УДК 343.102:004.08 DOI https://doi.org/10.26661/2616-9444-2019-2-09

Проблемні питання проведення слідчих (розшукових) дій, які супроводжуються вилученням електронних носіїв інформації

Єна І. В.

Запорізький національний університет, вул. Жуковського, 66, м. Запоріжжя, Україна
ena-irina@ukr.net

Ключові слова:
електронні носії інформації, інформаційне суспільство, інформатизація, експертна діяльність.

Надійшло до редколегії: 09.09.2019
Прийнято до друку: 17.10.2019

У статті досліджено складнощі, які виникають у практичній діяльності правоохоронних органів під час розслідування комп'ютерних злочинів, зокрема проблеми, які виникають під час проведення слідчих (розшукових) дій, які спрямовані на отримання доказово значущої інформації у провадженні та супроводжуються вилученням електронних носіїв інформації. Запропоновано правила їх ефективного вилучення.

Problems of issues of the investigative (definitive) actions the extraction of electronic media

Yena I. V.

Zaporozhye National University, str. Zhukovski, 66, Zaporizhzhya, Ukraine
ena-irina@ukr.net

Key words:
electronic media, evidence, sources of evidence information society, informatization, expert activity.

The article explores the difficulties that law enforcement agencies have in the investigation of computer crimes. Including problems that arise when conducting investigative (investigative) actions that are aimed at obtaining provably meaningful information and are accompanied by the seizure of such a specific source of evidence as electronic media. In addition, rules are proposed that comply with which can ensure the effectiveness of the removal of electronic storage media and the possibility of further use of the data obtained in the process of proof.

Sufficient conditions for further development of the information society have been created in Ukraine. However, there are a number of problems that affect this process, which can be attributed to: unjustifiably low availability of modern computer hardware not only for individual sectors of the economy, but also for entire regions, different sections of the population; poor computer literacy (especially for people over fifty); lagging behind the introduction of e-business technologies, etc.

In addition, there are factors that complicate the investigation of this category of unlawful acts: 1) insufficient logistical support for law enforcement units investigating computer crimes; 2) lack of proper level of cooperation and mutual information with law enforcement agencies of other countries, and this cooperation should be established, as cybercrime is transnational; 3) the basis of the national cybersecurity system is a fairly wide range of ministries and agencies and this leads to a lack of coordination of their actions; 4) the complexity of the construction of legal norms, which affects the correct qualification of this type of crime; 5) timeliness of investigative (investigative) actions also poses a

certain problem, etc.
In this way, we can formulate general rules that can be used to ensure that electronic data retrieval is effective and that the data obtained can be further used in the proofing process. First, the person who removes the electronic storage media must have special knowledge, training and skills. Second, the general criminal procedural and expert provisions must be strictly observed. Third, the removal must be made in such a way that it does not alter, damage, or destroy the electronic medium and the information stored therein. Fourth, all actions that took place when detecting and removing electronic storage media should be fully documented in the procedural documents.

Інформаційна сфера суспільства сьогодні є галуззю людської діяльності, яка найбільш динамічно розвивається. Суспільство стає більш інформаційно насиченим. Ми можемо констатувати формування інформаційного суспільства, якому притаманні такі ознаки, як наявність відкритих можливостей для будь-якої фізичної особи отримувати будь-яку інформацію для вирішення питань особистого чи суспільного характеру; наявність та доступність сучасної інформаційної технології будь-якій фізичній чи юридичній особі; розвиненість інформаційної інфраструктури; створення національних інформаційних ресурсів; прискорена автоматизація та роботизація всіх сфер і галузей національного господарства; розширення сфери інформаційної діяльності; зростання кількості зайнятих в інформаційній сфері національного господарства [1, с. 78].

Основною характеристикою інформаційного суспільства є його глобальна інформатизація. Інформатизація – це сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб, реалізацію прав громадян і суспільства на основі формування, розвитку, використання інформаційних систем, мереж, ресурсів та інформаційних технологій, створених на основі застосування сучасної обчислювальної та комунікаційної техніки [2]. Інформатизація є важливою властивістю суспільства та впливає на всі сфери людського життя, оскільки забезпечує підвищення рівня організації праці, освіти, швидкості виконання послуг, поширення інформації серед населення, у виробництво запроваджуються високі технології, з'являються нові галузі виробництва, полегшується та пришвидшується процес здійснення фінансових операцій тощо.

Про активізацію процесу інформатизації в Україні на державному рівні свідчать розроблення та введення в дію Законів України «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», Концепції Національної програми інформатизації, схваленої Законом України «Про Концепцію Національної програми інформатизації», Закону України «Про Національну програму інформатизації». Задля повноцінного переведення роботи органів виконавчої влади в електронну форму у 2018 році прийнято Постанову КМУ «Деякі питання документування управлінської діяльності», яка визначає електронну форму діловодства як основну для установ і підприємств державного сектору. Відповідно до Закону України «Про місцеве самоврядування в Україні» здійснюється запровадження технологій електронного урядування в місцевих органах виконавчої влади та органах місцевого самоврядування.

Місцева влада також не стоїть осторонь процесу інформатизації, про що свідчить розроблення Програм інформатизації в таких областях України, як Львівська, Вінницька, Одеська,

Рівненська, Харківська, Дніпропетровська, тощо, запровадження яких дасть змогу інтегрувати області до загальнодержавного та світового інформаційного простору. Отже, ми можемо стверджувати, що в Україні створені достатні умови для подальшого розвитку інформаційного суспільства, проте існує низка проблем, які впливають на цей процес, до яких можна віднести невиправдано низький рівень забезпеченості сучасною комп'ютерною технікою не тільки окремих галузей економіки, але й цілих регіонів, різних верств населення; низький рівень комп'ютерної грамотності населення (особливо це стосується людей віком старше п'ятдесяти років); відставання запровадження технологій електронного бізнесу.

Сподіваємось на те, що такі перепони будуть усунуті найближчим часом, оскільки у 2017 році за Розпорядженням Кабінету Міністрів України було розроблено Концепцію розвитку електронного урядування, відповідно до якої передбачається до 2020 року вжити заходів за такими трьома ключовими напрямами:

– модернізація публічних послуг (100 найбільш важливих онлайн-послуг для громадян та бізнесу);

– модернізація публічного управління (електронна взаємодія реєстрів);

– управління розвитком е-урядування (впровадження міжнародного досвіду роботи з державними актами за принципом "digital by default").

Масштабне формування інформаційного суспільства не тільки має позитивні аспекти, але й виводить на передній план проблему забезпечення безпеки інформації, як наслідок, охорони державних, суспільних, приватних інтересів. Так, Законом України «Про основи національної безпеки України» визначено, що на сучасному етапі основними реальними та потенційними загрозами національній безпеці України, стабільності в суспільстві та інформаційній сфері є прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства й держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації (ст. 7) [3].

Як бачимо, нові технології породжують нові глобальні проблеми, однією з яких є поява комп'ютерної злочинності, яка є в переліку, наведеному вище. Саме цей вид злочинної діяльності в сучасних умовах розвитку української державності отримав особливого значення, оскільки Україна живе в той час, коли всі громадяни держави, підприємства, установи, організації є незахищеними перед атаками кіберзлочинців. Ускладняється ситуація також тим, що комп'ютерна злочинність є специфічним різновидом злочинності, якому притаманний високий півень латентності; недостатня увага приділяється дослідженню кримінологічних, криміналістичних, кримінальних процесуальних проблем, пов'язаних з визначенням напряму розслідування, висуненням та відпрацюванням версій, особливостям провадження слідчих (розшукових) дій, дослідженням проблемних питань пошуку та закріпленням доказової інформації. Проте дослідження в цьому напрямі здійснюються. Вказана проблематика була в колі наукових досліджень таких учених, як Д.С. Азаров, М.В. Карчевський, Н.А. Розенфельд, П.Д. Біленчук, Н.І. Клименко, А.В. Іщенко, М.С. Вертузаєв, Т.В. Варфоломеєва. Однак досі залишається багато проблем, які впливають на ефективність розслідування цього виду злочинних дій, повноту, всебічність та об'єктивність дослідження обставин справи.

Одним з таких проблемних питань є питання правильного вилучення електронних носіїв інформації, які були виявлені в рамках розслідування під час проведення слідчих (розшукових) дій. Перш ніж розглядати питання ефективності вилучення електронних

носіїв інформації, слід приділити увагу з'ясуванню сутності поняття «електронний носій».

Електронний носій – це матеріальний носій, який використовують для записування, зберігання та відтворення інформації, обробленої засобами комп'ютерної техніки. До електронних носіїв належать жорсткі диски, флеш-пам'ять, CD-, DVD-, Blue-ray-диски, дискети, касети на магнітній стрічці тощо [4, с. 25].

Наведений перелік ми вважаємо неповним, оскільки технічний прогрес не стоїть на місці, запроваджуються нові технології, виготовляються сучасні технічні пристрої, тому ми пропонуємо розширити список, включивши до нього пластикові карти, електронні записники, відео-регістратори, мобільні телефони, планшети. Таке доповнення ми мотивуємо тим, що вказані технічні пристрої виконують специфічні функції завдяки вмонтованим відеокамерам, фотокамерам, можливостям звукозапису, розширенню можливостей користування мережею Інтернет тощо.

Зазначені носії інформації мають суттєве значення для розслідування й розкриття кримінальних правопорушень, будучи таким джерелом доказів, як документи. Відповідно до ст. 99 КПК України матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (зокрема, електронні) можуть належати до документів, якщо вони спеціально створені задля збереження інформації, містять зафіксовані за допомогою письмових знаків, звуку, зображення відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [5].

Однак за інших обставин такий носій інформації може виступати в ролі іншого джерела, а саме як речовий доказ. Такий висновок ґрунтується на тому, що перераховані вище різновиди електронних носіїв загалом є предметами матеріального світу, тобто речами, які виготовлені для зберігання інформації, її використання, трансформації тощо. В цьому разі критерієм, за яким можна відмежувати речові докази від суміжних джерел, є властивості носія інформації. Якщо електронний носій був використаний як знаряддя злочину (наприклад, на флешці зберігалась вірусна програма, за допомогою якої здійснювалася крадіжка інформації, грошових коштів); якщо він зберіг на собі сліди злочину або інші відомості, які мають доказове значення (наприклад, на CD, який має глянцеву поверхню, можуть бути збережені чіткі відбитки пальців); якщо носій був об'єктом злочинного посягання (наприклад, крадіжка мобільного телефону), електронний носій інформації є речовим доказом. Це питання сьогодні є дискусійним, тому докладніше буде розглядатися в рамках іншого дослідження. Проте до якого б із джерел доказів не належали електронні носії інформації, вони повинні бути виявлені й належним чином зафіксовані.

Найбільш результативними в аспекті виявлення доказової інформації, яка міститься саме на електронних носіях, ми вважаємо такі слідчі (розшукові) дії, як обшук та огляд, під час проведення яких слідчий повинен добре розбиратися в особливостях специфічного кіберпростору, володіти спеціальною термінологією тощо. На жаль, ми можемо констатувати, що сьогодні правоохоронні органи мають дефіцит слідчих, співробітників оперативних підрозділів, які є фахівцями в галузі інформаційно-комунікаційних технологій, а кіберзлочинці, як правило, є висококваліфікованими програмістами.

Крім того, є такі фактори, які ускладнюють розслідування цієї категорії протиправних діянь:

1) недостатнє матеріально-технічне забезпечення підрозділів правоохоронних органів, які розслідують комп'ютерні злочини;

2) відсутність належного рівня співпраці та взаємної поінформованості з правоохоронними органами інших держав, а ця співпраця повинна бути налагоджена, оскільки кіберзлочини мають транснаціональний характер;

3) досить широке коло міністерств та відомств, що становить основу національної системи

кібербезпеки, тому це приводить до не координованості їх дій;

4) складність конструкції правових норм, що впливає на правильну кваліфікацію цього виду злочинів;

5) своєчасність виконання слідчих (розшукових) дій.

Своєчасність виконання слідчих (розшукових) дій також є певною проблемою, оскільки, з одного боку, специфіка цього виду злочинів вказує на те, що будь-яке зволікання є неприпустимим, а з іншого боку, необґрунтований поспіх також може спричинити шкоду, виправити яку може бути складно, а іноді навіть неможливо. Саме тому ми вважаємо, що з моменту отримання оперативної інформації про вчинений злочин і впродовж виконання слідчих (розшукових) дій, в результаті проведення яких може бути отримана доказово значуща інформація, має пройти якомога менше часу, що мінімізує спроби зацікавлених осіб вчинити дії, спрямовані на приховування або знищення важливої для слідства інформації та допоможе слідчому сформувати інформаційну базу, яка створить якісну систему доказів.

Однак реалізацію цього положення ускладнює те, що, як правило, на момент прийняття рішення про початок кримінального провадження слідчий ще не має достатнього обсягу інформації, яка допоможе визначити напрям розслідування, тому слідчому необхідно мати певний час на те, щоб отримати та опрацювати певний обсяг інформації.

Найбільш ефективною в цьому разі є предметна форма фіксації отриманих результатів, яка є вилученням об’єкта в натурі та його консервацією, виготовленням матеріальних моделей (реконструкцією), зокрема макетування, копіювання, одержання відбитків, виготовлення зліпків [6, с. 19]. Отже, ми можемо сформулювати загальні правила, дотримання яких дасть змогу забезпечити ефективність вилучення електронних носіїв інформації та можливість подальшого використання отриманих даних в процесі доказування.

По-перше, особа, яка вилучає електронні носії інформації, повинна мати спеціальні знання, підготовку та навички. По-друге, повинні бути суворо дотримані загальні кримінальні процесуальні та експертні положення. По-третє, вилучення має бути здійснено таким чином, щоб не змінити, не пошкодити або не знищити електронний носій та інформацію, яка на ньому зберігається. По-четверте, всі дії, які мали місце під час виявлення та вилучення електронних носіїв інформації, повинні бути максимально повно задокументовані в процесуальних документах. По-п’яте, експерт, який буде в подальшому проводити дослідження носія інформації, повинен ретельно та акуратно проводити всі необхідні маніпуляції з об’єктом, не допускаючи його змін та несучи за нього відповідальність.

Література

1. Кахович О. О. Розвиток інформаційного суспільства : загрози для людини і держави. *Економічна та інформаційна безпека : проблеми та перспективи* : матеріали Всеукраїнської науково-практичної конференції (14 квітня 2017 року, м. Дніпро). Дніпро : Дніпропетровський державний університет внутрішніх справ, 2017. С. 77–79.
2. Про Концепцію Національної програми інформатизації : Закон України від 4 лютого 1998 року. URL : https ://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80/print.
3. Про основи національної безпеки України : Закон України від 19 червня 1993 року № 964-I. URL : http ://zakon2.rada.gov.ua/laws/show/964-15.
4. ДСТУ 7448 :2013. Інформація та документація. Бібліотечно-інформаційна діяльність. Терміни та визначення понять [Чинний від 2014]. Київ : Мінекономрозвитку України, 2014. 41 с.
5. Кримінальний процесуальний кодекс України від 13 квітня 2012 року. URL : https ://zakon.rada.gov.ua/laws/main/4651-17.

6. Лысов Н. Н. Криминалистическое учение о фиксации доказательственной информации в деятельности по выявлению и раскрытию преступлений : автореф. дисс. … докт. юрид. наук : спец. 12.00.09. Москва, 1995. 31 с.

References

1. Kahovich O. O. (2017), "Development of the information society : threats to the individual and the state", *Ekonomizna ta informaziina bezpeka : problema ta perspektivi* [Economic and Information Security : Challenges and Prospects] : materials of the All-Ukrainian Scientific and Practical Conference (April 14, 2017, Dnipro), Dnipro, pp. 77–79.
2. "On the Concept of the National Informatics Program" : Law of Ukraine of February 4, 1998, available at : https ://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80/print (access November 20, 2019).
3. "On the basics of Ukraine's national security" : Law of Ukraine of June 19, 1993 No. 964-I, available at : http ://zakon2.rada.gov.ua/laws/show/964-15 (access November 18, 2019).
4. DSTU 7448 : 2013. Information and documentation. Library and information activities. Terms and definitions [Effective 2014]. Kyiv : Ministry of Economic Development of Ukraine, 2014. 41 p.
5. The Criminal Procedure Code of April 13, 2012, available at : https ://zakon.rada.gov.ua/laws/main/4651-17 (access November 20, 2019).
6. Lisov, N. N. (1995), "Forensic doctrine on the fixation of evidentiary information in the activity of detection and disclosure of crimes", Thesis abstract for Doct. Sc. (Jurisprudence), 12.00.09, Moscow, Russia.

УДК 343.132:343.144:329.78-058.53 DOI https://doi.org/10.26661/2616-9444-2019-2-10

Особливості допиту підозрюваного – члена молодіжної неформальної групи (об'єднання) під час досудового розслідування

Ларкін М. О.

Запорізький національний університет, вул. Жуковського, 66, м. Запоріжжя, Україна
malark777@ukr.net

Ключові слова:
допит, підозрюваний, молодь, неформальна група, неформальне об'єднання.

Надійшло до редколегії: 19.09.2019
Прийнято до друку: 27.10.2019

Стаття присвячена особливостям проведення допиту підозрюваного – члена молодіжної неформальної групи (об'єднання). Завдяки аналізу емпіричного матеріалу запропоновано рекомендації з проведення зазначеної слідчої (розшукової) дії. Наголошено на тому, що неодмінною умовою проведення допиту підозрюваного-неформала стає підготовка до нього, яка має бути вкрай ретельною. Розглянуто окремі тактичні прийоми, що можуть застосовуватися під час допиту зазначеної категорії осіб. Визначено тактичні ризики, з якими може стикнутися слідчий (прокурор).