



7. Зверев Е.А. К вопросу о месте международных договоров в системе источников права Украины / Е.А. Зверев // Правовая жизнь современной Украины : матер. между нар. наук. конф. – О. Феникс, 2010. – С. 108–110.

8. О международных договорах Украины»: Закон Украины по состоянию на 12 декабря 2013 [Электронный ресурс]. – Режим доступа : <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?Nreg=1906-15>.

9. Епур Г.В. Внедрение международных документов в уголовное законодательство Украины : дис ... Канд. юрид. наук : 12.00.08 / Епур Григорий Владимирович. – М., 2005. – 195 с.

10. Конвенция Совета Европы о передаче производства по уголовным делам : по состоянию на 22 сентября 1995 [Электронный ресурс]. – Режим доступа : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_008.

11. Конвенция Совета Европы о международной действительности уголовных приговоров : по состоянию на 26 сентября 2002 [Электронный ресурс]. – Режим доступа : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_341.

12. Конвенция Совета Европы о передаче осужденных лиц : по состоянию на 18 декабря 1997 [Электронный ресурс]. – Режим доступа : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?Nreg=994_025.

13. Филатов В.М. Практика применения судами международных договоров Украины о признании и исполнении приговоров иностранных судов / В.М. Филатов, С.П. Бортновская. [Электронный ресурс]. – Режим доступа : <http://sudpraktika.in.ua/praktikazastosuvannya-sudami-mizhnarodnix-dogovoriv-ukraini-shhodo-viznannya-i-vikonannya-virokiv-inozemnix-sudiv>.

14. Трунцевский Ю.В. Нормы международного права как источник российского уголовного права : автореф. дис. на соискание ученой степени канд. юрид. наук: спец. 12.00.08 / Ю.В. Трунцевский. – Рязань, 1995. – 25 с.

15. Попович В.П. Имплементация норм международного уголовного права в уголовное законодательство Украины : автореф. дис. на соискание ученой степени канд. юрид. наук: 12.00.08 / В.П. Попович. – Львов, 2010. – 20 с.

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ИССЛЕДОВАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ В СУДЕБНОМ ЗАСЕДАНИИ

Валентин МУРАДОВ,

ассистент кафедры уголовного процесса и криминалистики
юридического факультета
Львовского национального университета имени Ивана Франко

Summary

In this article several issues of the scientific and technical progress, its applying in criminalistics and analyzing of special kinds of evidence are analyzed. Distinct features of fixation, analysis and use of a special kind of evidence, the electronic evidence are singled out. The peculiarities of such using while court hearings are highlighted. For the proper comprehension of the whole evidence and therefore increasing of digital evidence analysis effectiveness one can offer the usage of special technico-criminalistic means. Besides that it is necessary to take into account the ability of analyzing evidence from Internet straight at the court room.

Key words: information technology, electronic evidence, the research process, the electronic document file structure

Аннотация

В статье анализируется уровень научно-технического прогресса, его взаимодействие с криминалистикой в целом, а также в сфере исследования доказательств особенного вида в частности. Выделяются особенности фиксации, исследования и использования специфического вида доказательств – электронных. Подчеркиваются некоторые элементы такого использования во время судебных заседаний по уголовным делам. Предлагается увеличить эффективность исследования электронных доказательств в суде путём использования специальных технико-криминалистических средств для надлежащего восприятия всех составляющих элементов доказательственной информации. Также учитывается возможность исследования доказательственной информации в глобальной сети Интернет путём непосредственного анализа в зале судебного заседания.

Ключевые слова: информационные технологии, электронные доказательства, процесс исследования, электронный документ, файловая структура.

Постановка проблемы. Информационно-коммуникационные технологии на данном этапе своего развития представляют сложную развитую систему, которая тесно связана со многими сферами жизнедеятельности. Тяжело переоценить их огромное влияние на эффективность и результативность деятельности в разных отраслях общественной жизни. Но вместе с позитивными результатами такого явления можно также констатировать определённые негативные последствия. Например, упрощение и облегчение процессов, связанных с совершением уголовных правонарушений, уничтожением или маскировкой следов преступлений. Как известно, именно для криминалистики как науки основной задачей и первостепенным объектом является преступная деятельность как основа, которая обуславливает содержание деятельности относительно судопроизводства [9 с. 12]. Соответственно, сам процесс такой

деятельности, реализовываясь в объективной действительности, оставляет следы (материальные и нематериальные), которые содержат информацию о самом правонарушении, его участниках и последствиях. В результате криминалистической деятельности такие следы приобретают процессуальный статус доказательств. Всё чаще приходится наблюдать особенную сущность таких следов, а именно их специфическую природу. Это обуславливается спецификой использования современных средств связи, хранения информации, функционирования многих систем обработки данных в разнообразных сферах деятельности (от обычных игр до финансовых операций). Такие следы могут обрести достаточно специфический статус – статус электронных доказательств.

Изложение основного материала. Информационные технологии процессуального доказывания представляют собой новое направление научно-прак-



тической деятельности, возникшее в условиях информационного общества на стыке правовых и естественно-технических наук. Оно призвано обеспечить эффективность правосудия путем включения в процедуру его осуществления наиболее эффективных современных информационных технологий и приближения обоснованности правовых решений к уровню точных наук [1, с. 1]. В поддержку этого можно привести позицию К.Б. Калиновского и Т.Ю. Маркеловой: «Электронная информация стала широко использоваться во всех областях человеческой жизни, в том числе и криминальной. Не только преступления в сфере компьютерной информации (предусмотренные ст. 272-274 УК РФ) (а в УК Украины соответственно ст. 361-363-1 *авт. В.М.*), но и многие «традиционные» общественно-опасные деяния оставляют после себя электронные следы в компьютерных сетях, на магнитных или оптических носителях, экранах мониторов. В связи с этим возникает практическая проблема использования данных следов в процессе расследования и рассмотрения уголовного дела» [8, с. 18].

Криминалистика является наукой, которая использует данные других наук для решения собственных задач: расследования, раскрытия и предупреждения преступлений, и среди этого необходимо выделить такой важный аспект, как собирание и исследование различных видов доказательств. Рекомендации относительно такой деятельности значительно упрощают их поиск и фиксацию, а также повышают эффективность их исследования в будущем. Однако относительно такого особенного вида доказательств, как «электронные», такие рекомендации в достаточной мере не разработаны. По нашему мнению, в этом случае невозможно обойтись без данных ИТ (от англ. Information Technology), то есть широкого класса дисциплин и областей деятельности, относящихся к технологиям создания, сохранения, управления и обработки данных, в том числе с применением вычислительной техники (последнее время под информационными технологиями чаще всего понимают компьютерные технологии) [7]. Одной из попыток интегрировать эти науки есть создание частной криминалистической теории, которая

получила наименование «Форензика – компьютерная криминалистика» [12]. Небезосновательным является её разделение некоторыми авторами на непосредственно компьютерную криминалистику (computer forensics) и сетевую криминалистику (network forensics) [12, с. 11]. Анализ существующей в мире практики свидетельствует о том, что большинство преступлений, где электронные доказательства были привлечены в процесс расследования – это преступления в сфере экономики. Но такие случаи не единичны при расследовании и других видов преступлений [10]. Ситуацию можно назвать закономерной: уровень так называемой «технизации» общества постоянно растёт, отсюда и новые вызовы, в частности и для криминалистики. В криминалистической литературе можно найти позиции лишь относительно электронных доказательств-документов, однако есть все основания выделять ещё одну категорию – вещественные электронные доказательства. Ими могут быть орудия и средства совершения преступлений, предусмотренные соответствующими статьями Уголовного кодекса в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей. Конкретными орудиями в таком случае выступают так называемые «вредоносные программные средства», которыми могут быть компьютерные вирусы; программы, предназначенные для нейтрализации паролей, иных средств защиты компьютерных программ или компьютерной информации от несанкционированного доступа; программы-шпионы. Для исследования таких доказательств должны быть использованы особые методы и средства, которые позволят не только продемонстрировать сущность такого доказательства, его внутреннюю структуру, взаимосвязь составляющих элементов, способы существования и распространения, но и уровень опасности такого доказательства, реальный риск последствий его использования и степень причинённого ущерба.

Для полного понимания процесса исследования таких доказательств в судебном рассмотрении уголовных дел рассмотрим процесс размещения информации в сети Интернет и её последующее использование. Для начала такая информация должна быть преоб-

разована в особый формат, который позволит её размещение и распространение в сети. Общепринятым форматом текстовой информации в сети Интернет является язык программирования HTML (Hyper Text Markup Language – язык гипертекстового представления документов). После переформатирования она размещается на специальных компьютерных системах – носителях информации. Это постоянно включённые компьютеры, которые подсоединены к сети Интернет – серверы. Каждый из них имеет определённый адрес, который предоставляется доменным именем и IP-идентификатором (соответственно текстовый код-адрес и цифровой идентифицирующий код в виде четырёх чисел, записанных через точки). А информация, которая хранится на серверах, тоже имеет свой уникальный адрес, который существует в виде ссылки (URL – uniform resource locator). Информация в виде набора файлов, размещённых по определённому адресу и специальными программными средствами, сориентированными на аудиовизуальное ознакомление с ней (браузерами на компьютерах пользователей) воспринимается и усваивается. Важным элементом процесса такого размещения представляется участие определённых посредников, так называемых провайдеров, которые предоставляют услуги телематических служб (предмет их деятельности – функция передачи информации специальными каналами). В свою очередь такие собственники информационных систем предоставляют физическим и юридическим лицам возможность создать, разместить и обеспечить публичный доступ к информационным ресурсам. Но результат, который мы наблюдаем при просмотре и (-или) прослушивании такой информации при помощи интернет-браузеров (страницы с текстом, фото-, видео-, аудиоинформацией), фактически является визуальным образом набора компьютерных файлов. При подаче такого рода доказательств (а именно особых электронных документов) возникает вопрос, что именно необходимо подавать суду: отображение, которое воспринимается во время просмотра интернет-страниц, или набор отдельных файлов, которые являются полноценной информационной структурой.



Этот вопрос требует определённого уточнения. Понятие «документ» с позиции законодательства и практики Украины трактуется по-разному. Только в государственных стандартах зафиксировано, по меньшей мере, три таких дефиниции. А именно: документ – записанная информация, которая может рассматриваться как единица во время осуществления информационной деятельности [3, с. 12]. Также документ может идентифицироваться как материальный объект с информацией, закреплённой при помощи созданного человеком способа для её передачи во времени и пространстве [5, с. 2]. Другой акт определяет документ как информацию, зафиксированную на материальном носителе, основной функцией которого является её хранение, передача во времени и пространстве [4, с. 2]. В УПК Украины в статье 99 определение документа в контексте источников доказательств преподносится так: специально созданный с целью хранения информации материальный объект, который содержит зафиксированные (с помощью письменных знаков, звука, изображения) ведомости, которые могут быть использованы как доказательства факта или обстоятельств, которые устанавливаются во время уголовного производства. К документам, при условии наличия в них ведомостей, предусмотренных частью первой этой статьи, могут принадлежать: материалы фотосъёмки, звукозаписи, видеозаписи и иные носители информации (в том числе электронные); материалы, полученные путём осуществления во время уголовного производства мероприятий, предусмотренных действующими международными договорами, согласие на обязательность которых предоставлено Верховной Радой Украины; составленные в порядке, предусмотренном в УПК, протоколы процессуальных действий и приложения к ним, а также носители информации, на которых с помощью технических средств зафиксированы процессуальные действия; выводы ревизий и акты проверок.

На международном уровне признано определение документа как записанной информации, которая может быть использована как единица в документационном процессе. Такое определение разработано и утверждено Международной организацией по стандартиза-

ции (ISO) при участии Международной федерации библиотечных ассоциаций, Международной федерации по документации, Международного совета архивов, Международной организации по интеллектуальной собственности. Согласно стандарту ISO, информация может быть записана любым способом фиксации ведомостей при помощи не только знаков письма, но и изображения, звука и т. д. Такое определение позволяет отнести к документам все материальные объекты, которые могут быть использованы для передачи информации в обществе [2].

Следовательно, существует две основные точки зрения относительно сущности документа: это либо материальный носитель с информацией, либо информация сама по себе. Представляется, что правильное отождествление документа именно с информацией, а не только лишь с его носителем. Если, например, информация была передана при помощи голоса, потом переформатирована в текстовую форму или записана в форме фонограммы, содержание она не изменяется – изменяется лишь её носитель. Исследование такого доказательства как процесс непосредственного восприятия и анализа должно проводиться относительно информации, зафиксированной в нём, а это невозможно без использования необходимых для этого технико-криминалистических средств. Исследование только лишь носителя не даст желаемого результата (не представляется эффективным лишь внешний осмотр, скажем, компакт-диска с данными, необходимо подобрать соответствующие технические и программные элементы для декодирования именно информационного наполнения такого доказательства). Центральное место в исследовании таких доказательств занимает информация, восприятие которой и будет результатом исследования документа, его сущностью.

Но сам документ может существовать не только в привычной для нас материальной плоскости, но и в закодированном состоянии, находясь на различных технических носителях. Этот документ может приобрести статус электронного. Определение «электронный» можно обобщить по таким признакам: подача информации в цифровом виде (текст, звук, статическое или

движимое изображение в цифровых форматах), необходимость программных и аппаратных средств для её восприятия человеком (то есть компьютерного оборудования и программного обеспечения), необходимость телекоммуникационных средств для получения и распространения информации [11, с. 17].

Этот документ определяется государственными стандартами как документ, который создают и используют только в рамках компьютерной сети. А согласно ст. 5 Закона Украины «Про электронные документы и документооборот» (Закон України від 22 травня 2003 р. № 851-IV) электронным документом является документ, информация в котором зафиксирована в виде электронных данных, включая обязательные реквизиты документа. Реквизиты электронного документа должны размещаться в соответствии с действующими нормативными документами и стандартами. Так, законодатель существенно сузил это понятие.

В соответствии с ДСТУ 4163-2003 таких обязательных реквизитов пять: наименование организации-создателя документа; местонахождение организации-создателя документа (или почтовый адрес); наименование документа; дата изготовления документа; код изготовителя документа или утвердившего его лица [6].

Информация из таких источников, как сети (как локальные, так и глобальные), файловые системы, протоколы работы систем и подсистем, log файлы (файлы с записью внешних событий или протоколирование работы самой программы-источника записей в хронологическом порядке), сервисы хранения информации в сети Интернет (SkyDrive, Adrive, Box.net, Clip2Net, DropBoks, MediaMax и др.), электронные почтовые ящики, системы интернет-банкинга и т. д., фактически доминирует при использовании и обработке. Значительная часть такой информации не подпадает под понятие «электронный документ» из-за отсутствия необходимых реквизитов. Возникает вопрос о том, как представлять эти документы в суде. Оригиналом документа является сам документ из первоисточника, а оригиналом электронного документа – его отображение. Но что тогда считать таким отображением?



Возвращаясь к вопросу о том, что именно необходимо предоставлять суду: отображения, которые воспринимаются во время просмотра интернет-страниц (иных электронных документов посредством специальных технических и программных продуктов), или же набор отдельных файлов, которые представляют собой полноценную информационную структуру. Полагаем, выбор необходимо сделать в пользу именно полноценной файловой структуры, а в случаях сложности или невозможности этого – обращая внимание на внешний вид документа вместе с информацией из места его хранения с записью внешних событий или протоколирования работы самой программы-источника записей в хронологическом порядке. Такой способ даст возможность отследить определённые изменения, которым подверглась информация полностью или частично. В случае ограничения исследования подобной информации лишь ознакомлением с внешней структурой в форме отображения на экране или мониторе при просмотре интернет-страниц (иных электронных документов), не удастся обнаружить изменения, которые могли вноситься в её структуру в течение определённого времени.

Такой способ исследования представляется наиболее адекватным по отношению к характеру и особенностям данного рода доказательств. Для этого в контексте технико-криминалистического обеспечения такого исследования необходимо уделить внимание таким элементам, как средства, приёмы и субъекты использования.

Чтобы на должном уровне проводить такое исследование в суде необходимы средства компьютерной техники (с характеристиками не ниже чем частота процессора 3.2 ГГц / RAM 4 ГБ / HDD 500 ГБ / Intel HD Graphics / DVD+/-RW) и определёнными портами и приложениями. Интегрированные мониторы в количестве не менее четырёх (которые будут непосредственно передавать изображение и сопутствующую информацию суду, сторонам, а также присутствующим) соответствующих размеров и разрешением не ниже 1920 x 1080 точек. Также на соответствующем уровне должно быть представлено и специальное программное обеспечение (включая операционную,

антивирусную и программную составляющие). Особое внимание следует обратить также на лицензионность таких средств, поскольку из-за отсутствия этой составляющей возникает опасность изменения сущности доказательственной информации или её полного уничтожения. Также для оперативного доступа к требуемой информации необходимым элементом выступает канал передачи данных сети Интернет со скоростью такой передачи не ниже 5 Мбит/с. Следует также учитывать опасность постоянного подключения указанного комплекса средств к такому каналу, поскольку в этом случае также возможно умышленное уничтожение или повреждение доказательственной информации путём проникновения извне, использования вредоносного программного обеспечения. Такое подключение следует осуществлять лишь только в случае возникновения необходимости, а также с учётом требований информационной безопасности.

Выводы. Необходимым субъектом такого исследования можно назвать специалиста, который будет принимать участие в этом процессе, сфера специальных знаний которого позволяет адекватно исследовать конкретную информационную модель. Такой специалист должен учитывать в своей работе специфику сути конкретного исследования, требования непосредственного места и вспомогательных средств его проведения.

Необходимо отметить, что процедура исследования электронных доказательств в судебном заседании по уголовному делу требует существенного совершенствования в указанных направлениях, а также дальнейшего развития и наращивания эффективности.

Список использованной литературы:

1. Вещественные доказательства: Информационные технологии процессуального доказывания / Под общ. ред. д. ю. н., проф. В.Я. Колдина. – М. : Издательство НОРМА, 2002.
2. Документ. [Электронный ресурс]. – Режим доступа : <http://uk.wikipedia.org/wiki/Документ>.
3. ДСТУ 2392-94. Інформація та документація. Базові поняття. Терміни та визначення. Затверджено і введено в

дію наказом Держстандарту України № 68 від 29 березня 1994. – К. : Держстандарт України, 1994.

4. ДСТУ 2732:2004. Діловодство й архівна справа. Терміни та визначення понять. Прийнято та надано чинності : наказ Держспоживстандарту України від 28 травня 2004 р. № 97. – К. : Держспоживстандарт України 2005.

5. ДСТУ 3017-95. Видання. Основні види. Терміни та визначення. Затверджено і введено в дію наказом Держстандарту України № 58 від 23 лютого 1995 р. Чинний від 01.01.96. – К. : Держстандарт України, 1996.

6. ДСТУ 4163-2003. Державна уніфікована система документації. Вимоги до оформлення документів. Затверджено наказом Держспоживстандарту України від 7 квітня 2003 р. № 55. Надано чинності 01.09.2003 – К. : Держспоживстандарт України 2004.

7. Информационные технологии. Википедия [Электронный ресурс]. – Режим доступа : http://ru.wikipedia.org/wiki/Информационные_технологии.

8. Калиновский К.Б., Маркелова Т.Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. 2001. № 6.

9. Когутич І.І. Криміналістика: Курс лекцій. – К. : Атіка, 2008.

10. Котляревський О.І., Киценко Д.М. Комп'ютерна інформація як речовий доказ у кримінальній справі. [Електронний ресурс]. – Режим доступу : <http://www.bezpeka.com/ru/lib/spec/crim/art70.html>.

11. Палеха Ю.І., Леміш Н.О. Загальне документознавство. – К., Ліра-К, 2009.

12. Федотов Н.Н. Форензика – компьютерная криминалистика – М. : Юридический Мир, 2007.