из-за технических или процедурных ошибок либо ошибок в интерпретации» (McKemmish, 2008, p. 6). Проще говоря, полученные данные не должны быть каким-либо образом изменены, то есть их целостность должна быть сохранена. В

рамках Программы тестирования инструментов компьютерной криминалистики Национального института стандартов и технологий США

была принята методология тестирования программных средств компьютерно-технической экспертизы на основе разработки общих спецификаций инструментов, процедур испытаний, критериев испытаний, наборов тестов и оборудования для тестирования. Тестирование дает возможность получить информацию, которая необходима разработчикам для совершенствования разрабатываемых инструментов, позволяет пользователям делать осознанный выбор в отношении приобретения и использования инструментов компьютерно-технической экспертизы и способствует пониманию возможностей инструментов всеми заинтересованными сторонами.

Криминалистическая экспертиза Интернета вещей

Интернет вещей означает сеть взаимосвязанных и взаимодействующих друг с другом устройств с выходом в Интернет (например, камеры, телевизоры, холодильники, духовые шкафы, осветительные приборы, счетчики электрической энергии, одежда, игрушки, аксессуары и многое другое), которые позволяют отслеживать объекты, людей, животных и растения, а также осуществлять сбор, анализ, хранение и распространение данных о них (Maras, 2015). Поскольку сетевые устройства Интернета вещей могут содержать значительный объем информации о пользователях этих устройств (см. модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных» для ознакомления с типами информации, которые можно обнаружить с помощью этих устройств), данные, полученные из этих устройств, представлялись в качестве доказательств в судах (Maras and Wandt, 2018). Например, в Соединенных Штатах данные из FitBit, сетевого устройства Интернета вещей, которое отслеживает состояние здоровья и физическую активность, были представлены в качестве доказательства убийства Конни Дабэйт (Altimari, 2018). Учитывая, что данные из сетевых устройств Интернета вещей представляются в качестве доказательств в судах, необходимо разрабатывать процедуры, стандарты и инструменты для проведения криминалистической экспертизы таких сетевых устройств (Maras and Wandt, 2018).

Хотите знать больше?

- Conti, Mauro, Ali Dehghantanha, Katrin Franke, and Steve Watson. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, Vol. 78(2), 544-546.
- MacDermott, Aine, Thar Baker, and Qi Shi. (2018). IoT Forensics: Challenges for the IoA Era 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (2 April 2018). https://core.ac.uk/download/pdf/146487345.pdf.
- Watson, Steve and Ali Dehghantanha. (2016). Digital forensics: The missing piece of the Internet of Things promise. *Computer Fraud & Security*, Vol. 6, 5-8.

Целью этапа анализа является определение значимости и доказательственной силы свидетельств. Это делается, например, путем определения того, имеет ли рассматриваемое доказательство «тенденцию делать существование любого факта, имеющего значение для разрешения дела, более или менее вероятным, чем это было бы без этого доказательства» (Правило 401, Федеральные правила США о доказательствах) (см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» для получения дополнительной информации).

Этап *отчетности* включает в себя подробное описание шагов, предпринятых на протяжении всего процесса цифровой судебной экспертизы, обнаруженных цифровых доказательств и выводов, сделанных на основе результатов цифровой судебной экспертизы и обнаруженных доказательств (см. модуль 6 серии модулей по киберпреступности: «Практические аспекты расследования киберпреступлений и цифровой криминалистики» для получения дополнительной информации). *Искусственный интеллект* (т.е. «вычислительные модели человеческого поведения и мыслительных процессов, предназначенные для рациональной и разумной работы»; Maras, 2017, p. 7) может использоваться для получения достоверных результатов. Однако использование искусственного интеллекта может создавать проблемы на этапах анализа и представления данных процесса цифровой судебной экспертизы, поскольку эксперты могут быть не в состоянии объяснить, как были получены эти результаты (Maras and Alexandrou, 2018).

ИСО/МЭК опубликовали дополнительные руководства по процессу цифровой криминалистики, которые охватывают: достоверность и надёжность инструментов и методов цифровой судебной экспертизы (ISO/IEC 27041:2015, Руководство по обеспечению пригодности и адекватности метода расследования инцидентов), а также

этапы исследования (или анализа) и интерпретации процесса цифровой судебной экспертизы (ISO/IEC 27042:2015, Руководство по анализу и интерпретации цифровых свидетельств).

> *Примечание:*
>
> Эти стандарты не предназначены для нетрадиционных вычислительных систем, таких как облачные вычисления. Тем не менее, Cloud Security Alliance (Альянс безопасности в облаке) опубликовал документ под названием «Привязка криминалистического стандарта ISO/IEC 27037 к облачным вычислениям» с целью «нового истолкования руководства ISO 27037 для облачногоконтекста» (CSA, 2013, p. 130).
>
> Для получения дополнительной информации см.: https://downloads.cloudsecurityalliance.org/initiatives/imf/Mapping-the-Forensic-Standard-ISO-IEC-27037-to-Cloud-Computing.pdf.

В настоящее время доступны руководства по передовой практике для определения и популяризации обоснованных и надежных процессов и результатов цифровой судебной экспертизы. В качестве примеров можно привести руководство по передовой практике, разработанное в США Научной рабочей группой по цифровым доказательствам, для компьютерно-технической судебной экспертизы, сбора цифровых доказательств и сбора данных для компьютерно-технической экспертизы, а также руководство по передовой практике *Европейской Сети* судебно-экспертных учреждений для судебной экспертизы цифровых технологий.

Эти стандарты и передовые практические методы используются с целью установления *обоснованности* и *достоверности* результатов цифровой судебной экспертизы. Во-первых, для того они были допустимыми, инструменты и методы, используемые в процессе цифровой судебной экспертизы, должны быть «научно обоснованными», то есть путем эмпирического тестирования должно быть доказано, что они дают точные результаты. Во-вторых, результаты цифровой судебной экспертизы должны быть достоверными, то есть одни и те же результаты должны быть получены в разных случаях с использованием одних и тех же данных, инструментов и методов (Maras, 2014; p. 48). В частности, результаты должны быть повторяемыми и воспроизводимыми. Результаты являются *повторяемыми*, когда одни и те же результаты цифровой судебной экспертизы получаются с использованием одних и тех же тестируемых предметов, оборудования, лаборатории и оператора (Maras, 2014, p. 48). Результаты являются *воспроизводимыми*, когда одни и те же результаты цифровой судебной экспертизы получаются с использованием одних и тех же тестируемых предметов, но с использованием разных

видов оборудования, лабораторий и операторов (Maras, 2014, p. 49). Как отметил Национальный совет начальников полиции Соединенного Королевства, важным принципом практики цифровой криминалистики является способность «независимой третьей стороны… изучать эти процессы и достигать того же результата» (Принцип 3) (UK Association of Police Chiefs, 2012, p. 6).

Антикриминалистика

Антикриминалистика (или цифровая антикриминалистика) – это термин, используемый для описания «инструментов и методов, [используемых] для удаления, изменения, нарушения данных или иного влияния на доказательства преступной деятельности в цифровых системах, аналогично тому, как если бы преступники удалили доказательства с места преступления в физическом мире» (Conlan, Baggili, and Brietinger, 2016, p. 67). Методы антикриминалистики включают в себя сокрытие данных (например, шифрование, которое дополнительно рассматривается в модуле 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных», и стеганография – практика сокрытия секретных данных, изображений, аудиозаписей, видеоматериалов и иного контента путем их встраивания в несекретные данные, изображения, аудиозаписи, видеоматериалы и иной контент), стирание артефактов и/или содержимого цифровых устройств (например, с помощью программного обеспечения, предназначенного для удаления отдельных или всех данных и/или содержимого устройств) и запутывание цифрового следа (например, тактика спуфинга (подмены), рассматриваемая в модуле 2 серии модулей по киберпреступности: «Основные виды киберпреступности»; ошибочная идентификация данных, дезинформация и/или фабрикация данных; и использование прокси-серверов, которые действуют как шлюз или посредник между запросами, направляемыми от цифровых устройств, подключенных к Интернету, в другие серверы) (Shanmugam, Powell, and Owens, 2011; Maras, 2014; Brunton and Nissenbaum, 2016; Liskiewicz, Reischuk, and Wolfel, 2017). Использование методов антикриминалистики затрудняет усилия по проведению цифровой судебной экспертизы (Caviglione, Wendzel, and Mazurczyk, 2017).

Хотите знать больше?

См.: Conlan, Kevin, Ibrahim Baggili, and Frank Breitinger. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation* Vol. 18, 66-75.

Заключение

Цифровая криминалистика включает в себя процессы идентификации, получения, сохранения, анализа и представления цифровых доказательств. Цифровые доказательства должны быть аутентифицированы, чтобы обеспечить их допустимость в суде. В конечном счете артефакты для судебно-экспертного анализа и используемые криминалистические методы (например, сбор данных в статическом режиме или в реальном времени) зависят от устройства, его операционной системы и его средств защиты. Запатентованные операционные системы (с которыми следователи могут быть незнакомы) и средства защиты (например, шифрование) служат препятствиями для проведения цифровой судебной экспертизы. Например, *шифрование*, которое блокирует доступ третьих лиц к информации о пользователях и их сообщениям, может помешать правоохранительным органам получить доступ к данным, содержащимся в цифровых устройствах, таких как смартфоны (см. модуль 10 серии модулей по киберпреступности: «Конфиденциальность и защита данных» для получения дополнительной информации).

Список использованной литературы

- Alba, Manuel. (2014). Order out of chaos: technology, intermediation, trust, and reliability as the basis for the recognition of legal effects in electronic transactions. *Creighton Law Review*, Vol. 47, 387–521.
- Altimari, Dave. (2018). All Evidence Turned Over As Fitbit Murder Case Moves Toward Trial. *Hartford Courant*, 20 July 2018. https://www.courant.com/news/connecticut/hc-news-fit-bit-murder-dabate-trial-20180720-story.html.
- Antwi-Boasiako, Albert and Hein Venter. (2017). A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). *Advances in Digital Forensics* (pp. 23-38). Springer.

- Baryamureeba, Venansius and Florence Tushabe. (2004). The Enhanced Digital Investigation Process Model. Proceedings of the Digital Forensic Research Conference (DFRWS) (Baltimore, Maryland, 11-13 August 2004). https://www.dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf.
- Bazin, Philippe. (2008). An Outline of the French Law on Digital Evidence. *Digital Evidence and Electronic Signature Law Review*, Vol. 5, 179-182. http://sas-space.sas.ac.uk/5543/1/1864-2592-1-SM.pdf
- Biasiotti, Maria Angela, Jeanne Pia Mifsud Bonnici, Joe Cannataci (eds.) (2018). *Handling and Exchanging Electronic Evidence Across Europe*. Springer.
- Brunton, Finn and Helen Nissenbaum. (2016). *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press.
- Carrier, Brian and Eugene H. Spafford. (2003). Getting Physical with the Investigative Process. *International Journal of Digital Evidence*, Vol. 2(2), https://pdfs.semanticscholar.org/915b/524318e2f0689b586ba7ae89ea39e9b22ce3.pdf.
- Casey, Eoghan, Monique Ferraro, and Lam Nguyen. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. *Journal of Forensic Sciences*, Vol. 54(6), 1353-1364.
- Caviglione, Luca, Steffen Wendzel, and Wojciech Mazurczyk. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security & Privacy*, Vol. 15(6), 12-17.
- Conlan, Kevin, Ibrahim Baggili, and Frank Breitinger. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. *Digital Investigation* Vol. 18, 66-75.
- Conrad, Scott, Greg Dorn and Philip Craiger. (2010). Forensic analysis of a Playstation 3 console. Advances in Digital Forensics VI: IFIP International Conference on Digital Forensics (pp. 65-76). https://hal.inria.fr/hal-01060610/document.
- De La Torre, Gonzalo, Paul Rad, and Kim-Kwang Raymond Choo. (2018). Driverless vehicle security: Challenges and future research opportunities. *Future Generation Computer Systems*, available online 11 January 2018.
- Du, Xiaoyu, Nhien-An Le-Khac, and Mark Scanlon. (2017). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. 16th European Conference on Cyber Warfare and Security (Dublin, Ireland, June 2017). https://arxiv.org/pdf/1708.01730.pdf.
- Duranti, Lucciana and Corrine Rogers. (2012). Trust in digital records: an increasingly cloudy legal area. *Computer Law & Security Review*, Vol. 28(5), 522–531.
- Goode, Steven. (2009). The admissibility of electronic evidence. *The Review of Litigation*, Vol. 29, 1–64.

- Kasper, Agnes and Eneli Lauritis. (2016). Challenges in Collecting Digital Evidence: A Legal Perspective. In Tanel Kerikmae and Addi Rull. *The Future of Law and eTechnologies*. Springer.
- Kent, Karen, Suzanne Chevalier, Timothy Grance, and Hung Dang. (2006). SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology. https://dl.acm.org/citation.cfm?id=2206298.
- Le-Khac, Nhien-An, Daniel Jacobs, John Nijhoff, Karsten Bertens, Kim-Kwang, and Raymond Choo. (2018). Smart vehicle forensics: Challenges and case study. *Future Generation Computer Systems*, available online 7 June 2018.
- Liskiewicz, Macief, Rudiger Reischuk, and Ulrich Wolfel. (2017). Security levels in steganography – Insecurity does not imply detectability. *Theoretical Computer Science* Vol. 692(5), 25-45.
- Maras, M.-H. (2014). *Computer Forensics: Cybercriminals, Laws and Evidence* (2nd edition). Jones and Bartlett.
- Maras, Marie-Helen. (2017). Social Media Platforms: Targeting the "Found Space" of Terrorists. *Journal of Internet Law*, *21*(2), 3-9.
- Maras, Marie-Helen and Miranda, Michelle D. (2014). Forensic Science. In J. Backhaus (Ed.). *Encyclopedia of Law and Economics*. Springer.
- Maras, Marie-Helen and Alexandrou, Alex. (2018). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. *International Journal of Evidence and Proof*, published online 28 October 2018.
- Maras, Marie-Helen and Wandt, Adam. (2018). IoT Data Collection and Analytics. Presentation for FBI, DHS, and Secret Service agents and members of the National Cyber-Forensics & Training Alliance, at John Jay College of Criminal Justice, City University of New York (2 May 2018).
- McKemmish, Rodney. (2008). When is digital evidence forensically sound? Advances in Digital Forensics IV: IFIP International Conference on Digital Forensics (pp. 3-15). https://link.springer.com/content/pdf/10.1007%2F978-0-387-84927-0_1.pdf.
- Palmer, G. (2001). DFRWS Technical Report: A Road Map for Digital Forensic Research. Digital Forensic Research Workshop. Utica, New York. http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf.
- Parkinson, M. J. and Matthew G. McKay. (2016). The Evolution of Vehicle Forensics. *The Expert Witness*, 31 May 2016. http://www.expertwitnessjournal.co.uk/forensics/732-the-evolution-of-vehicle-forensics.
- Read, Huw, Elizabeth Thomas, Iain Sutherland, Konstantinos Xynos and Mikhaila Burgess. (2016). A forensic methodology for analyzing Nintendo 3DS devices. Advances in Digital Forensics XII: IFIP International Conference on Digital Forensics (pp. 127-143).

- Reith, Mark, Clint Carr, and Gregg Gunsch. (2002). An Examination of Digital Forensics Models. *International Journal of Digital Evidence*, Vol. 1(3).
- Shanmugam, Karthikeyan, Roger Powell and Tom Owens. (2011). An Approach for Validation of Digital Anti-Forensic Evidence. *Information Security Journal: A Global Perspective* 20(4-5), 219-230.
- Valijarevic, Aleksandar and Hein S. Venter. (2015). A Comprehensive and Harmonized Digital Forensic Investigation Process Model. *Journal of Forensic Sciences*, Vol. 60(6), 1467-1483.
- UK Association of Police Chiefs. (2012). ACPO Good Practice Guide for Digital Evidence. https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
- U.S. National Institute of Justice. (2008). Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Second Edition. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf
- U.S. National Institute of Standards and Technology. Computer Forensics Tool Testing Program. https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

Список дел

- *Regina (O) v. Coventry Magistrates Court* [2004] EWHC 905.

Законы

- Закон об электронных доказательствах 2011 года (Белиз) (https://www.centralbank.org.bz/docs/default-source/2.10-national-payment-system-act/cap-95-01-electronic-evidence-act.pdf?sfvrsn=2).
- Закон об электронных операциях 2015 года (Танзания) (http://velmalaw.com/wp-content/uploads/2016/11/Electronic-Transactions-Act-2015.pdf).
- Закон о доказательствах 1950 года (Малайзия) (https://empowermalaysia.org/isi/uploads/sites/3/Act-56-Evidence-Act-1950.pdf).
- Закон о доказательствах 1967 года (Танзания) (http://www.fiu.go.tz/evidenceact.pdf).
- Закон о доказательствах (с поправками) 2012 года (Сингапур) (https://sso.agc.gov.sg/Acts-Supp/4-2012/Published/20120416?DocDate=20120416).
- Федеральные правила о доказательствах (Соединенные Штаты Америки) (https://www.law.cornell.edu/rules/fre).

- Постановление правительства №.82 от 2012 года (Индонезия) (http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html).
- Закон об информационных технологиях 2000 года (Индия) (http://www.wipo.int/wipolex/en/text.jsp?file_id=185998).
- Закон №.11 от 2008 года об электронной информации и операциях (Индонезия) (http://www.bu.edu/bucflp-fig/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf).
- Закон о письменных законах (с различными поправками) 2007 года (Танзания) (https://www.fiu.go.tz/MiscellaneousAmendmentsAct.pdf).

Упражнения

Упражнение №.1 – О данных

Цифровые устройства получили широкое распространение. Специалистам по цифровой судебной экспертизе необходимо быстро обрабатывать и анализировать большие объемы данных.

Попросите своих учащихся осуществить поиск в Интернете и выбрать цифровое устройство (в качестве альтернативы они могут обсудить устройство, которым они владеют). Учащиеся должны быть готовы обсудить устройство и ответить на следующие вопросы на занятии:

Вопросы для обсуждения

1. Какие данные хранит это устройство?
2. К какому типу относятся эти данные?
3. Где расположены эти данные?
4. Как можно определить местоположение этих данных?

Методические рекомендации для лектора

Это упражнение в некоторой степени зависит от технической подготовки учащихся. Если учащиеся имеют техническую подготовку, попросите их обсудить конкретные места, где хранятся данные, и как их можно оттуда извлечь. Если учащиеся не имеют технической

подготовки, попросите их рассмотреть их собственные данные, и как они могут обнаружить данные, когда им это нужно.

Упражнение №.2 – Инструменты цифровой криминалистики

На рынке доступно большое количество инструментов для проведения цифровой судебной экспертизы. Попросите учащихся поискать инструмент цифровой криминалистики, наиболее широко используемый в их стране.

Вопросы для обсуждения

1) Для какого типа судебной экспертизы используется этот инструмент?
2) Является ли этот инструмент надежным с точки зрения криминалистики?

Возможная структура занятия

Ниже описана рекомендуемая структура для занятия. Учащиеся должны закончить прочтение обязательной литературы до начала занятия. Лекции призваны закрепить материал, с которым учащиеся ознакомились при прочтении литературы, а упражнения предназначены для практического применения знаний, полученных из прочтенной литературы и лекций. Для трехчасового занятия предлагается следующая структура. Лекторы могут изменить эту структуру, исходя из своих потребностей и расписания занятий.

Представление занятия и результатов обучения

Лекция (10 минут):

- Вкратце представьте занятие и его содержание
- Определите и обсудите конечные результаты занятия

Цифровые доказательства

Лекция (30 минут):

- Обсудите данные и определите источники данных
- Опишите и обсудите цифровые доказательства

- Опишите цифровые доказательства и традиционные доказательства и объясните различия между ними
- Обсудите способы аутентификации цифровых доказательств

Упражнение (20 минут):
В разделе «Упражнения» данного модуля имеется отдельное упражнение под заголовком «Упражнение №.1 – О данных». Используйте вопросы из этого упражнения для проведения обсуждения этой темы.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

Групповое упражнение (20 минут):
Попросите учащихся выполнить «Домашнее задание №.1 ~ Групповое упражнение: Традиционные доказательства в сравнении с цифровыми доказательствами» в разделе «Оценка учащихся» до начала занятия и попросите их обсудить результаты во время лекции.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

Перерыв

Время: 10 минут

Цифровая криминалистика

Лекция (30 минут):

- Опишите и критически оцените модели процесса цифровой криминалистики

Стандарты и передовые практические методы в области цифровой криминалистики

Лекция (40 минут):

- Критически оцените стандарты и передовые практические методы в области сбора цифровых доказательств и проведения цифровой судебной экспертизы

Упражнение (20 минут):
В разделе «Упражнения» данного модуля имеется отдельное упражнение под заголовком «Упражнение №.2 – Инструменты цифровой криминалистики ». Используйте вопросы из этого упражнения для проведения обсуждения этой темы.
[*Напоминание: это упражнение должно быть выполнено до начала занятия].

Список основной литературы

Следующие публикации (в основном доступные в открытых источниках), входящие в категорию обязательной для прочтения литературы, должны быть заданы учащимся и прочтены ими до начала занятий по данному модулю:

- Altheide, Cory and Harlan Carvey. (2011). *Digital Forensics with Open Source Tools* (pp. 1-8). Science Direct.
- Bulbula, H. I., H. Guclu Yavuzcanb, and Mesut Ozel. (2013). Digital forensics: An Analytical Crime Scene Procedure Model (ACSPM). *Forensic Science International*, Vol. 233(1–3), 244–256.
- Casey, Eoghan, Monique Ferraro, and Lam Nguyen. (2009). Investigation Delayed Is Justice Denied: Proposals for Expediting Forensic Examinations of Digital Evidence. *Journal of Forensic Sciences*, Vol. 54(6), 1353-1364.
- ISACA. (2015). Overview of Digital Forensics. http://www.infosecurityeurope.com/__novadocuments/83665?v=635652368156170000.
- Karie, Nickson M. and H. S. Venter (2015). Taxonomy of Challenges for Digital Forensics. *Journal of Forensic Sciences*, Vol. 60(4), 885–893.
- Maras, Marie-Helen. (2014). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Jones and Bartlett.
- Myers, Matthew and Marcus Rogers. (2007). Digital Forensics: Meeting the Challenges of Scientific Evidence. Advances in Digital Forensics: IFIP International Conference on Digital Forensics (pp. 43-50).
- Roussev, Vassil, Candace Quates, and Robert Martel. (2013). Real-time digital forensics and triage. *Digital Investigation* Vol. 10(2), 158–167.
- Sammons, John. (2017). *Digital forensics*, 2st edition. Elsevier.

Список дополнительной литературы

Следующая литература рекомендуется учащимся, заинтересованным в более детальном изучении тематических вопросов, охваченных данным модулем:

- Alavrez, Karolina and Masooda Bashir. (2015). Exploring the Effectiveness of Digital Forensics Tools on the Sony PlayStation Vita. Joshua I. James and Frank Breitinger, eds. 7th International Conference on Digital forensics and Cyber Crime, Selected Conference Papers (Seoul, South Korea, 6-8 October 2015).
- Antwi-Boasiako, Albert and Hein Venter. (2017). A Model for Digital Evidence Admissibility Assessment. G. Peterson and S. Shenoi. (eds.). *Advances in Digital Forensics* (pp. 23-38). Springer.
- Barmpatsalou, Konstantia, Dimitrios Damopoulos, Georgios Kambourakis, and Vasilios Katos. (2013). A critical review of 7 years of Mobile Device Forensics.
- *Digital Investigation*, Vol. 10(4), 323-349.
- Burke, Paul and Philip Craiger. (2007). Forensic Analysis of Xbox Consoles. Advances in Digital Forensics III: IFIP International Conference on Digital Forensics (pp. 269-280).
- Eden, Peter, Andrew Blyth, Pete Burnap, Yulia Cherdantseva, Kevin Jones, High Soulsby, and Kristin Stoddart. (2015). A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure. 10the International Conference, Critical Information Infrastructure Security (CRITIS), Berlin, Germany (pp. 27-39).
- Joshi, R. C. and Pilli, Emmanuel S. (2016). *Fundamentals of Network Forensics: A Research Perspective*. Springer.
- Pieterse, Heloise and Martin Olivier. (2014). Smartphones as Distributed Witnesses for Digital Forensics. Advances in Digital Forensics X: IFIP International Conference on Digital Forensics (pp. 237-251). https://hal.inria.fr/hal-01393774/document.
- Quick, Darren and Kim-Kwang Raymond Choo. (2017). Pervasive social networking forensics: Intelligence and evidence from mobile device extracts.
- *Journal of Network and Computer Applications*, Vol. 86, 24-33.
- Sommer, Peter. (2018). Accrediting digital forensics. *Digital Investigation*, Vol. 25, 116-120.
- Suleman, Khan, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Muhammad Shiraz, and Iftikhar Ahmad. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications* 66, 214-235.
- UK Crown Prosecution Service. (n.d.). Cybercrime - prosecution guidance.

https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

Оценка учащихся

В дополнение к упражнениям, другими средствами для оценки учащихся, используемыми в данном модуле, являются обзорные вопросы и домашние задания.

Обзорные вопросы

Эти вопросы могут также использоваться для стимулирования групповых обсуждений во время лекции.

1. В чем заключается различие между данными, относящимися к контенту, и метаданными? Какие типы информации может содержать каждый из этих типов данных?
2. Какие типы электронных доказательств существуют?
3. В чем заключается различие между электронными доказательствами и традиционными доказательствами?
4. Как осуществляется аутентификация цифрового доказательства?
5. Какие существуют модели процесса цифровой криминалистики? Назовите и опишите две модели.
6. С какой целью используются стандарты и передовые практические методы сбора цифровых доказательств и проведения цифровой судебной экспертизы?

Домашние задания

Домашнее здание №.1 ~ Групповое упражнение: Традиционные доказательства в сравнении с цифровыми доказательствами

До начала занятия учащихся следует в произвольном порядке распределить по группам, чтобы они могли выполнить задание до того, как все группы соберутся в классе. Каждой группе в произвольном порядке должна быть определена страна.

Поручите учащимся определить и рассмотреть нормы доказательственного права, относящиеся к цифровым доказательствам, в распределённой им стране. Учащиеся

должны также определить, являются ли требования, действующие в распределённой им стране в отношении допустимости доказательств, схожими для традиционных доказательств и цифровых доказательств.

Учащиеся должны быть готовы к обсуждению своих результатов в классе.

Домашнее здание №.2 ~ Допустимость цифровых доказательств

Следующее задание предлагается выполнить в течение двух недель после проведения лекции по данному модулю:

Рассмотрите дела, рассматривавшиеся в судах в вашей стране в прошлом, и опишите факторы и обстоятельства, которые учитывались судами, при принятии решения о признании цифровых доказательств допустимыми. Когда цифровые доказательства были признаны допустимыми? При каких обстоятельствах они отклонялись? Пожалуйста, используйте доводы, основанные на фактах, в подтверждение своего ответа. Рекомендуемый максимальный объем: 1500 слов.

Дополнительные средства обучения

Вебсайты

- DFIR Science, Digital Forensic Science.
  https://dfir.science/.
- INFOSEC Institute, Digital Forensics Models.
  https://resources.infosecinstitute.com/digital-forensics-models/#gref.

Видео

- Основы компьютерно-технической экспертизы – 2: Основные сведения о хэш-функции и ш*естнадцатеричной системе счисления*.
  https://www.youtube.com/watch?v=-2zJGzKpL6k.
  >> На этом видео рассматриваются хэшированные файлы и их использование в цифровой криминалистике (продолжительность: 8:42).

- Профессор Адам Вандт (Adam Wandt), Лекция о цифровой криминалистике: аппаратные средства.
  https://www.youtube.com/watch?v=-qPVtaxJWv4.
  >> На этом видео представлены примеры типов аппаратных средств, используемых специалистами по цифровой криминалистике (продолжительность: 14:52).
- Решения IBM для управления цифровыми доказательствами.
  https://www.youtube.com/watch?v=RfjGBd2SyeI.
  >> На этом видео представлены примеры источников цифровых доказательств и показано, как эти доказательства могут обобщаться для получения информации об инцидентах (продолжительность: 5:56).
- Ассоциация по аудиту и контролю информационных систем (ISACA), Обзор цифровой криминалистики.
  https://www.youtube.com/watch?v=ZUqzcQc_syE.
  >> На видео представлено краткое описание процесса цифровой судебной экспертизы (продолжительность: 5:24).

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-3389, www.unodc.org