Часопис Національного університету "Острозька академія". Серія "Право". – 2016. – №1(13)

UDC 34

Мате И. Ж.
Судебно-информатический эксперт
(Докторантура юридического
факультета Университета г. Печ)

СУДЕБНЫЙ ИТ-ЭКСПЕРТ – МЕТОДЫ И ИНСТРУМЕНТЫ В УГОЛОВНОМ ДЕЛЕ

1. Постановка проблемы

Среди участников уголовного процесса судья, прокурор и адвокат являются компетентными в специальных юридических вопросах, в то время как судебно-информатический эксперт несёт ответственность за специальные технические вопросы. Принимая во внимание отсутствие методологических рекомендаций со стороны Венгерской Палаты судебных экспертов, для того, чтобы решить, соответствует ли работа эксперта, дающего своё заключение по конкретному делу, профессиональным требованиям, необходимо привлечение другого эксперта. Учитывая абсурдность этого положения, специалисты приступили к разработке методологии и системы критериев работы судебно-информатических экспертов, и эта статья является частью этого процесса.

Digital Forensic Science

Digital Forensic Science (Судебная информатика) по мнению автора настоящих строк «...включает в себя те научные методы и процедуры,

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

которые предоставляют достоверную информацию в уголовном деле в тех случаях, когда цифровые данные и / или - в широком смысле этого термина – компьютерная система являются частью такого дела» [1]. Эта область как вспомогательная дисциплина юриспруденции помогает раскрыть факты в соответствии с основным положением, известным из римского права:» Da mihi factum, dabo tibi ius – Дай мне факт и я дам тебе право» [2]. В то же время, участники процесса должны учитывать не только цели, но и процедуры, методы, а также средства (как аппаратного, так и программного обеспечения) для достижениях этих целей должны использоваться, применяться таким образом, чтобы они соответствовали правовым нормам и профессиональным стандартам, относящимся к деятельности судебно-информатического эксперта. При проведении исследования наше внимание фокусируется именно на нормах и стандартах, потому что само понятие «Digital Forensic Science» есть редким, а профессиональные регламенты Судебной информатики почти совсем не встречаются в венгерской профессиональной литературе. В дальнейшем мы попытаемся восполнить этот недостаток посредством формулировки основных методических и инструментальных понятий.

Виды «Digital Forensic Science» в Венгрии

Определение понятия «вида» судебной экспертизы содержится в постановлении Министерства юстиции от 9/2006 (II. 27) «О видах судебной экспертизы и о профессиональной квалификации и прочих условиях, связанных с ними]. Законодательство в области информационных технологий выделяет следующие их разделы:

1. ИТ-и, компьютеры, периферийные устройства и локальные сети (хардвер);
2. Информационная безопасность;

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

3. Планирование и организация информатических систем;

4. Студийная технология, ИТ деятельность, связанная с мультимедийными технологиями;

5. Компьютерные базы данных, структуры данных;

6. Программное обеспечение.

Можно заметить, что некоторые подвиды, с одной стороны, могут пересекаться (напр. база данных – программное обеспечение), с другой стороны, могут находиться довольно далеко друг от друга (напр.: информационная безопасность – мультимедиа). На этом фоне следует выделить такую методологическую и инструментальную структуры, которые не только обоснуют, но и позволят обслуживать потребности в области судебной ИТ-экспертизы.

Методологические предпосылки «Digital Forensic Science»

Методологические основы работы судебного ИТ-эксперта обозначены в первом разделе Закона XLVII от 2005 года «О судебно-экспертной деятельности» [3]:

«1. § (1) Задача судебного эксперта состоит в том, чтобы на основании постановления или по поручению суда, нотариуса, прокуратуры, полиции и других органов власти, установленных законом, помочь в установлении фактов, принятии компетентного решения посредством дачи заключения, составленного с учётом научных данных и использованием результатов технического прогресса.

Второй раздел определяет и метод, используемый для выполнения данной задачи:

«(2) Судебно-информатический эксперт обязан осуществлять свою деятельность наилучшим образом, соблюдая положения настоящего закона

и других правовых нормативов, а также требования профессиональных регламентов, регулирующих данный вид деятельности,».

Подчёркивая суть вопроса: следует решить профессиональный вопрос с учётом научных достижений (включая и технические науки) в соответствии с директивными регламентами. В этой главе мы подробно рассмотрим директивные профессиональные регламенты.

В большинстве случаев источником этих регламентов могут быть рекомендации (методические заметки), изданные национальными или международными профессиональными организациями, в том числе национальные и/или международные стандарты, созданные с учётом этих рекомендаций.

Палата судебных экспертов Венгрии всё ещё остаётся в долгу в плане отечественных рекомендаций по некоторым сферам деятельности (издание которых возлагается на неё, либо уполномочивается в соответствии с положениями Закона CXIV от 1995 года «О Венгерской Палате судебных экспертов»), поэтому мы сможем рассмотреть рекомендации только международных организаций. Процессуальная модель исследования, разработанная организацией «Digital Forensics Research Workshop», созданной в 2001-ом году, идентифицировала следующие операции в экспертной работе [4]:

Identification – идентификация;

Preservation – сохранение;

Collection – сбор;

Examination – исследование;

Analysis – анализ;

Presentation – презентация;

Decision – решение.

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

В дальнейшем исследователи «Digital Forensic» расширили и дополнили эту модель с учётом собственных предпочтений, но, по существу, во всех последующих моделях отражается научное обоснование 2001-ого года. Это касается и первого международного стандарта ISO 27037, разработанного посредством «Digital Forensic», который следующим образом обобщает главные задачи:

5.4.1 Общие принципы:

Возможные цифровые доказательства должны рассматриваться в соответствии со следующими принципами:

– *Минимизация доступа;*

– *Документирование и обоснование всех изменений;*

– *Соблюдение правил обращения с доказательствами;*

– *Деятельность в пределах компетенции.*

5.4.2 Идентификация

В случае потенциальных цифровых доказательств поиск, идентификация и документирование должны осуществляться следующим образом:

– *Установление приоритетов в процессе сбора доказательств с учётом их изменчивости (волатильности);*

– *Минимизация причинения вреда;*

– *Идентификация скрытых цифровых доказательств.*

5.4.3 Сбор

Сбор представляет собой такой процесс, при котором средства, которые могут содержать цифровые доказательства, удаляются с места их исходного положения, а затем подвергаются анализу в какой-либо лаборатории, в контролируемой среде с целью извлечения данных.

5.4.4 Получение

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

Это процесс, посредством которого делается копия возможных цифровых доказательств.

5.4.4 Сохранение

Сохранение целостности возможных цифровых доказательств. Возможное цифровое доказательство и устройство следует защищать от некомпетентного доступа или повреждения [5].

Несмотря на то, что несколько стандартов из пакета ISO/IEC 27К (как уже опубликованные, так и ещё находящиеся в процессе подготовки) рассматривают области экспертных методологий (особенно стандарты 2703× и 2704×), в последующем мы сфокусируем внимание на вопросы, связанные с практическим применением вышеупомянутого стандарта в Венгрии.

В ходе реализации общих принципов эксперт, в первую очередь, рассматривает свою профессиональную компетентность, то есть имеет ли он полномочия давать экспертное заключение, касающееся данной области. Эта процедура выполняется посредством сопоставления профессиональной квалификации с содержанием экспертизы. Давайте рассмотрим некоторые конкретные примеры:

Задача	Круг компетентности	Экспертный номер дела
Экспертиза видеозаписи	Студийная техника, ИТ-деятельность, связанная с мультимедийными технологиями	1/2007
Определение создателя записи в блоге	Информационная безопасность	4/2010

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

Исследование компьютерной системы	ИТ- оборудование, компьютеры, периферия и локальные сети (хардвер)	13/2013

В Венгрии совместное распоряжение Министерств относительно обращения с доказательствами содержит рекомендации, в которых нет специальных указаний, касающихся информационных систем, таким образом следователи, несущие ответственность за их соблюдение, часто нарушают требования минимального доступа. Чтобы избежать этого, органы следствия могут обратиться к консультанту или эксперту при проведении обысков и конфискаций.

При идентификации возможных цифровых доказательств (Identification) основным требованием является выявление последовательности изменчивости доказательств (Order of Volatility), которое также определяет последовательность розыска и идентификации доказательств. На практике это означает, что первичным является идентификация и сохранение наиболее быстро меняющегося содержания: например, содержание оперативной памяти компьютера (обратите внимание, что это не жёсткий диск или другое устройство постоянного хранения), или содержание памяти активных компонентов компьютерной сети (напр.: маршрутизатор, мост, сетевой коммутатор). Аналогичным образом задачей эксперта является идентификация скрытых цифровых доказательств, которыми могут быть небольшой блок памяти, локальная или дистанционная облачная услуга, достигаемая через компьютерную сеть, или даже сетевое устройство, отправляющее данные скрытой камеры видеонаблюдения. Обнаружение и приобщение этих ресурсов с наименьшими повреждениями к кругу доказательств (Minimize the damage to the potential digital evidence) существенно влияет на возможность их

дальнейшего применения. Оценка и осуществление всех этих действий является задачей эксперта, однако их применение возможно только в том случае (учитывая отечественную практику), если по причине сложности расследуемого дела органы следствия привлекают эксперта к участию в расследовании уже на стадии наложения ареста.

На стадии сбора доказательств (Collection) мы подходим к такому этапу, на котором появляется возможность использования экспертом оборудования (аппаратное и программное обеспечение). Это касается особенно тех случаев, когда невозможно изъять устройства, привлекаемые к расследованию и предположительно содержащее доказательства, и/или они расположены вне места обыска. В качестве примера можно привести определение физического расположения веб-сервера, обслуживающего веб-сайт, посредством анализа сетевых подключений пользователей (веб-браузеров) (номер экспертного дела: 25/2013). Если устройство является мобильным, то операция, гарантирующая, что устройство и его содержимое, используемые в качестве доказательств, находится под постоянным и документированным наблюдением на протяжении всего уголовного процесса может быть выполнена только после безопасного, корректного и документированного останова устройства (Chain of Custody).

В оптимальном случае извлечение данных (Acquisition) происходит в экспертной лаборатории, в контролируемой среде, однако после надлежащей подготовки – когда следственные органы и эксперт заранее планируют данную операцию – извлечение может осуществляться и на месте почти без потери качества. Ключевым моментом извлечения данных на месте является время, на что необходимо обратить внимание в ходе планирования (планирование времени детализуется в разделе оборудования).

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

Процедуры сохранения и подготовки извлеченных данных для презентации так же важны, как и их идентификация, сбор или извлечение. Так как на следственном этапе сохраненные цифровые доказательства попадают в руки следователя, который должен их интерпретировать, сделать определённые выводы. Все эти действия невозможны, если эксперт не передаст данные в правильном формате, на соответствующем носителе, который обеспечит их целостность и достоверность в ходе процесса передачи.

Учитывая условия Венгрии, мы можем сказать, что этот этап работ является одним самых сложных. В отношении носителей и форматов данных следственные органы находятся в менее благоприятном положении по сравнению с грамотностью в области информатики в целом, это касается как оснащенности оборудованием, так и наличия навыков и знаний. Это означает, что приём некоторых носителей данных не решён (напр.: Blu-ray диск), потому что нет считывающих устройств, а без надлежащего количества устройств, снабженных защитой от записи, нет возможности для безопасного считывания жёстких дисков, хранящих большое количество информации (подробности ниже), кроме того подготовленность следователей в области информатики недостаточна для оценки цифровых доказательств.

Вследствие этих обстоятельств весь результат процесса по вышеупомянутой методологии может стать сомнительным и соответственно с этим, требует немедленного действенного вмешательства руководящих работников по вышеупомянутым пунктам.

5. Инструментарий «Digital Forensic Science»

Иструментарий, использованный на отдельных этапах вышеописанной методологии, состоит из двух основных компонентов:

программного обеспечения – софтвер и аппаратного обеспечения – хардвер. На этапе сбора и получения информации основное внимание уделяется элементам аппаратного обеспечения, а на этапах сохранения, анализа и представления данных – программному обеспечению.

Основой используемого оборудования являются так называемые полевые комплекты, которые подразумевают их применение на месте расследования, но, конечно, могут использоваться и при лабораторной работе. Эти комплекты состоят из множества многоцелевых аппаратных средств: дупликатов, защит от записи, адаптеров для жестких дисков, кабелей, кабельных адаптеров, блоков питания и программного обеспечения, как обеспечивающего функционирование этих средств, так и использующего результаты услуг, предоставляемые этими средствами. Давайте рассмотрим отдельные компоненты подробно:

Forensic duplicator. Это устройство, делающее судебную копию долговременной памяти, дающее возможность аутентичного, «бит за битом» копирования. Система создаёт цифровой контрольный номер для сделанных копий, напр., по алгоритму MD5 или SHA-1 HASH, который гарантирует, что изменение даже одного бита копии станет обнаруживаемым, благодаря тому, что изменение даже одного бита приведёт к изменению перегенерированного контрольного номера. Важность копирования «бит за битом» становится ясным, если мы знаем, что удаление данных из компьютерных систем, в первую очередь, означает так называемое логическое удаление, то есть данные физически не удаляются, изменяется только статус ячеек памяти, они становится перезаписываемыми/допускающими изменения. При копировании «бит за битом» в дальнейшем (напр., в ходе лабораторного исследования) восстановление удалённых данных также станет возможным (с помощью программных средств). Характерной особенностью устройств является

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

количество копий, которое делается одновременно: 1:1, 1:2, или 1:3; типы интерфейсов со стороны исследуемого устройства: USB3/PATA,SATA, скорость передачи данных, достигающая 15 GB/s. Последняя характеристика играет важную роль в ходе уже упомянутого выше планировании временных затрат, необходимых для расследования на месте на основании ранее имеющихся или оценочных данных. Следует отметить, что эта операция может быть реализована также программным обеспечением компьютера, для этого требуется компьютер и так называемый софтвер для клонирования, но это решение требует значительно большего времени, чем копирование дупликатором.

Forensic bridges. Устройства защиты записи предназначены для изучения постоянных устройств хранения, имеющих различные интерфейсы (обычно HDD, SSD). Аппаратные устройства препятствуют записи данных на изучаемый диск, т.е. препятствуют удалению, модификации, и в конечном итоге потере аутентичности цифровых доказательств. Они как и дупликаторы имеют в своём распоряжении несколько типов входных и выходных интерфейсов, для использования которых требуется и компьютер (в отличие от дупликаторов), поэтому для выполнения работы требуется больше времени. Устройства, подходящие для типичных лабораторных исследований, обеспечивают экспертным компьютерам высокоскоростные интерфейсы USB3, или eSata, тогда как рассмотренные выше технические средства посредством использования PATA/SATA/SAS, Firewire, или USB-порта и адаптера могут иметь почти любые интерфейсы. Устройства защиты от записи, встроенные в компьютеры экспертов, могут достичь более высоких скоростей за счёт непосредственной связи с каналами передачи данных самих компьютеров.

Эти устройства появляются и в работе следственных органов, особенно в последние несколько лет, когда в отдельных случаях большое

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

количество данных передаётся экспертом следственным органам (приближается к терабайтной величине – ёмкость хранения информации прибл. к 200 стандартным DVD дискам) и самым целесообразным средством для сохранения этого большого количества данных является жёсткий диск. Изучение данных со стороны следственных органов производится таким образом, что доказательства в ходе этого процесса не изменяются, таким образом, в ближайшем будущем возрастёт роль устройств защиты от записи и в работе следователей.

Защита от записи может быть решена и с помощью программного обеспечения, однако в этом случае необходимо обеспечить (подтвердить, контролировать) 100 % способность блокирования записи посредством применяемого метода или программного обеспечения.

Adapters. Широкий спектр устройств, рассмотренных экспертами, требует от специалиста применения разнообразной аппаратуры. Использование адаптеров для выполнения упомянутых требований является наиболее эффективным способом с точки зрения экономии. Это такие преобразователи сигналов интерфейса данных и интерфейса питания, которые позволяют осуществить подключение к компьютеру эксперта специальных устройств, напр., жёсткого диска ноутбука 1,8” PATA (через устройства защиты от записи).

Программное обеспечение Forensic

Из-за широкого диапазона судебно-программного обеспечения и пространственных ограничений в последующем мы рассмотрим только основные категории. В числе первых необходимо выделить так называемые комплексные системы, управляющие делами, которые обеспечивают полную поддержку экспертной группы, начиная с извлечения данных, далее классификацию существенной информации по делу, и кончая её документированием. Системы управления делами в

тесной интеграции с уже упомянутыми средствами аппаратного обеспечения могут извлекать данные из различных устройств (планшетов, смартфонов, носителей информации и, и т.д.), а также сохранять их в стандартном формате и представлять в виде отчётов.

Некоторые свойства этих комплексных систем появляются и в качестве автономного программного обеспечения. Наиболее важные из них следующие:

Imager – извлечение данных из какого-либо устройства длительного хранения;

Data Recovery – восстановление данных (восстановление удалённых данных);

Emai Recovery/Converter – восстановление базы данных электронной почты, извлечение сохранённых сообщений;

Mobile Forensic – сохранение и восстановление данных смартфонов и традиционных мобильных устройств;

Password Tools – приложения для взлома паролей.

Кроме того, мы могли бы перечислить многие подразделы программного обеспечения, которые являются частью комплекта ИТ-устройств эксперта.

Как видно из сказанного, совокупность инструментов судебно-информатического эксперта является чрезвычайно сложным, как в плане аппаратного, так и в плане программного обеспечения, кроме того он должен соответствовать требованиям, перечисленным в разделе о методологии. Это не простая задача, учитывая, что значительная часть технических средств производится вне Европейского Союза и их покупка связана со значительными расходами.

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

6. Заключение

Систематизация методологического и инструментально-системного аспектов деятельности судебно-информатического эксперта является актуальной задачей не только для экспертов, но также и для руководящих лиц, ответственных за определение параметров упомянутой системы. В то время эксперты занимаются вопросами признания методологических стандартов в отечественной практике, т.е.:

– приобретение и признание стандартов (Отделение Компьютерных технологий Палаты Судебных Экспертов Венгрии);

– профессиональная переподготовка: руководящие органы должны найти ответы на вопросы, касающиеся карьеры экспертов, а именно:

– урегулирование финансового вопроса судебных ИТ-экспертов,

– субсидирование для поддержки высокого уровня парка технических средств, используемого экспертами (хардвер, софтвер) (поддержка в использовании law enforcement льгот),

– формирование навыков и техническое подготовка организаций, использующих результаты экспертиз, для анализа и оценки цифровых доказательств.

Это основные проблемы, а предлагаемые решения, (см. выше) в полной мере влияют на качество и удобство использования заключений судебных ИТ-экспертов, связанных с расследованием уголовных дел, как со стороны экспертов, так и со стороны следственных органов [7].

Ссылки

[1] Мате Иштван Жолт: Digital Forensic Science – работа по стандартизации «давно» и сегодня. В.: ISZAK2013 в трудах конференций

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

CD-ROM, Будапешт, Палата судебных экспертов Будапешта, 2013. 1.p. ISBN: 978-963-08-7882-1.

[2] Феньвеши Чаба: Основные вопросы криминалистики: В.: Гаал Дьюла, Хауцингер Золтан (ред.): Научные публикации о пограничной службе 14, Печ: Венгерское Общество Военной Науки, Венгерское Отделение Пограничного Управления, 2013. стр. 341-349.

[3] Закон XLVII от 2005 года «О деятельности судебного эксперта».

[4] PALMER, G. (ed.) (2001). A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, 7–8 August 2001. DFRWS Technical Report DTR-T001-01, 6 November 2001.

[5] ISO/IEC 27037:2012(E) Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. First edition 2012-10-15

[6] 11/2003. (V. 8.) IM-BM-PM Коллективное распоряжение о правилах изъятия, далее ведения, регистрации, предварительной продажи и ликвидации изъятых вещей в ходе уголовного процесса, и также о проведении конфискации.

[7] Мате Иштван Жолт: Цифровые доказательства. В.: Тёрё Чаба; Червак Чаба; Риксер Адам; Фабиан Ференц; Мишколци Боднар Петер; Дереш Петронелла; Госпожа Тренченьи Домокош Андреа.(ред.). Всевенгерская профессиональная встреча юристов докторантов 2013. Место и время встречи: Будапешт, Венгрия. 24 ноября 2013 года, Будапешт: Реформатский Университет им. Гашпар Кароли 2014 стр. 86-94. (Право и государтство; 2009) (ISBN:978-963-9808-56-0).

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.

Мате И. Ж.

Судебный ИТ-эксперт – методы и инструменты в уголовном деле

В ходе выполнения своей работы судебный ИТ-эксперт использует специальные средства аппаратного и программного обеспечений, руководствуясь такими методиками, понимание, оценка и доказательство соответствия (валидация) которых, обычно превышают уровень знания участников отечественного уголовного процесса в области ИТ-технологий. Это жесткое заявление также означает, что участники уголовного процесса находятся в зависимости от судебных ИТ-экспертов, а с другой стороны на эксперта ложится огромное бремя ответственности, не соответствующее его должностным обязанностям. В настоящей статье автор рассматривает сложившуюся ситуацию, предлагая те ключевые моменты и методы, посредством которых работа судебного ИТ-эксперта станет более проверяемой, то есть, увеличится гарантия качества его труда.

Ключевые слова: уголовный процесс, судебный ИТ-эксперт, доказывание.

Computer systems are most complicated digital evidences. Computer forensics experts need to help investigators because digital evidences are volatile and changeable. This paper presents forensic expert's methods and best practices during prequisition.

Key words: penal procedure, forensic IT expert, perquisition.

▪ Судебный ИТ-эксперт – методы и инструменты в уголовном деле / И. Ж. Мате // Часопис Національного університету «Острозька академія». Серія «Право». – 2016. – № 1(13) : [Електронний ресурс]. – Режим доступу : http://lj.oa.edu.ua/articles/2016/n1/16mizvud.pdf.