УДК 004.9:343.14

ГОВОРУХА В.І., начальник підрозділу Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
СТЕПАНОВ В.А., *кандидат технічних наук,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ ЯК РІЗНОВИД НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Анотація. *Стаття присвячена проблемі зняття інформації з електронних інформаційних систем як різновиду негласних слідчих (розшукових) дій.*
Ключові слова: *негласні слідчі (розшукові) дії, зняття інформації, електронна інформаційна система, спеціальні технічні засоби для зняття інформації з каналів зв'язку, технічні засоби негласного отримання інформації.*

Summary. *The article is devoted to the problem of interception of information from electronic information system as form of covert investigative (search) actions.*
Keywords: *covert investigative (search) actions, interception of information, electronic information system, special technical means for interception of the information from communication channels, technical means for private obtaining of information.*

Аннотация. *Статья посвящена проблеме снятия информации с электронных информационных систем как разновидности негласных следственных (розыскных) действий.*
Ключевые слова*: негласные следственные (розыскные) действия, снятие информации, электронная информационная система, специальные технические средства для снятия информации с каналов связи, технические средства негласного получения информации.*

Постановка проблеми. З метою отримання (збирання) доказів або перевірки вже отриманих доказів у конкретному кримінальному провадженні проводяться слідчі (розшукові) дії.

Різновидом слідчих (розшукових) дій відповідно до ст. 246 Кримінального процесуального кодексу України (далі – КПК України) є негласні слідчі (розшукові) дії, відомості про факт та методи проведення яких не підлягають розголошенню за винятком випадків, передбачених зазначеним кодексом України [1].

До негласних слідчих (розшукових) дій, які передбачають втручання у приватне спілкування, віднесені заходи зі зняття інформації з електронних інформаційних систем (ст. 264 КПК України). Такі дії проводять у разі, якщо відомості про злочин і особу, яка його вчинила, неможливо отримати іншим способом. Вони проводяться на підставі ухвали слідчого судді виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів (ст. 246 КПК України). Водночас, закон не містить визначення заходів зі зняття інформації з електронних інформаційних систем. Тому існує нагальна потреба їх конкретизації, розкриття змістовних ознак цих заходів з урахуванням меж втручання правоохоронних органів у приватне життя.

Результати аналізу наукових публікацій. Після прийняття КПК України 2012 року вивченням різних аспектів інституту негласних слідчих (розшукових) дій займалися такі науковці, як Бандурко О. [2], Галстян Г. [3], Допілка В. [4], Луцик В. [5], Манжай О. [2], Перепелиця М. [2], Тертишник В. [6], Уваров В. [7] та інші.

Праці зазначених науковців, безсумнівно, є вагомим внеском в дослідження цього інституту. Проте, аспекти негласної розшукової дії (далі – НСРД), пов'язаної зі зняттям інформації з електронних інформаційних систем, залишаються не повною мірою висвітленими, а тому потребують додаткового дослідження.

Метою статті є визначення на основі аналізу та узагальнення поняття НСРД "зняття інформації з електронних інформаційних систем".

Виклад основного матеріалу. Таємниця приватного спілкування як частина приватного життя, визнана та гарантована міжнародним законодавством, яке регулює суспільні відносини у галузі прав людини, як невід'ємна складова будь-якого сучасного правового, демократичного суспільства, а також передбачена національним законодавством багатьох країн, у тому числі і України. Під спілкуванням розуміють передавання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою засобів зв'язку будь-якого типу. Спілкування є приватним, якщо інформація передається та зберігається за таких фізичних чи юридичних умов, за яких учасники спілкування можуть розраховувати на захист інформації від втручання інших осіб (ч. 3 ст. 258 КПК України) [1].

У ст. 32 Конституції України передбачено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання і використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Втручання у таємницю спілкування можливе лише на підставі судового рішення, у випадках, передбачених КПК України, з метою виявити та запобігти тяжкому чи особливо тяжкому злочину, встановити його обставини, особу, яка вчинила злочин, якщо іншими способами неможливо досягти мети.

Втручання у приватне спілкування полягає в отриманні доступу до нього та змісту інформації приватного спілкування однієї особи з іншою без відома цих осіб.

Дослідження НСРД "зняття інформації з електронних інформаційних систем" ускладнюється тим, що на даний час в законодавстві України відсутнє визначення самого поняття "електронні інформаційні системи".

Під електронною інформаційною системою слід розуміти взаємозв'язок технічних засобів (комп'ютерів, серверів, апаратно-програмних комплексів, зовнішніх накопичувачів інформації, локальних комп'ютерних мереж та/або інших технічних засобів) з інформаційними технологіями, що реалізують інформаційні процеси та призначені для збору, зберігання, обробки, пошуку, розповсюдження, передачі та надання впорядкованої інформації (даних) в електронному вигляді. В той же час, під частинами електронних інформаційних систем слід вважати бази даних, системи управління базами даних, клієнтське програмне забезпечення, доступ до яких обмежується їх власником, володільцем або утримувачем, зокрема застосуванням системи логічного захисту.

Сутність НСРД "зняття інформації з електронних інформаційних систем" полягає у здійсненні на підставі ухвали слідчого судді пошуку, виявлення і фіксації відомостей, що містяться в електронній інформаційній системі або її частинах, без відома власника, володільця або утримувача системи. Зазначена НСРД проводиться, у разі якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування.

Зняття інформації з електронних інформаційних систем або їх частин може здійснюватися, як шляхом безпосереднього фізичного доступу до них фахівцями уповноважених підрозділів правоохоронних органів, так і шляхом програмного

проникнення. Негласне зняття інформації з засобів електронно-обчислювальної техніки полягає у застосуванні технічних засобів із великими ресурсами оперативної та довгочасної пам'яті, яка забезпечує повне копіювання інформації із жорсткого диску (дисків) та інших електронних носіїв інформації підозрюваного, обвинуваченого. Програмне проникнення до електронних інформаційних систем (їх частин) здійснюється шляхом застосування спеціальних програмних продуктів, які забезпечують подолання системи захисту і копіювання інформації, що обробляється в зазначених системах (їх частинах), на віддалений комп'ютер, що перебуває у користуванні уповноваженого органу, який проводить цю НСРД.

Сукупність таких технічних та програмних засобів для проведення зазначеної НСРД складає окремий вид спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації (далі – СТЗ). Під СТЗ автори розуміють створені або модернізовані та пристосовані з наданням нової якості та властивості технічні засоби, обладнання, інструменти, програмне забезпечення, препарати та інші вироби, які за своєю технічною забезпеченістю або за безпосередньою обумовленістю їх застосування придатні для негласного отримання інформації або доступу до неї у скритний спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення негласних слідчих (розшукових) дій.

Саме застосування СТЗ, на нашу думку, зумовлює уточнення деяких ознак поняття "зняття інформації з електронних інформаційних систем" в контексті НСРД.

Умовно в згаданій НСРД можливо виділити дві функціональні площини:

1) отримання доступу до інформації електронних інформаційних систем шляхом установлення їх логічного або фізичного місцезнаходження, програмного проникнення та/або безпосереднього фізичного (технічного) доступу до них;

2) відбір інформації за визначеними ознаками з електронних інформаційних систем або їх частин шляхом її копіювання, зняття, передачі, фіксації та обробки.

Луцик В.В. всі способи зняття інформації з електронних інформаційних систем об'єднує в дві основні групи: перша – це способи безпосереднього доступу, друга – способи опосередкованого (віддаленого) доступу до комп'ютерної інформації шляхом підключення до лінії телекомунікацій користувача з проникненням в комп'ютерну систему за допомогою підбору паролів або перехоплення імен та паролів користувачів [5, с. 283].

Також до другої групи належить спосіб електромагнітного перехоплення, який дозволяє отримати інформацію без підключення до електронної інформаційної системи, за рахунок перехоплення випромінювань центрального процесора, комунікаційних каналів та інших, а також – знімати і розшифрувати випромінювання працюючого принтера на відстані до 150 м, а випромінювання моніторів – до 500 м [8, с. 161].

Сучасні технології дозволяють оперативно відстежувати діяльність злочинних співтовариств принципово на іншому рівні. Представляє значний інтерес досвід спецслужб США в розробці і застосуванні систем "Oasis" (ЦРУ) і "Magic Lantern" (ФБР), які уможливлюють не тільки контролювати інформаційний обмін злочинних співтовариств, але і "зламувати" комп'ютери підозрюваних, упроваджувати в них "трояни" (програми-віруси, що дозволяють відстежувати інформацію у цьому комп'ютері) тощо [7, с. 940].

Отже, враховуючи функціональні особливості та методи отримання інформації з електронних інформаційних систем, автори виділяють наступні типи СТЗ:

1) засоби для зняття (шляхом фізичного/технічного доступу) інформації з електронних інформаційних систем або з їх частин;

2) спеціалізовані програми для зняття (шляхом програмного проникнення), порушення цілісності, знищення, блокування та/або копіювання інформації з електронних інформаційних систем або з їх частин;

3) закладні пристрої, що розміщують безпосередньо в засобах обчислювальної техніки (USB-портах, системних платах, клавіатурах тощо) або в периферійному обладнанні (модемах, принтерах та інших пристроях);

4) засоби зняття, фіксації та аналізу побічних електромагнітних випромінювань від електронних інформаційних систем;

5) спеціальні засоби для експрес копіювання, руйнування (знищення) інформації з технічних носіїв.

Серед інших особливостей застосування таких СТЗ слід виділити:

- подолання системи логічного захисту електронних інформаційних систем;
- пошук, виявлення, обстеження, відбір, фіксація/копіювання інформації;
- передачу інформації третій стороні (при цьому можуть застосовуватись методи кодування чи шифрування інформації, передача за прискореними алгоритмами, активація за розкладом або за допомогою дистанційного керування, використання радіотехнологій);
- інші дії з інформацією в електронних інформаційних системах (порушення цілісності, знищення, блокування).

Як видно із наведених ознак СТЗ, крім зняття інформації з електронних інформаційних систем, такі засоби дозволяють здійснювати інші дії з інформацією, а саме: порушення цілісності, знищення та блокування.

Ці особливості функціонування СТЗ дають підстави для опису дій із отримання доступу до інформації електронних інформаційних систем в контексті пояснення ознаки “отримання інформації”.

Поняття “знищення інформації”, “блокування інформації”, “порушення цілісності інформації” наведені в Законі України “Про захист інформації в інформаційно-телекомунікаційних системах” [9].

Крім КПК України, визначення поняття “зняття інформації з електронних інформаційних систем” міститься в Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні. Згідно з цією Інструкцією “зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача” полягає в одержані інформації, у тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп’ютерах), автоматичних системах, комп’ютерній мережі [10].

Тертишник В.М., аналізуючи поняття “зняття інформації з електронних інформаційних систем”, виділяє наступні ознаки цього заходу [6]:

1) за своєю архітектурою електронні інформаційні системи можуть бути як локальними, в яких всі їх компоненти (база даних, система управління базою, клієнтське програмне забезпечення) знаходяться на одному комп'ютері, так і розподіленими, в яких компоненти розподілені по кількох комп'ютерах; розподілені даних електронні інформаційні системи, у свою чергу, розділяють на файл-серверні інформаційні системи (в них база даних знаходиться на файловому сервері, а система управління базою даних та клієнтське програмне забезпечення знаходяться на робочих станціях) та клієнт-серверні інформаційні системи (в них база даних та система управління базою даних

знаходяться на сервері, а на робочих станціях знаходиться клієнтське програмне забезпечення);

2) як локальні, так і розподілені електронні інформаційні системи можуть бути відкритими і закритими для громадян, тобто доступ до яких обмежений їх власником, володільцем або утримувачем шляхом розміщення файлових серверів та робочих станцій інформаційної системи у публічно недоступних місцях, житлі чи іншому володінні особи та встановленням систем логічного захисту доступу до електронної інформаційної системи з робочих станцій локальної мережі підприємства, установи, організації тощо, або з робочих станцій, зв'язаних з файловим сервером через мережу Інтернет [6].

У клопотанні слідчого, узгодженому з прокурором, про дозвіл на зняття інформації з електронних інформаційних систем повинні бути вказані ідентифікаційні ознаки електронної інформаційної системи (найменування електронної інформаційної системи, фізична адреса розташування її файлових серверів та робочих станцій або електронна адреса в мережі Інтернет, її власник, володілець або утримувач) та спосіб, яким обмежений доступ до неї [6].

В проекті Закону України "Про оперативно-розшукову діяльність" передбачено, що зняття інформації з електронних інформаційних систем є оперативно-розшуковим заходом, який полягає у негласному пошуку, виявленні шляхом програмного та/або технічного доступу, відборі, фіксації відомостей, що містяться в електронних інформаційних системах або їх частинах, доступ до яких обмежується їх власником, володільцем або утримувачем, чи пов'язаний із подоланням системи логічного захисту [11].

На наш погляд, у цих визначеннях наведені не всі ознаки "зняття інформації з електронних інформаційних систем", зокрема, не згадані такі, як спосіб "негласного отримання інформації"; дія з "доступу до інформації"; дії з отримання інформації "копіювання, зняття, передача, обробка, порушення цілісності, знищення та блокування інформації"; "використання СТЗ".

Висновки.

За результатами аналізу законодавства та інших джерел, вважаємо за доцільне запропонувати таке визначення заходів із зняття інформації з електронних інформаційних систем: *"зняття інформації з електронних інформаційних систем" – заходи, що полягають в негласному доступі до інформації електронних інформаційних систем (установленні їх логічного або фізичного місцезнаходження, програмному проникненні до них та/або встановленні безпосереднього фізичного/технічного контакту з ними та відборі інформації за визначеними ознаками), в отриманні інформації з електронних інформаційних систем або їх частин (копіюванні, знятті, передачі, фіксації та обробки), а також в інших діях з зазначеною інформацією (порушенні цілісності, знищенні або блокуванні), з використанням спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації.*

Уточнення в законодавстві України запропонованого поняття НСРД "зняття інформації з електронних інформаційних систем" сприятиме забезпеченню законності під час її проведення.

Перспективи подальших досліджень зазначеної НСРД вбачаються в удосконалені практичних рекомендацій щодо застосування окремих СТЗ під час її проведення.

Використана література

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.12 р. № 4651-VI. *Відомості Верховної Ради України*. 2013. №№ 9-10, 11-12, 13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 25.07.2020).

2. Оперативно-розшукова компаритівстика: монографія / О.М. Бандурка, М.М. Перепелиця, О.В. Манжай та ін. Харків: Золота миля, 2013. 352 с.

3. Галстян Г.Г. Зарубіжний досвід використання оперативно-технічних засобів. *Науковий вісник Херсонського державного університету. Серія Юридичні науки*. 2018. Т. 2. С. 78-81.

4. Допілка В.О. Контрабанда спеціальних технічних засобів негласного отримання інформації. *Митна справа*. 2012. № 2. С. 45-49.

5. Луцик В.В. Зняття інформації з електронних інформаційних систем. URL: http://www.pravoznavec.com.ua/period/article/3719/% (дата звернення: 21.01.2019).

6. Тертишник В.М. Коментар до Кримінального процесуального кодексу України. Вид. 16-е, доп. і перероб. Київ: Правова Єдність, 2020. 1070 с. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2 (дата звернення: 25.07.2020).

7. Уваров В.Г. Зняття інформації з електронних інформаційних систем: новели КПК України та євро стандарти. *Форум права*. 2012. № 4. С. 939-943. URL: http://arhive.nbuv.gov.ua/e-journals/FP/2012-4/12uvgute.pdf (дата звернення: 25.07.2020).

8. Егорышев А.С. Криминалистический анализ неправомерного доступа к компьютерной информации. *Южно-уральские криминалистические чтения. Межвузовский сборник научных трудов*. 2001. № 9. С. 156-165. URL: http://ndki.narud.ru/library/articles/Egoryshev_AS-Krim_har1.html. (дата звернення: 25.07.2020).

9. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 р. № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

10. Про затвердження Інструкції "Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні": наказ Генеральної прокуратури України, МВС, СБУ, Адміністрації ДПС, Мінфіну, Мінюсту України від 16.11.12 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text (дата звернення: 25.07.2020).

11. Про оперативно-розшукову діяльність: проект закону України від 04.04.17 р. № 6284. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1 (дата звернення: 25.07.2020).

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~