

УДК 23.1448

ВИСУНЕННЯ І ПЕРЕВІРКА СЛІДЧИХ ВЕРСІЙ ПРО ЦИФРОВЕ АЛІБІ ПІДОЗРЮВАНОВОГО (ОБВИНУВАЧЕНОГО)

Давидюк П.П.

Національний університет водного господарства та природокористування

Кубай І.Ю.

Навчально-науковий інститут права

Національного університету водного господарства та природокористування

Стаття присвячена питанню перевірки версії про цифрове алібі – ситуації, коли підозрюваний (обвинувачений) заявляє, що у момент учинення злочину він виконував роботу з комп'ютером, який знаходився поза зоною місця його здійснення. Алібі є логічною системою, що складається з трьох елементів: час скоєння злочину, місце його здійснення і місце фактичного знаходження заявника алібі у момент скоєння злочину. Визначення категорій «цифрові» докази, ідеальні, матеріальні, візуальні сліди та їх практичне застосування при плануванні перевірки версії. Аналіз віртуальних слідів, що виникають в ході роботи з комп'ютером, мають найбільше значення при перевірці версій про цифрове алібі підозрюваного (обвинуваченого), оскільки вони, в силу своєї природи, мають жорстку прив'язку до часу їх виникнення. Дослідження комп'ютерної інформації як предмету перевірки в ході слідчих дій, та в подальшому як доказова інформація при судовому розгляді справи. Розгляд механізму здійснення фальсифікації цифрової інформації та його впливу на визначення достовірності алібі підозрюваного (обвинуваченого).

Ключові слова: цифрове алібі, слідча версія, момент здійснення злочину, персональний комп'ютер, цифрова інформація, фальсифікація, докази.

Постановка проблеми. З розвитком технологій в сучасному житті люди дедалі більше взаємодіють з електронними системами (працюють з персональним комп'ютером, користуються мобільним телефоном, потрапляють у поле зору камер спостереження, авторизуються у системах контролю доступу до приміщень). Єдиним «свідком» цієї взаємодії стає машина та інформація в ній. Тому визначити чи дійсно в певний момент часу особа, яка підозрюється або обвинувачується у скоєнні злочину працювала з комп'ютером дуже складно. З цього випливає необхідність висунути і перевірити слідчі версії про цифрове алібі.

Аналіз останніх досліджень та виокремлення нерозв'язаних проблем. Для нашої правової доктрини поняття «цифрових доказів» і «цифрового алібі» є досить новим, хоча й привертало увагу таких вчених як В. М. Бутузов, В. Б. Вехов, С. Й. Гонгало, М. А. Іванов, Т. Е. Кукарнікова, Л. Б. Краснова, А. В. Касаткін, Ю. М. Літвінов, В. В. Лисенко, В. О. Мещеряков, Д. В. Пашнев, М. М. Федотов тощо.

Водночас, розроблені науковцями пропозиції та надані рекомендації не були враховані під час підготовки нового Кримінального процесуального кодексу України, що знову актуалізує цю проблему, яка вимагає комплексного вивчення та обговорення вченими із урахуванням нових реалій.

Метою статті є аналіз теоретико-прикладних підходів щодо розуміння цифрового алібі та визначення його місця у системі засобів доказування.

Виклад основного матеріалу. При кримінально-процесуальному дослідженні злочинів з матеріальним складом, механізм скоєння яких містить в собі які-небудь дії підозрюваного (обвинуваченого) на місці злочину в момент його скоєння (а таких – більшість), завжди виникає необхідність у висуненні і перевірці кримінологічних версій про алібі підозрюваного (обвинуваченого) бо існує прив'язка до часу. В основі висунення таких версій, в більшості випадків, лежить інформа-

ція, отримана в ході допиту вказаних осіб, які, як переконливо покаже практика кримінального судочинства останніх років, в обґрунтуванні заявляючого алібі все частіше посилаються на те, що в момент скоєння злочину вони здійснювали роботу з персональним комп'ютером чи іншим гаджетом, який знаходиться в іншому місці. За кордоном такі пояснення отримали, на мій погляд, цілком влучну назву «цифрове алібі», так як основним джерелом формування доказів виступає інформація, записана в цифровій формі на машинних носіях [3, с. 455].

На основі такої інформації, отриманої в ході допиту та інших слідчих дій, експертиз та перевірки носія інформації – персонального комп'ютера, може бути сформульована версія про цифрове алібі особи в будь-якому із можливих варіантів:

1. Підозрюваний (обвинувачений) має цифрове алібі.

2. Підозрюваний (обвинувачений) не має цифрове алібі.

3. Цифрове алібі підозрюваного (обвинуваченого) сфальсифіковано.

Беручи до уваги, що криміналістична версія лише уявний образ тої чи іншої події, практичні перевірці піддаються тільки наслідки з неї, які обумовлюють відповідні напрями пошуку.

Як відомо, причина веде до свого вичерпного відображення в наслідках своєї дії – робота особи з комп'ютером тягне появу відповідних слідів. Будь-які дії з ресурсами комп'ютера можна простежити за допомогою слідів в пам'яті комп'ютера чи залишеної інформації в інтернет мережі.

Користуючись системою, розробленою криміналістикою для класифікації слідів злочину, яка, на мою думку, універсальна і застосовна для будь-якого процесу дійсності, серед вказаних слідів роботи з комп'ютером цілком обґрунтовано можна виділити ідеальні, матеріальні і віртуальні сліди.

Дійсно, процес роботи з комп'ютером відбивається у свідомості, пам'яті користувача – ви-

никають ідеальні сліди. Особа при допиті розповідає скільки часу працювала з персональним комп'ютером, які саме операції здійснювала і вказує на наявні файли чи інші цифрові форми відображення інформації, які можуть мати вказівку на час їх створення, зміни чи видалення, що дозволить визначити алібі підозрюваного (обвинуваченого). На периферійному устаткуванні комп'ютера, клавішах, «миші» інших матеріальних об'єктах що беруть участь в процесі роботи (наприклад, листках паперу при роздруку текстів на принтері), залишаються матеріальні сліди – відбитки пальців, потожирові сліди, сліди тютюну і т.д. Проте велика частина інформації в процесі роботи з комп'ютером виникає і зберігається в пам'яті комп'ютера, на машинних носіях у вигляді віртуальних слідів, що займають проміжне положення між матеріальними і ідеальними [5, с. 209].

Саме віртуальні сліди, що виникають в ході роботи з комп'ютером, мають найбільше значення при перевірці версій про цифрове алібі підозрюваного (обвинуваченого), оскільки вони, в силу своєї природи, мають жорстку прив'язку до часу їх виникнення.

Так, наприклад, час включення і відключення комп'ютера, підключення до комп'ютерної мережі і зовнішнього устаткування, час запуску і зупинки системних служб, час установки програмного забезпечення і інших подій фіксується в системному «журналі подій».

Окрім системного «журналу подій», більшість застосованих програм (текстових редакторів, Інтернет-браузерів, систем обміну миттєвими повідомленнями) мають вбудовані функції збереження історії своєї роботи. Також багато комп'ютерних програм «ведуть» власні, так звані, файли протоколу [1, с. 437].

Крім того, при роботі особи з персональним комп'ютером відбувається зміна файлів і їх тимчасових міток (часу створення, модифікації, останнього доступу).

Також на сьогоднішній день більшість людей має доступ до Інтернет-мережі, відвідує різні сайти та особливо соціальні мережі. На сьогодні набули популярність портативні комп'ютери та смартфони, які мають споряджені функцією «геолокації» за допомогою якої можна визначити місце знаходження користувача, за умови його під'єднання до Інтернет-мережі. Проте прив'язати місцезнаходження абонента в певний відрізок часу за допомогою такої схеми складно, адже час перебування на тому чи іншому місці переносного комп'ютера не завжди співпадає із місцем перебування особи, якій належить даний комп'ютер.

При цьому необхідно враховувати, що комп'ютерна інформація є такою, що легко модифікується і є украй нестійкою. Звідси виникає не менш важливе завдання встановлення, чи не були віртуальні сліди роботи підозрюваного (обвинуваченого) з комп'ютером під час скоєння злочину, сфальсифіковані в цілях створення собі алібі.

Фальсифікація віртуальних слідів роботи можлива шляхом переведення системних годинників комп'ютера, додаванням неправдивої інформації у файли «журналу подій» і файли протоколу, використанням макросів, а також іншими способами.

Зауважу, що можливість встановлення фальсифікації обґрунтована положенням про те, що знищуючи, додаючи або модифікуючи віртуальні сліди роботи з комп'ютером, користувач породжує інші сліди, відповідно, сліди знищення, додавання чи модифікації інформації.

Таким чином, з методологічних позицій і для цілей формування системи наслідків, що впливають на процес висунення версії відносно цифрового алібі, необхідно враховувати, що:

1) алібі є логічною системою, що складається з трьох елементів: час скоєння злочину, місце його здійснення і місце фактичного знаходження заявника алібі у момент скоєння злочину [2, с. 308];

2) основним джерелом формування доказів, що підтверджують або спростовують цифрове алібі, виступає інформація, що знаходиться в цифровій формі на машинних носіях, яку можна отримати в ході знайдення та дослідження матеріальних, ідеальних та віртуальних слідів залишених в пам'яті комп'ютера та на периферії;

3) ця інформація, завдяки своїй природі, легко може бути створена, змінена (модифікована) і знищена, в тому числі і в цілях її фальсифікації для подальшого забезпечення доказів неправдивого алібі.

Згідно розглянутих вище положень, в найзагальнішому вигляді, можна виділити необхідні ознаки версій про цифрове алібі:

1) слідів роботи з комп'ютером у момент часу, зафіксований як час злочину, немає;

2) є сліди роботи особи на стаціонарному (не портативному) комп'ютері, що знаходиться в місці відмінному від місця злочину, у момент часу, зафіксованому як час здійснення злочину;

3) є сліди роботи особи на портативному комп'ютері (ноутбук, нетбук) місцезнаходження якого на час здійснення злочину не встановлено;

4) ознак фальсифікації (модифікації, штучного створення) слідів роботи з комп'ютером в указаний час нема [4, с. 376].

Зауважу, що встановити місцезнаходження портативного комп'ютера в момент часу, що цікавить, можливо лише за наявності слідів його підключення у цей момент часу до мережі Інтернет або до периферійного не портативного устаткуванню, місцезнаходження якого встановлено.

Очевидно, що для спростування цифрового алібі підозрюваного (обвинуваченого) досить хоч би одного з наступних елементів:

1) слідів роботи з комп'ютером у момент часу, зафіксованого як час злочину, немає;

2) є ознаки фальсифікації (модифікації, штучного створення) слідів роботи з комп'ютером у момент часу, зафіксованого як час злочину.

Крім того, можуть бути розглянуті і можливі наслідки, витікаючі з версії про цифрове алібі. Наприклад, за наявності підключення комп'ютера підозрюваного (обвинуваченого) до комп'ютерної мережі Інтернет можна виділити наступні наслідки:

1) у постачальника послуг Інтернет (Інтернет-провайдера) є дані про сеанс роботи з комп'ютером підозрюваного (обвинуваченого);

2) хтось міг зв'язуватися з підозрюваним (обвинуваченим) за допомогою Інтернет-комунікацій (системи миттєвих повідомлень, електронна пошта, відеоконференції, Інтернет-телефонія і т.д.) [6, с. 208].

3) при підключенні до Інтернет-мережі можна визначити місцезнаходження («геолокацію») портативного комп'ютера, в який вбудована система визначення перебування.

Сформульована система необхідних і можливих наслідків з версій про цифрове алібі зумовлює планування їх перевірки. Практична перевірка повинна привести або до підтвердження версії про цифрове алібі, або до її спростування. У якості першочергових дій, як правило, є дії, спрямовані на виявлення і фіксацію швидко змінюючих слідів, а також доказів, які можуть бути втрачені або умисне видозмінені.

Враховуючи виправдовувальну силу алібі взагалі, практична значущість розробки питань перевірки слідчої версії про цифрове алібі цілком очевидна. Актуальність проблеми усвідомлюється повніше, якщо взяти до уваги дані статистики: необхідність в перевірці алібі

найчастіше виникає у випадках розслідування умисних вбивств, здійснених як прийнято говорити, не в умовах очевидності, тобто злочинів, які розкрити найскладніше.

Висновки та пропозиції. Підсумовуючи викладене, відзначу, що перманентне збільшення цифрової інформації та її систематичне використання у різних сферах життєдіяльності зумовлює необхідність вироблення оптимальних підходів щодо її використання у доказуванні в кримінальних провадженнях. З урахуванням того, що цифрові докази можуть бути використані як забезпечення підозрюваному (обвинуваченому) алібі існує необхідність уведення категорії «цифрового алібі» під яким слід розуміти доказ невинуватості підозрюваної у правопорушення особи, оскільки в момент правопорушення (скоєння злочину) вона перебувала в іншому місці за роботою з комп'ютером.

Список літератури:

1. Грошевий Ю. М. Докази і доказування у кримінальному процесі: наук.-практ. посіб. / Ю. М. Грошевий, С. М. Стахівський. – К.: КНТ, 2006. – 272 с.
2. Иванов Н. А. Применение специальных знаний при проверке «цифрового алиби» / [Электронный ресурс]. – Режим доступа: <http://www.infolaw.ru/lib/2006-4>
3. Пономарев И. П. Цифровое алиби и его проверка / И. П. Пономарев // Вестник ВГУ. Серия: Право, 2011. – № 2. – 437 с.
4. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования / В. А. Мещеряков; науч. ред. О. Я. Баев. – Воронеж: Изд-во Воронежского государственного университета, 2002. – 102 с.
5. Федотов Н. Н. Форензика – компьютерная криминалистика / Н. Н. Федотов. – М.: Юрид. мир, 2007. – 360 с.
6. Цехан Д. М. Правові аспекти використання цифрової інформації як доказу у кримінальному судочинстві / Д. М. Цехан // Процесуальні, тактичні та психологічні проблеми, тенденції та перспективи вдосконалення досудового слідства: матеріали міжнар. наук.-практ. конф. (Одеса, 30 травня 2008 р.). – Одеса, 2008. – 209 с.

Давидюк П.П.

Национальный университет водного хозяйства и природопользования

Кубай И.Ю.

Учебно-научный институт права

Национальный университет водного хозяйства и природопользования

ВЫДВИЖЕНИЕ И ПРОВЕРКА СЛЕДСТВЕННЫХ ВЕРСИЙ О ЦИФРОВОМ АЛИБИ ПОДОЗРЕВАЕМОГО (ОБВИНЯЕМОГО)

Аннотация

Статья посвящена вопросу проверки версии о цифровом алиби-ситуациях, когда подозреваемый (обвиняемый) заявляет, что в момент совершения преступления он выполнял работу с компьютером, который находился вне зоны места его осуществления. Алиби является логической системой, состоящей из трех элементов: время совершения преступления, место его совершения и место фактического нахождения заявителя алиби в момент совершения преступления. Определение категорий «цифровые» доказательства, идеальные, материальные, визуальные следы и их практическое применение при планировании проверки версии. Анализ виртуальных следов, возникающих в ходе работы с компьютером, имеющие наибольшее значение при проверке версий о цифровом алиби подозреваемого (обвиняемого), поскольку они, в силу своей природы, имеют жесткую привязку ко времени их возникновения. Исследование компьютерной информации как предмета проверки в ходе следственных действий, и в дальнейшем в качестве доказательной информации при судебном рассмотрении дела. Рассмотрение механизма осуществления фальсификации цифровой информации и его влияния на определение достоверности алиби подозреваемого (обвиняемого).

Ключевые слова: цифровое алиби, следственная версия, момент осуществления преступления, персональный компьютер, цифровая информация, фальсификация, доказательства.

Davudiyk P.P.

National University of Water and Environmental Engineering

Kubay I.Y.

Institute of Law

National University of Water and Environmental Engineering

ADVANCEMENT AND VERIFICATION OF INQUISITIONAL VERSIONS ABOUT DIGITAL ALIBI SUSPECTED (DEFENDANT)

Summary

The article deals with checking versions of digital alibi- situations where the suspect (accused) said that at the time of commission of the crime heper formed work on the computer, which was outside his place of execution. Alibi is a logical system consisting of three elements: time of the offense, the place of his execution and the actual location of the applicant's alibi att he time of the crime. Determining the categories of «digital» proof, perfect, physical, visual trace sand their practical application in planning inspections version. Analysis of virtual track sthatarise in the course of a computer, are most important when testing digital versions oft he alibi of a suspect (accused) because they, by virtue of their nature, are concerned with the time of their occurrence. The study of computer data as a subject inspection during their vestigation, and fur ther information as evidence at trial. Review Mechanism off al sification of digital media and it simpart on the determination of there liability of the alibi of a suspect (accused).

Keywords: digital alibi, inquisitional version, moment of realization of crime, personal computer, digital information, falsification, proofs.