УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА

УДК 343.14

К ВОПРОСУ ОБ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВАХ В УГОЛОВНОМ ПРОЦЕССЕ УКРАИНЫ

Наталья АХТЫРСКАЯ,
кандидат юридических наук, доцент,
главный научный сотрудник отдела научно-методического обеспечения деятельности
Высшей квалификационной комиссии судей Украины и Высшего совета юстиции
Национальной школы судей Украины

SUMMARY

On the basis of analysis of current criminal-procedure legislation of Ukraine and international obligations in the field of fight with cybercrime there is a suggestion at standardization concepts "Electronic proofs", sources of their receipt, determination under investigation of cybercrime to the National center of fight with cybercrimes of Ukraine.

Key words: electronic proofs, computer information, information about informative streams, international cooperation.

АННОТАЦИЯ

На основании анализа действующего уголовно-процессуального законодательства Украины и международных обязательств в сфере борьбы с киберпреступностью вносится предложение об унормировании понятия «электронные доказательства», источников их получения, определении подследственности киберпреступлений Национальному центру борьбы с киберпреступностью Украины.

Ключевые слова: электронные доказательства, компьютерные данные, данные об информационных потоках, международное сотрудничество.

Постановка проблемы. По мнению С. Джобса, только инновация отличает лидера от догоняющего [3]. Научно-технический прогресс проникает во все сферы человеческой деятельности, в том числе и сферу уголовного судопроизводства. Современные средства, методы, специальные знания всегда тщательно исследовались криминалистами на предмет возможного использования их для обнаружения и фиксации доказательств. Г. Гросс классифицировал доказательства на «формальные» и «универсальные», или «неподкупные». Под первыми он понимал показания свидетелей, по которым можно получить лишь «формальную» истину, отмечая: «Злая воля и обман, ошибки и заблуждения, а чаще всего собственные выводы свидетеля и его уверенность, что он говорит лишь о том, что видел и слышал, влияют столь бесконечно много, что мы лишь в самых редких случаях можем признать показание свидетеля объективным, абсолютно правильным и ни в какой мере не внушенным». Предмет изучения криминалистики Г. Гросс определяет так: «Каким способом мы можем изыскать те или другие доказательства, как дойти до них, как их охранить и как их использовать – все это настолько же важно, как важен и тот результат, которого мы достигаем отправлением правосудия. Найденные и использованные следы преступника, аккуратно составленный чертеж, хотя бы и несложный, какой-нибудь микроскопический препарат, расшифрованная переписка, фотографические снимки, татуировка, восстановленное обуглившееся письмо, какое-нибудь точное измерение и тысячи подобных реальностей – не что иное, как неподкупные свидетели, не допускающие опровержения, и в то же время допускающие постоянную проверку, свидетели, в отношении которых исключается возможность ошибки, одностороннее понимание, злая воля, клевета и подобное. С каждым успехом криминалистики <…> повышается значение универсальных доказательств» [2].

В 1898 г. в предисловии к третьему изданию книги «Руководство для судебных следователей как система криминалистики» Г. Гросс предвидел: «Криминалистика, еще столь молодая наука, не может предсказать, к каким конечным итогам она непременно должна привести, но ей известно, что эти будущие изменения также не останутся постоянными, что постоянство вообще никогда не будет достигнуто, что единственно вечным будет состояние беспрерывного движения» [2].

В соответствии со ст. 22 Соглашения об ассоциации Украины с Европейским Союзом стороны договорились, в частности, бороться с киберпреступностью (п. «f» ч. 2) [10]. Для этого в Украине создана правовая база построения информационного общества – приняты законы Украины «Об Основных принципах развития информационного общества в Украине на 2007–2015 гг.», «Об информации», «О доступе к публичной информации», «О защите персональных данных», «О защите информации в информационно-телекоммуникационных системах», «Об электронной цифровой подписи», которые регулируют общественные отношения в сфере создания информационных электронных ресурсов, защиту интеллектуальной собственности, внедрение электронного документооборота.

В современных условиях компьютеризации одним из дискуссионных вопросов уголовного процесса и крими-

налистики является использование электронных доказательств как в национальном законодательстве, так и в сфере оказания международной правовой помощи.

Цель и задачи статьи. С учетом глобализации компьютерного пространства необходимо провести унификацию законодательства, регламентирующего расследование, оценку доказательств и международное сотрудничество при использовании электронных доказательств. Как справедливо отмечает А. Волеводз, практика международного сотрудничества в борьбе с преступностью свидетельствует, с одной стороны, о появлении и все более широком распространении преступлений в сфере компьютерной информации, а с другой – о возрастании роли новых методов получения доказательств и перспективности использования высоких технологий в этой деятельности [1, с. 9]. Для эффективной имплементации норм международного права в сфере борьбы с киберпреступностью целесообразно обосновать необходимость законодательного определения электронных доказательств, источников их формирования, допустимости международного сотрудничества путем обмена электронными доказательствами, целесообразность использования электронных способов направления запросов и ответов об их выполнении, возможность применения контрольной поставки информации для расследования транснациональных компьютерных преступлений.

Изложение основного материала исследования. В соответствии со ст. 84 Уголовного процессуального кодекса Украины (далее – УПК Украины) доказательствами являются фактические данные, полученные в установленном порядке, на основании которых следователь, прокурор, следственный судья и суд устанавливают наличие или отсутствие фактов и обстоятельств, имеющих значение для уголовного производства и подлежащих доказыванию. Процессуальными источниками доказательств являются показания, вещественные доказательства, документы, выводы экспертов. При этом документами признаются специально созданные с целью сохранения информации материальные объекты, содержащие зафиксированные с помощью письменных знаков, звука, изображения и так далее сведения, которые могут быть использованы как доказательство факта или обстоятельства, устанавливаемого в рамках уголовного судопроизводства (ст. 99 УПК Украины). В п. 1 ч. 2 ст. 99 УПК Украины содержится указание на то, что документами могут быть признаны материалы фотосъемки, звукозаписи, видеозаписи и иные носители информации, *в том числе электронные.* Несмотря на расширение сферы использования электронных документов, в том числе и при совершении преступлений, Уголовный процессуальный кодекс Украины, принятый в 2012 г., не содержит специального раздела, посвященного понятию, сбору, фиксации и оценке данного вида доказательств [6]. Законодатель ограничился лишь фрагментарным упоминанием об использовании такого вида доказательств. Так, одним из видов негласных следственных (розыскных) действий является вмешательство в частное общение, при этом его разновидностями являются аудио-, видеоконтроль лица, арест, осмотр и выемка корреспонденции, снятие информации с транспортных телекоммуникационных систем, *снятие информации с электронных информационных систем* (ч. 4 ст. 258 УПК Украины).

На законодательном уровне закреплено, что поиск, обнаружение и фиксация сведений, содержащихся в электронной информационной системе, или их частей, доступ к электронной информационной системе либо ее частей, а также получение таких сведений без ведома их собственника, владельца или держателя может осуществляться на основании определения следственного судьи при существовании сведений о наличии информации в *электронной системе* либо ее части, что имеет значение для определенного досудебного расследования. Не требуется разрешение следственного судьи на получение сведений из *электронных информационных систем*, доступ к которым не ограничивается их собственником, владельцем или держателем либо не связан с преодолением системы логической защиты. В определении следственного судьи дополнительно должны быть указаны идентификационные признаки *электронной информационной системы*, в которой может осуществляться вмешательство в частное общение (ст. 264 УПК Украины).

Согласно ч. 2 ст. 265 УПК Украины содержание информации, полученной вследствие снятия сведений с электронных информационных систем либо их частей, фиксируется на соответствующем носителе лицом, осуществляющим снятие, которое обязано обеспечить обработку, сохранение и передачу информации.

Исследование информации, полученной при применении технических средств, в случае необходимости осуществляется с участием специалистов. Технические средства, применявшиеся во время проведения негласных следственных (розыскных) действий, а также первичные носители полученной информации должны сохраняться до вступления приговора в законную силу. Указанные носители информации могут быть предметом исследования соответствующих специалистов или экспертов (ст. 266 УПК Украины).

Стоит отметить тот факт, что с помощью компьютерных технологий может быть совершено множество преступлений (угроза террористического акта, изготовление порнографической продукции, финансовые преступления и другие), а это обуславливает необходимость проводить осмотр компьютерной техники, обыск, что сопровождается специфической процедурой фиксации и изъятия, исследования электронных доказательств. Отсутствие четкого законодательного закрепления понятия электронных доказательств, их видов, источников, допустимости приводит к низкому уровню раскрываемости отдельных видов преступлений, к непризнанию их в суде. В частности, кибератаки представляют серьезную угрозу банковской системе Украины. Однако официальные данные Государственной судебной администрации Украины свидетельствуют, что до судов с обвинительными актами доходит незначительное количество уголовных производств. Так, в 2014 г. за преступления в сфере использования электронно-вычислительных машин (компьютеров), компьютерных систем и систем электросвязи в судах Украины рассмотрено 51 уголовное производство в отношении 87 лиц; обвинительные приговоры постановлены лишь по 35 уголовным производствам. По 3 делам утверждены соглашения о примирении, по 9 делам – о признании вины. 9 производств закрыто, 2 направлены на дополнительное расследование (согласно Уголовно-процессуальному кодексу Украины 1960 г.) [5]. В 2015 г. открыто уголовное производство в отношении председателя суда за вмешательство в электронный документооборот суда с целью нарушения автоматизированного порядка распределения дел между судьями, что свидетельствует об использовании электронных доказательств также относительно преступлений, связанных с коррупцией.

Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве) от 23.11.2001 г. (далее – Конвенция) определила содержание нескольких дефини-

ций: «компьютерные данные» – любое представление фактов, сведений или понятий в форме, пригодной для обработки с помощью компьютерных систем, в том числе программы, предназначенные для выполнения компьютерной системой определенных действий; «данные трафика» – любые компьютерные данные, связанные с операциями по передаче данных посредством компьютерной системы, которые созданы компьютерной системой, являвшейся звеном в цепочке передачи данных, и указывают на источник сообщения, его назначение, маршрут, время, дату, размер, длительность или тип лежащей в его основе услуги [4]. Следует отметить, что указанные определения не являются исчерпывающими. В данном случае украинский законодатель при формировании национального стандарта компьютерных доказательств сталкивается с релятивизмом, поскольку особенностью международных актов является лишь общее закрепление понятий, не ограничивающее законотворческую деятельность и особенность внутреннего права страны.

Подписанты Конвенции взяли на себя обязательства принять такие меры законодательного и иного характера, которые могут понадобиться для установления полномочий и процедур, предусмотренных в целях проведения определенных уголовных расследований или разбирательств, а именно: 1) к уголовным преступлениям, предусмотренным ст. ст. 2–11 Конвенции (незаконный доступ; незаконный перехват, вмешательство в данные, вмешательство в систему, ненадлежащее использование устройств; подлог компьютерных данных; компьютерное мошенничество, преступления, связанные с детской порнографией; преступления, связанные с нарушениями авторского права и смежных прав; покушение, пособничество и подстрекательство); 2) к другим уголовным преступлениям, совершенным посредством компьютерной системы; 3) к сбору доказательств по уголовному преступлению в электронной форме.

Согласно ст. 19 Конвенции каждая из сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам путем произведения обыска или сходным образом получать доступ на ее территории к компьютерной системе в целом или отдельной ее части, хранящимся там компьютерным данным, а также к носителю компьютерных данных, на котором могут храниться компьютерные данные. Эти меры должны включать в себя такие полномочия: а) по конфискации либо изъятию компьютерной системы или ее части, носителя компьютерных данных; б) по изготовлению и сохранению копии таких компьютерных данных; в) по поддержанию целостности соответствующих сохраненных компьютерных данных; г) по прекращению доступа к этим компьютерным данным в компьютерной системе, к которой получен доступ, или удалению их из этой системы.

Конвенция в ст. 20 предусматривает право сбора компьютерных данных в режиме реального времени. Каждая из сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить ее компетентным органам собирать или записывать (путем применения технических средств на территории данной стороны), а также принуждать поставщика услуг (в пределах имеющихся у него технических возможностей) собирать или записывать (путем применения технических средств на территории этой стороны) или сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные трафика, связанные с определенными операциями по передаче данных на ее территории, осуществляемыми посредством компьютерной системы.

Стоит отметить возможность перехвата данных содержания (ст. 21 Конвенции) в отношении ряда серьезных преступлений, определенных в соответствии с национальным законодательством, которые позволили бы компетентным органам собирать или записывать путем применения технических средств на территории этой стороны и принуждать поставщика услуг (в пределах имеющихся у него технических возможностей) собирать или записывать (путем применения технических средств на территории этой стороны) или сотрудничать с компетентными органами и помогать им собирать или записывать в режиме реального времени данные содержания определенных передач информации на территории государства, осуществляемых посредством компьютерной системы.

Особое внимание уделено вопросам юрисдикции, поскольку каждая из сторон должна принять такие меры законодательного и иного характера, которые могут понадобиться, чтобы установить юрисдикцию по любому из преступлений, предусмотренных ст. ст. 2–11 Конвенции, если оно совершено на ее территории, на борту судна под флагом данной стороны, на борту воздушного судна, зарегистрированного согласно законам данной стороны, или одним из подданных данной стороны, если правонарушение подпадает под действие уголовного законодательства на территории, где оно было совершено, или же если правонарушение совершено вне территориальной юрисдикции любого государства (ст. 20 Конвенции).

Согласно ст. 23 Конвенции в целях расследования или судебного преследования уголовных преступлений, связанных с компьютерными системами и данными, а также в целях сбора доказательств по уголовным преступлениям в электронной форме стороны должны осуществлять самое широкое сотрудничество друг с другом через применение соответствующих международных документов о международном сотрудничестве в деле борьбы с преступностью, договоренностей, достигнутых на основе единообразного или взаимообязывающего законодательства, а также национальных законов.

В Уголовном процессуальном кодексе Украины предусматривается, что в рамках международного сотрудничества запрос направляется почтой, а в неотложных случаях – электронным, факсимильным или иным способом. В таком случае оригинал запроса направляется почтой не позже трех дней с момента его передачи электронной почтой. Выполнение такого запроса осуществляется исключительно при условии подтверждения его оригиналом (ч. 4 ст. 548 Конвенции). Направление компетентному органу иностранного государства материалов выполнения запроса возможно лишь после получения украинской стороной оригинала запроса (ч. 5 ст. 548 Конвенции). Очевидным является закрепление в законе обязательности существования электронного и письменного запроса, что указывает на ограниченное правовое действие первого, заключающееся лишь в исполнении требований, но не обязывающее предоставить информацию другому государству. Прерогативой пользуется только письменный запрос, имеющий двухвекторную обязательность.

Существующий пробел в УПК Украины относительно электронных доказательств логично должен быть устранен принятием специального Закона Украины «О борьбе с киберпреступностью», проект которого содержит понятие киберпреследования, компьютерных данных, данных об информационных потоках и так далее [8]. Из анализа норм законопроекта усматривается отсутствие указаний

на источники электронных доказательств. В этой части проект надлежит дополнить нормой следующего содержания: «Источниками электронных доказательств являются электронные устройства: компьютеры и периферийные устройства, компьютерные сети, мобильные телефоны, цифровые камеры и другие портативные устройства, в том числе устройства для хранения информации, а также сеть Интернет. Информация из этих источников не имеет обособленной физической формы».

Электронные доказательства во многом сходны с традиционными, однако имеют они и ряд уникальных характеристик:

1) их не видно невооруженным глазом: извлечь их может только специалист;

2) они очень неустойчивые: на некоторых устройствах или в определенных обстоятельствах во время обычной эксплуатации устройства информация в его памяти (а значит, и доказательства, которые оно содержит) может изменяться. Например, при разрядке устройства или нехватке памяти система накладывает (записывает) новую информацию поверх старой. Компьютерная память может быть повреждена или уничтожена под воздействием физических факторов (большой влажности или высокой температуры) и электромагнитных полей;

3) они могут быть изменены или уничтожены в процессе обычной эксплуатации устройства: память компьютерных устройств постоянно изменяется по запросу пользователей («сохранить документ», «скопировать файл») либо операционной системы;

4) их можно копировать без потери качества: цифровые данные можно копировать неограниченное количество раз, и любая последующая копия ничем не будет отличаться от оригинала. Благодаря этой уникальной особенности разные специалисты могут параллельно и независимо друг от друга исследовать разные копии одного и того же электронного доказательства, не затрагивая при этом оригинал;

5) стремительная эволюция источников электронных доказательств: новые технологии появляются и развиваются с невероятной скоростью, поэтому методы и процедуры по работе с электронными доказательствами нужно постоянно пересматривать и обновлять [9].

Тщательная подготовка операций и следственных действий по сбору электронных доказательств охватывает решение некоторых вопросов. Во-первых, необходимо знать местонахождение данных (физическое размещение), поскольку не исключается нахождение оборудования в одном месте, а данных – в другом. Если не учитывать такую вероятность, то уже после прибытия на место может оказаться, что для последующих действий нужно разрешение компетентного органа (особенно если данные находятся в другой юрисдикции) или дополнительные технические навыки/оборудование.

Во-вторых, рекомендуется предварительно установить профессиональные навыки подозреваемого. Для этого необходимо собрать как можно больше информации о подозреваемом. Если он хорошо разбирается в компьютерных технологиях, то он может осуществить манипуляции, помогающие ему «замести следы» своих деяний или помешать изъятию оборудования и данных, например, поставить на устройство пароль или установить программу необратимого уничтожения ключевых данных. Нужно подготовиться к подобным ситуациям, то есть предпринять контрмеры. Подозреваемый может хранить данные в облачном хранилище или на других онлайн-ресурсах, и тогда на самом оборудовании не будет никакой информации.

В-третьих, следователь не должен игнорировать наличие альтернативных источников доказательств. Прежде чем приступать к любым действиям, которые предполагают прямой контакт с подозреваемым и выемку данных или оборудования, на подготовительном этапе нужно проверить, существуют ли другие, более предпочтительные источники той же информации. Например, для получения данных об электронном сообщении можно обратиться ко второй стороне – адресату сообщения либо третьей стороне – поставщику интернет-услуг или онлайн-услуг [9].

Следователь должен принять тактическое решение, где искать данные: у подозреваемого или у другого владельца этой же информации. В некоторых странах закон требует от компаний уведомлять клиентов о любых запросах на предоставление данных, а это может насторожить подозреваемого, он может спрятать или уничтожить доказательства. Лица, ведущие расследование, должны оценить, каким образом процедура истребования доказательств у третьих лиц может повлиять на его эффективность, особенно если данные хранятся на территории другого государства. Кроме того, важно определить оптимальный источник доказательств, который поможет получить наиболее важную информацию.

В процессе подготовки к обыску необходимо установить, какие устройства информации либо коммуникационное и сетевое оборудование могут быть обнаружены на месте обыска; кто отвечает за компьютерные устройства; сколько единиц оборудования может быть обнаружено; какой объем данных, которые нужно будет скопировать; существует ли резервная копия данных и на каком носителе она хранится.

Иногда в получении доказательств может помочь нотариус или аналогичный специалист. В романо-германских правовых системах одной из функций нотариуса является проверка и удостоверение подлинности определенных юридических документов и соглашений, которые предоставляются в качестве судебных доказательств. Нотариус может войти в Интернет через свой компьютер, осмотреть необходимые веб-сайты или страницы, после чего формально засвидетельствовать их подлинность. Что касается международного сотрудничества, то многие страны заключили соглашения о взаимном признании нотариально заверенных документов.

Конвенция предусматривает возможность трансграничного доступа к компьютерным данным, находящимся в системах общего доступа, либо при получении соответствующего разрешения (ст. 32). Любая из сторон имеет право, без согласия другой стороны, получать доступ к компьютерным данным из открытых источников, находящихся в системах общего доступа, независимо от территориального местонахождения этих данных; а также посредством компьютерной системы на своей территории получать доступ к компьютерным данным, расположенным на территории другой стороны, при получении правомерного и добровольного согласия со стороны лица, обладающего законным правом на предоставление данных этой стороне посредством вышеупомянутой компьютерной системы [4].

Несмотря на наличие конвенционных обязательств, национальное законодательство Украины и других стран не содержит прямую регламентацию их реализации. В законодательстве Украины этот вопрос не решен, поскольку международное сотрудничество в рамках уголовного производства должно осуществляться через уполномоченные на то органы. Примером попытки реализации права на получение правоохранительными органами информации от лица,

обладающего законным правом на предоставление данных другой страны, минуя направление запроса в центральный орган досудебного расследования, является опыт Бельгии в расследовании компьютерного мошенничества [7]. Так, на территории этой страны было совершено одномоментно несколько преступлений в сфере финансового мошенничества с использованием компьютерных систем. Определив общие признаки, прокуратура Бельгии объединила все эпизоды в одно производство на основании того, что все потерпевшие накануне «атаки» получали письма от незнакомца через систему «Yahoo». Поскольку Директорат «Yahoo» находится в Калифорнии, прокурор для ускорения получения IP-адресов подозреваемых направил электронный запрос непосредственно директорату, а не в прокуратуру США. Компания «Yahoo» отказалась выполнять запрос, направленный прокурором другой страны, что создало препятствия для эффективного расследования преступления. Суд Бельгии удовлетворил иск прокурора Бельгии к Директорату «Yahoo» о наложении штрафа за невыполнение предписания прокурора о предоставлении информации, имеющейся в распоряжении держателя, необходимой для производства в рамках уголовного преследования.

В законодательстве Украины в рамках международного сотрудничества предусматривается «контрольная поставка» (ст. 569 УПК Украины), но только в случае обнаружения контрабанды. По нашему мнению, этот метод необходимо распространить и при сборе электронных данных в случае обнаружения признаков подготовки к совершению хакерских атак, хаквитизма (преступлений, посягающих на конфиденциальность информации), деструктивных киберпреступлений из территории другого государства. Такой подход объясняется тем, что киберпространство – это смоделированное с помощью компьютера информационное пространство, в котором находятся данные о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символическом или ином виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям, или сведения, сохраняющиеся в памяти какого-либо физического или виртуального приспособления, а также иного носителя, специально предназначенного для их хранения, обработки и передачи, уникальная среда, не размещенная в географическом пространстве, но доступная каждому в любой точке мира с помощью доступа в Интернет.

Международными соглашениями предусмотрено создание специализированного органа по расследованию данной категории преступлений. На выполнение международных обязательств в проекте Закона Украины «О борьбе с киберпреступностью» определен статус Национального центра борьбы с киберпреступностью, который является государственным органом, подчиненным и подотчетным Министерству внутренних дел Украины, и должен быть создан на базе Управления борьбы с коррупцией.

Выводы. В контексте евроинтеграции Украины актуализируется проблема изучения опыта становления информационного общества в странах-членах Европейского Союза, а также имплементации норм правовых актов Европейского Союза в информационное законодательство Украины. В перечне приоритетов стратегического развития Украины особое место должны занимать защита прав, свобод и безопасности в информационной сфере, отказ от идей тотального информационного контроля. С этой целью необходимо в законодательстве определить понятие «электронное доказательство» как данные, подтверждающие факты, информацию либо концепцию в форме, приспособленной для обработки с помощью компьютерной системы, в том числе программы выполнения компьютерной системой тех или иных действий. Источниками электронных доказательств целесообразно признать электронные устройства: компьютеры и периферийные устройства, компьютерные сети, мобильные телефоны, цифровые камеры и другие портативные устройства, в том числе устройства для хранения информации, а также сеть Интернет. Информация из этих источников не имеет обособленной физической формы. В рамках международного сотрудничества необходимо интенсифицировать использование электронных способов передачи запрашиваемой информации, а не только направления запросов. По мнению А.-Л. Шатлен, существует социальный запрос на создание нового направления в сфере выявления, фиксации, исследования электронных доказательств – цифровой криминалистики, занимающейся обработкой электронных доказательств для их законного использования в суде [11].

Список использованной литературы:

1. Волеводз А. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.
2. Гросс Г. Руководство для судебных следователей как система криминалистики / Г. Гросс. – М. : ЛексЭст, 2002. – 1088 с.
3. Джобс С. Афоризмы, цитаты, высказывания / С. Джобс [Электронный ресурс]. – Режим доступа : http://aphorism-citation.ru/index/0-783.
4. Европейская Конвенция по киберпреступлениям (преступлениям в киберпространстве) от 23.11.2001 г. [Электронный ресурс]. – Режим доступа : http://conventions.coe.int/Treaty/RUS/Treaties/Html/185.htm.
5. Форма № 1 «Звіт судів першої інстанції про розгляд справ у порядку кримінального судочинства»; форма № 1-1 «Звіт судів першої інстанції про розгляд матеріалів кримінального провадження» : звіти Державної судової адміністрації України за 2015 р. [Электронный ресурс]. – Режим доступа : http://ks.zt.court.gov.ua.
6. Кримінальний процесуальний кодекс України від 13.04.2012 р. // Офіційний вісник України. – 2012. – № 37.
7. Материалы семинара для председателей судов общей юрисдикции «Особенности оценки доказательств по делам, связанным с использованием компьютерных технологий» (г. Киев, 16 февраля 2011 г.). – К., 2011.
8. Про боротьбу з кіберзлочинністю : проект Закону України [Электронный ресурс]. – Режим доступа : http://rada.gov.ua.
9. Руководство по работе с электронными доказательствами для сотрудников полиции, прокуратуры и судов. Отдел по защите данных и борьбе с компьютерными преступлениями / Генеральный директорат по правам человека и верховенству права. – Страсбург, 2014.
10. Угода про асоціацію України з Європейським Союзом від 27.06.2014 р. : ратифікована Законом України від 16.09.2014 р. [Электронный ресурс]. – Режим доступа : http://eeas.europa.eu/delegations/ukraine/eu_ukraine/association_agreement/index_uk.htm.
11. Шатлен А.-Л. Висновок БДІПЛ/ОБСЄ щодо проекту Закону України «Про боротьбу з кіберзлочинністю» (2014 р.) та дотримання стандартів прав людини під час розробки законодавства, пов'язаного з кіберзлочинністю / А.-Л. Шатлен // Матеріали Комітету з інформаційної політики Верховної Ради України. – 2015. – 26 березня.