Ключевые слова: *киберпреступность, борьба с киберпреступностью, подразделения по борьбе с киберпреступностью, подготовка кадров, Департамент по борьбе с киберпреступностью, МВД Украины.*

LITVINOV M. Y. THE WORLD AND UKRAINIAN PRACTICE OF COMBATING CYBERCRIME

The world economic processes at the present stage are increasingly shifting in the direction of cyberspace because of its use as a tool of doing business allows you to significantly increase profits. However, you can also observe the criminal elements shift in the direction of this virtual environment. So, today in almost any crime mentioned in Criminal Code of Ukraine, can be committed out with the use of cyberspace.

Assessment of the crime situation in the Cyber sphere gives ground to take decisive action on the part of law enforcement officers for the purpose of its improvement, reduction of risk for ordinary citizens to fall into the trap of cybercriminals.

The main peculiarity of the fight against cybercrime is that the state alone is not in a position to confront the phenomenon itself. Only international community in permanent close cooperation can deal with such issue as a security threat of cybercrime.

The real threat for as ordinary people security as well of security for government structures made many countries of the world to adopt a number of regulations aimed at prevention and punishment of cybercrime.

In this article the world approaches in organizing of cybercrime prevention have been analyzed.

In Ministry of Internal Affairs of Ukraine the function of combating cybercrime is performed by Department of Cybercrime Combating. Currently, the Department established constructive cooperation with other countries' law enforcement agencies in combating cybercrime.

In the article the examples of legal documents in cybercrime combating are provided and relative Ukraine legislation are presented.

The main task for the Department today is the exchange of achievements; continuous learning and professional development; use the experience of international experts; the development of virtual communities, which at the informal level contribute to combating cybercrime.

Another important direction of Department activity is the personnel training. The article deals with problems that exist in the training of personnel for units to combat cybercrime.

Based on the analysis of public authorities activity of different countries in the field of combating cybercrime, the article outlines a number of the most topical issues in this area that need solution.

Keywords: *cybercrime, combating cybercrime, cybercrime units, training of personnels, Department of Cybercrime Combating, MIA Ukraine.*

УДК 343.985

В. В. МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

Р. Р. САВЧЕНКО,
курсант
Харківського національного університету внутрішніх справ

ПРИНЦИПИ НАЛЕЖНОСТІ ЕЛЕКТРОННИХ ДОКАЗІВ, ОТРИМАНИХ З МОБІЛЬНИХ ПРИСТРОЇВ

Актуальність цього дослідження обумовлена відсутністю будь-яких досліджень в Україні щодо мобільної форензики, зокрема відносно відповідних електронних доказів, з урахуванням положень вітчизняного законодавства. Проаналізовано сутність мобільної форензики та електронних доказів, визначено джерела електронних доказів та дано характеристику принципів належності електронних доказів, отриманих з мобільних пристроїв.

Ключові слова: *комп'ютерна форензика, мобільна форензика, кіберзлочин, електронні (цифрові) докази, джерела електронних доказів, принципи належності електронних доказів.*

Комп'ютерна форензика – це відносно нова течія в українській криміналістиці, яка характеризується стрімким розвитком та включає в себе ретельний збір і дослідження електронних доказів із метою не лише оцінки завданих електронною атакою збитків, а також для відновлення втраченої інформації з таких систем для подальшого обвинувачення злочинця [1]. Як зазначають закордонні дослідники, це наука про зберігання, валідацію, ідентифікацію, аналіз, документування та представлення цифрових доказів, які розташовані на комп'ютерних жорстких дисках та інших ресурсах (CD та DVD-диски, зовнішні пристрої, модулі флеш-пам'яті, сервери голосової пошти) із метою сприяння реконструкції неправомірних подій та які можуть бути використані як докази в суді [2–4].

Зазначимо, що не лише розвиток комп'ютерної техніки є одним із факторів удосконалення методів здійснення кіберзлочинів, сьогодні використання смартфонів, які зберігають інформацію різноманітного характеру, теж представляють інтерес для правопорушників. Наслідки цього явища започаткували науку «мобільна форензика», яка стала невід'ємною частиною вітчизняної криміналістики.

Зазначимо, що смартфони за своєю суттю є невеликими комп'ютерами, тож під час збирання та дослідження цифрових доказів можуть бути застосовані і основні положення комп'ютерної форензики. Але є і суттєві відмінності: дані у смартфонах найвищою мірою є енергозалежними та постійно змінюються (якщо смартфон не вимкнений), додатково не можна просто скопіювати зміст пам'яті, оскільки дані зашифровані, тощо [5]. Таким чином, працівники правоохоронних органів, збираючи докази, мають знаходити вирішення цих та інших проблем, враховуючи той факт, що з випуском нової мобільної операційної системи або нового телефону виникає ряд інших труднощів.

Аналіз відповідних джерел [5; 6] дає підстави стверджувати, що найбільш удалим є таке визначення мобільної форензики (або форензики мобільних пристроїв) – це категорія комп'ютерної форензики, яка включає в себе мобільні телефони, смартфони, портативні обчислювальні пристрої (PDA), системи глобального позиціонування (GPS).

Вважаємо за необхідне звернути увагу на такий технічний атрибут мобільних пристроїв, як флеш-пам'ять, так як під час збирання електронних доказів виникає ряд проблем через потребу отримання з флеш-пам'яті незмінних даних. Відомо, що мобільні пристрої створюються невеликими за розміром, кожен тип пристрою має свої певні характеристики, задля збереження невеликого фізичного розміру пам'яті використовується флеш-пам'ять, яка, у свою чергу, поділяється на два види – NOR та NAND. Як будь-який накопичувач на жорстких дисках, флеш-пам'яті не потрібна напруга для підтримки даних на чипі. Не вдаючись до дискусій щодо технічних нюансів роботи флеш-пам'яті, оскільки це не є нашою метою, зазначимо таке:

1) флеш-пам'ять має менший проміжок часу свого існування, ніж будь-який інший накопичувач на жорстких дисках через швидке зношування, що призводить до стирання даних на чипі;

2) у пам'яті існує вбудована GC («збірка сміття») – процес утилізації пам'яті, що звільняється у процесі роботи програми або системи. Цей факт, що пам'ять переміщує дані та перезаписує сектори або сторінки без контролю операційної системи, робить її непередбачуваною.

Наведений приклад призводить до висновку, що фахівцям під час збор та дослідження електронних доказів потрібно не лише мати ґрунтовні знання у галузі комп'ютерних технологій, але й бути обізнаними щодо критеріїв, за якими отримані електронні докази будуть належними.

Отже, ґрунтуючись на цілях та призначенні форензики мобільних пристроїв, а також враховуючи практичну потребу в установленні єдиного підходу щодо отримання електронних (цифрових) доказів з мобільних пристроїв, метою цієї роботи є аналіз необхідних умов визнання електронних (цифрових) доказів, отриманих із мобільних пристроїв, належними. При цьому слід зазначити, що належними визнаються докази, які відповідно до кримінального процесуального кодексу України здатні своїм змістом встановлювати факти і обставини, які мають значення для кримінального провадження [7]. Тобто «…належність відповідає, з одного боку, на питання про наявність зв'язку між змістом доказу і фактом, який підлягає встановленню; з іншого боку – визначає, наскільки точно встановлено шуканий факт. Іншими словами, належний доказ має визначену доказову силу; не належний – не має її зовсім» [8, с. 9].

Зазначимо, що вітчизняними фахівцями досліджено загальні питання визначення поняття та принципів належності і допустимості доказів у кримінальному процесі [8; 9], але будь-яке теоретичне дослідження питання належності електронних доказів, отриманих з мобільних телефонів, в Україні відсутнє. Тому вбачаємо за необхідне використовувати здобутки зарубіжних учених у цій сфері для здійснення аналізу цього явища відповідно до визначеної мети.

Серед науковців, які у своїх роботах розглядали окремі аспекти цієї проблематики, варто зазначити Пітера Соммера, Генрі Лі, Елані Пагліаро, Алана Пендлетона, Павла Гладишева та ін.

Варто зауважити, що практика комп'ютерної форензики включає в себе формальні, загальноприйняті техніки для збирання, аналізу та представлення даних у суді, при цьому концентрується увага на принципах належності, допустимості, цілісності доказів, на законності цього процесу, на підготовці та отриманні експертного висновку [2]. Застосування комп'ютерної форензики потребує спеціальної підготовки і обізнаності у методах, інструментах та програмному забезпеченні для оцінки потенційної корисності комп'ютерних даних, для отримання та інтерпретації «прихованих» даних з комп'ютерних носіїв [2]. Але на сьогодні в Україні ще недостатньо приділяється увага розробкам методичних рекомендацій щодо алгоритму дій для виявлення, отримання та збереження електронних доказів.

Отже, досліджуючи питання принципів належності електронних доказів, отриманих із мобільних пристроїв, на нашу думку, спочатку варто надати визначення електронних доказів, їх значення, потім надати їх стислу характеристику, а вже потім перейти безпосередньо до характеристики принципів.

Переводячи наше дослідження у площину загальних підстав розповсюдження комп'ютерної техніки та мобільних пристроїв, а отже і актуальності обраної тематики, зауважимо, що внаслідок доступності електронних пристроїв велика кількість людей володіють мобільними телефонами, кишеньковими комп'ютерами, медіа-програвачами (IPod), інтернет-планшетами (iPad) та іншими персональними пристроями, встановлюють камери відеоспостереження, монітори та інші пристрої для запису інформації. Слідчі мають вилучати та зберігати всі ці типи пристроїв та будь-які цифрові камери, автовідповідачі, відеокамери, комп'ютери та пристрої накопичення даних. Зразки інформації, що можуть становити слідчий інтерес, включають у себе записи телефонних розмов, імейл-повідомлення, відновлені з жорстких дисків комп'ютера підозрюваного, відеозапис із камери спостереження банку тощо [10].

Зазначимо, що Прашант Малі називає електронними або цифровими доказами будь-яку доказову інформацію, яка зберігається або передається в цифровій формі, яку сторони можуть використовувати в судовому процесі [11]. В свою чергу Харлі Козушко зазначає, що цифрові докази – це всі цифрові дані, які можуть свідчити, що злочин було здійснено, та дозволяють встановити зв'язок між злочином і його жертвою, або між злочином і злочинцем [12]. Погоджуємося з наведеними визначеннями, оскільки вони доповнюють одне одного та виявляють сутності особливості електронних доказів.

В аспекті нашого дослідження зазначимо, що перед тим, як прийняти цифрові докази, суд визначатиме, чи є вони актуальними, справжніми, чи допустиме використання копії або обов'язковим є використання лише оригіналу тощо.

Важливим є і питання визначення джерел електронних доказів: вони можуть бути знайдені в електронних листах, цифрових фотографіях, лог-файлах, документах, в історіях повідомлень, у файлах, збережених у бухгалтерських програмах, електронних таблицях, у базах даних історій інтернет-браузерів, у вмісті пам'яті комп'ютера, в комп'ютерних резервних копіях, у комп'ютерних роздруківках, у логах, залишених глобальною системою позиціонування, в журналах із готельних електронних замків і цифрового відео або аудіофайлів, у мобільних телефонах та смартфонах, в конфігураційних файлах, в лог-файлах антивірусного програмного забезпечення тощо [11; 13]. Слід звернути увагу і на те, що цифрові докази схильні до масивності, менше піддаються руйнуванню, простіше модифікуються та дублюються.

Отже, детермінувавши сутність електронних доказів, їх значимість та джерела, спрямуємо наше дослідження безпосередньо на визначення принципів належності у випадку їх отримання з мобільних пристроїв.

Аналіз літератури [1; 6; 13–16], яку присвячено різним аспектам збирання електронних доказів не тільки з мобільних пристроїв, а і з

персональних комп'ютерів, дозволив виділити такі принципи належності електронних доказів, отриманих із мобільних пристроїв.

1. Допустимість. Докази мають бути збережені і зібрані таким чином, щоб вони могли використовуватись у суді. Як наслідок здійснення помилок може бути визнання частини доказів недопустимими.

Розглянемо декілька прикладів, щоб проілюструвати важливість та сутність такого принципу, як допустимість.

Зазначимо, що iPhone, будучи закритим пристроєм, не дозволяє безперешкодно виймати жорсткий диск, але на певному рівні можна вилучити дані.

Одна з найбільших помилок, що допускається стосовно пристроїв iOS, полягає у знищенні доказів під час використання деяких програм через користувацький інтерфейс. Наприклад, одним із важливих доказів, збережених на iPhone, є останні налаштування GPS, які зберігаються в кеші, коли GPS включений. Недосвідчений експерт може запустити додаток Google Maps на пристрої для відновлення адрес, за якими здійснювався пошук, випадково активувати GPS, тим самим знищити останні GPS налаштування і замінити їх поточними. Ці, здавалося б, нешкідливі дії також завантажать графічні зображення карти відносно поточної позиції, що перезапише дані в кеш. Внаслідок цього не тільки GPS-докази було знищено, а й інші карти, що залишились, може бути визнано недопустимими та відхилено суддею.

Інший приклад, де використання користувацького інтерфейсу може знищити докази, є запуск браузера Safari, який перезавантажує сторінки, які було раніше завантажено, всякий раз, коли завантажується додаток. Якщо одна зі сторінок належала до сторінок певного форуму або іншого веб-сайту для окремої спільноти людей, кеш може стати важливим місцем зберігання корисних доказів. Але запуск Safari може перезавантажити сторінку та переадресувати експерта до головної сторінки сайту, тим самим перезаписавши скриншоти та дані кешу, які містили докази.

2. Справжність. Докази мають бути релевантними відносно справи, і експерт-криміналіст повинен мати можливість оцінити справжність доказів.

Наприклад, перехоплення передачі електронної пошти не достатньо для доведення, що передбачуваний відправник є відповідальною особою за повідомлення. Має бути встановлений зв'язок між повідомленням та обліковим записом користувача або комп'ютером, з якого було відправлено повідомлення, та людиною, яка це повідомлення відправила. Якщо дійсно повідомлення було відправлено, повинен залишитись слід у вигляді доказів на кількох комп'ютерах у різних інтернет-провайдерів, які це підтверджують.

3. Повнота. Цей принцип полягає в тому, що наведені докази мають проілюструвати всю картину подій, які відбулися.

Чітка і повна картина подій має бути наведена з тим, щоб прояснити, яким чином було залишено докази. Зрозуміло, що неперевірена частина неповних доказів може залишитись непоміченою, що є набагато небезпечнішим, ніж відсутність доказів взагалі.

Розглянемо приклад, наведений у дослідженні Мета Енгмана [5], відносно чоловіка, який був звинувачений у зберіганні фотографій із дитячою порнографією. Наведені докази свідчили, що фотографії відповідного змісту було завантажено на робочий комп'ютер обвинуваченого, але пізніше захисник виявив, що ці фотографії було завантажено внаслідок дії вірусу на машині а не самим обвинуваченим. Як результат – невинну людину було майже засуджено і посаджено до в'язниці, тому що експерт з боку обвинувачення не надав повні докази, а присяжні не володіли необхідними технічними знаннями, щоб це помітити.

Отже, враховуючи всю різноманітність процесів, які можуть відбуватися на комп'ютері, на мобільному телефоні, вельми важливою постає можливість ув'язати частину доказів із їх першоджерелом та уявити всю картину подій, що відбулися.

Ґрунтуючись на практичних аспектах застосування цього принципу – повноти електронних доказів – здійснимо аналіз ще кількох прикладів його використання.

Так, здійснення корпоративних розслідувань сприяло встановленню такого першорядного правила, як безпечне видалення даних з метою забезпечення цілісності пристрою [5]. Наприклад, підозрюваний може стверджувати, що видалена фотографія не належить йому. Якщо дані з пристрою не було надійно знищено перед його експлуатацією наступним користувачем, то захисник може опротестувати підозру тією обставиною, що дані на пристрої

залишились після попереднього користувача. В свою чергу це спричинить необхідність знайти відповіді на такі питання: яким чином цей доказ потрапив на цей мобільний пристрій, і завдяки чиїм діям це відбулося?

Розглядаючи питання належності електронних доказів, отриманих із мобільних пристроїв, зазначимо, що можливими джерелами отримання зображень можуть бути вбудовані камери iPhone, результати синхронізації з робочим столом як підозрюваного, так і будь-якої іншої особи, збережені зображення з електронної пошти або браузера, завод-виробник мобільного пристрою тощо [5].

Таким чином, щоб електронні докази були повними, потрібно прийняти до уваги, де саме зображення або будь-який інший електронний доказ був створений.

4. Надійність. Сутність цього принципу полягає в тому, що будь-які зібрані докази мають бути надійними, і ця їх характеристика залежить від обраних інструментів та методології, підґрунтя для надання переваги яким складає науковий підхід.

Слід підкреслити, що методи, які використовуватимуться, мають бути достовірними і загальноприйнятими в цій галузі. Також акцентуємо увагу на тому, що будь-яку активність слід задокументовувати: випадки перезавантаження мобільного пристрою, виникнення непередбачуваних ускладнень під час роботи з мобільним пристроєм, маніпуляції з електронними доказами тощо.

5. Зрозумілість та правдоподібність. Цей принцип полягає в тому, що судовий експерт повинен бути в змозі чітко та лаконічно пояснити, які прийоми він використовував під час дослідження доказів і яким чином була збережена цілісність даних. Докази мають піддаватися легкому поясненню і бути правдоподібними.

Отже, названі вище характеристики доказів є гарантом прийняття законних і обґрунтованих процесуальних рішень, а також засобом запобігання порушення прав і свобод громадян, покарання невинуватого або виправдання особи, яка вчинила злочин. У роботі поділяється позиція, що приведений перелік принципів належності електронних доказів, отриманих із мобільних пристроїв, не є вичерпним, але подібне узагальнення, що носить рекомендаційний характер, здійснюється вперше у вітчизняній комп'ютерній, а саме мобільній, форензиці.

Також вбачається доцільним у подальшому напрямку дослідження цієї тематики вирішити питання щодо встановлення підстав недопустимості електронних доказів (отриманих із будь-яких цифрових носіїв), здійснити ґрунтовний аналіз питання визначення та узгодженості електронних (цифрових) доказів, їх класифікації та правового порядку отримання відповідно до кримінального процесуального кодексу України та цивільного процесуального кодексу України.

Список використаних джерел

1. Bui S. Issues in Computer Forensics [Електронний ресурс] / Sonia Bui, Michelle Enyeart, Jenghuei Luong. – May 22, 2003. – [36 p.]. – Режим доступу: http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf.

2. Computer Forensics Defined [Електронний ресурс]. – Режим доступу: http://www.electronicevidenceretrieval.com/eer_computer_forensics_defined.htm.

3. Gladyshev P. Formalising Event Reconstruction in Digital Investigations : dissertate / Pavel Gladyshev. – 2004 [Електронний ресурс]. – Режим доступу: http://www.gladyshev.info/publications/thesis/.

4. Kessler International – Forensic Accounting, Computer Forensics, Corporate Investigation [Електронний ресурс]. – Режим доступу: http://www.investigation.com/computer_forensics.htm.

5. Engman M. Forensic investigations of Apple's iPhone [Електронний ресурс] / Mats Engman. – Maj 2013. – [35 p.]. – Режим доступу: http://www.diva-portal.org/smash/get/diva2:651693/FULLTEXT01.pdf.

6. Zdziarski J. iOS Forensic Investigative Methods : technical draft : 5/13/12 [Електронний ресурс] / Jonathan Zdziarski. – [164 p]. – Режим доступу: http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods.pdf.

7. Кримінальний процесуальний кодекс України. Науково-практичний коментар. [Електронний ресурс] / за ред. Гончаренко В. Г., Нора В. Т., Шумила М. Є. – Харків : Право, 2012. – 844 с. – Режим доступу: http://pidruchniki.ws/1233090949171/pravo/kriminalniy_protsesualniy_kodeks_ukrayini_naukovo-praktichniy_komentar_-_tatsiy_vya.

8. Степанов О. С. Належність та допустимість доказів у кримінальному процесі України : автореф. дис. … канд. юрид. наук : 12.00.09 / Степанов Олег Станіславович. – Київ, 2007. – 20 с.

9. Шумило М. Є. Гносеологічна і процесуальна природа доказів у кримінальному процесуальному кодексі України / М. Є. Шумило // Актуальні питання кримінального процесуального законодавства України (Київ, 26 квіт. 2013 р.) : зб. матеріалів міжвуз. наук. конф. / Нац. акад. прокуратури України. – Київ : Алерта, 2013. – С. 13–27.

10. Lee H. C. Forensic Evidence and Crime Scene Investigation / Henry C. Lee and Elaine M. Pagliaro // Forensic Investigation. – 2013. – Vol. 1, Issue 1. – [5 p.] [Електронний ресурс]. – Режим доступу: http://www.avensonline.org/wp-content/uploads/2013/10/JFI-2330-0396-01-0004.pdf.

11. Mali P. Electronic Evidence & Cyber Law [Електронний ресурс] / Prashant Mali // CSI Communications, September 2012. – P. 30–31. – Режим доступу: http://www.csi-india.org/c/document_library/get_file?uuid=d817e5eb-ca5a-40c2-b8aa-d6302c26443a&groupId=10157.

12. Kozushko H. Digital Evidence [Електронний ресурс] / Harley Kozushko. – [17 p.]. – November 23, 2003. – Режим доступу: http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf.

13. Sommer P. Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers [Електронний ресурс] / Peter Sommer. – [3-rd ad.]. – [Mar. 2012]. – [115 p.]. – Режим доступу: http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf.

14. Grafinkel S. L. Digital Forensics [Електронний ресурс] / Simson L. Grafinkel // American Scientist. – September – October 2013. – Vol. 101, Num. 5. – Режим доступу: http://www.americanscientist.org/issues/feature/2013/5/digital-forensics.

15. Best Practices For Seizing Electronic Evidence. Vol. 3 : A Pocket Guide for First Responders / U.S. Secret Service Criminal Investigative Division, United States of America. – 2007. – 24 p. [Електронний ресурс]. – Режим доступу: http://www.forwardedge2.com/pdf/bestpractices.pdf.

16. Pendleton A. Admissibility of Electronic Evidence: A New Evidentiary Frontier [Електронний ресурс] / Alan Pendleton. – Oct. 14, 2013. – Режим доступу: http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/.

Надійшла до редколегії 18.03.2014

МАРКОВ В. В., САВЧЕНКО Р. Р. ПРИНЦИПЫ ПРИНАДЛЕЖНОСТИ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ, ПОЛУЧЕННЫХ С МОБИЛЬНЫХ УСТРОЙСТВ

Актуальность этого исследования обусловлена отсутствием каких-либо исследований в Украине относительно мобильной форензики, в частности относительно соответствующих электронных доказательств, с учётом положений национального законодательства. Работа посвящена анализу сущности мобильной форензики и электронных доказательств, определению источников электронных доказательств и характеристике принципов принадлежности электронных доказательств, полученных с мобильных устройств.

Ключевые слова: *компьютерная форензика, мобильная форензика, киберпреступление, электронные (цифровые) доказательства, источники электронных доказательств, принципы принадлежности электронных доказательств.*

MARKOV V. V., SAVCHENKO R. R. PRINCIPLES OF ELECTRONIC EVIDENCE'S BELONGING RECEIVED FROM MOBILE DEVICES

The paper is devoted to the analysis of mobile forensic and electronic evidence's essence, identifying possible sources of electronic evidence and characteristics of the principles of electronic evidence's belonging received from mobile devices.

The relevance is defined by the absence of any research in Ukraine about mobile forensic as a part of the computer forensic science, in particular concerning the way of receiving electronic evidence from mobile devices and characteristics of belonging and admissibility of obtained evidence. These attributes are the guarantee of making legal and grounded procedural decisions and a way to prevent violations of human rights and freedoms, sentencing an innocent or justifying a person who committed a crime.

The paper asserts the position that mobile forensic is a category of computer forensic, which includes cell phones, smart phones, portable devices of accounting (PDA), global positioning systems (GPS).

The author agrees with the definition of electronic evidence provided by foreign scientists, where it is any evidence information stored or transmitted in digital form, which the parties can use within the trial, and that is evidence of a crime commission and allows to set relation between a crime and its victim or between a crime and a criminal.

The result of the research is to determine the following principles of electronic evidence's belonging received from mobile devices: admissibility, authenticity, completeness, reliability, clarity and credibility.
It is reasonable, as the further direction of research of this topic, to solve the problem of establishing grounds for electronic evidence's inadmissibility (received from any digital devices), realization of a thorough analysis of the determination and consistency of electronic (digital) evidence, their classification and legal order of receiving under the Criminal Procedural Code of Ukraine and the Civil Procedural Code of Ukraine.

Keywords: *computer forensic, mobile forensic, cybercrime, electronic (digital) evidence, sources of electronic evidence, principles of electronic evidence's belonging.*

УДК 343.26

К. А. НОВІКОВА,
аспірант
Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

СПІВВІДНОШЕННЯ ОБМЕЖЕННЯ ВОЛІ ТА ПРОБАЦІЇ: ЗАРУБІЖНИЙ ДОСВІД

Досліджено засоби, що пов'язані з обмеженням особистої свободи особи, яка вчинила злочин. Розглянуто питання про співвідношення пробації за кримінальним правом англосаксонських держав (на прикладі США) із заходами кримінально-правового впливу кримінального права країн пострадянського простору (на прикладі Російської Федерації). Підкреслено необхідність відмежування заходів суто кримінальної відповідальності і заходів, які за правовою природою не пов'язані з нею.

Ключові слова: *вид покарання, система покарань, обмеження волі, пробація, зміст покарань.*

Останнім часом світове співтовариство як на національних, так і на міжнародному рівнях переймається проблемою пошуку найбільш адекватних заходів протидії злочинності. Давно вже стало очевидним, що одна тільки кримінальна відповідальність та покарання як її складова не можуть бути єдиними засобами у такій протидії. Саме тому особливо актуалізувалося питання пошуку заходів, альтернативних кримінальній відповідальності. Внаслідок такого пошуку у правових системах багатьох країн з'являються заходи, альтернативні кримінальній відповідальності, такі, наприклад, як заходи безпеки, заходи відновлення і примирення, інші заходи кримінально-правового характеру. Через це традиційне «одноколійне» кримінальне право відходить у минуле, і йому на зміну приходить так звана система «багатоколійного» кримінально-правового впливу на злочинність.

Серед засобів кримінально-правового впливу на злочинність істотне місце посідають такі засоби, які пов'язані з обмеженням особистої свободи особи, що вчинила злочин. У деяких зарубіжних країнах подібні заходи називаються пробацією. Відомо, що сам термін пробація є полісемічним [1, с. 61], однак ми її розглядаємо як саме захід кримінально-правового впливу, який застосовується від імені держави судом. Крім того, у науці часто зустрічаються судження про пробацію, в якій суб'єкт виконання – громада (суспільство) [2, с. 28–30]. Ми вважаємо, що такі заходи мають відміну від кримінально-правової природи і залишаються за межами цього дослідження.

Крім того, інститут пробації та схожий з ним інститут покарання у виді обмеження волі ми розглянемо крізь призму правових систем Росії та США. Це обумовлено тим, що саме ці країни найбільше потребують розробки заходів, альтернативних позбавленню волі, адже США – перша у світі країна за кількістю ув'язнених на душу населення, Росія – друга [3]. Незважаючи на ідеології підходів, які суттєво відрізняються між собою, порівняння вбачається нам доцільним. Аналізуючи обмеження волі за кримінальним правом Росії та пробацію за кримінальним правом США, знаходимо значну кількість спільних рис. Водночас, істотну проблему становить відсутність відповідних понять, якими можна б було скористатись для такого порівняння, або