Український Науковий журнал "Інформаційна безпека", 2014, т. 20, випуск 2, с. 176-184.

4. Закон України «Про Службу безпеки України» від 25.03.1992 р. № 2229-XII / Відомості Верховної Ради України, 1992, № 27, ст. 38.

5. [Електронний ресурс]: https://pidruchniki.com/1513061645193/pravo/ rezhim_derzhavnoyi_tayemnitsi.

6. Божков І.І. Державна таємниця та система її охорони. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. №4. 2002. С.7-10 [Електронний ресурс]. Режим доступу: http://pnzzi.kpi.ua/4/04_p7.pdf.

7. Оцінювання ефективності системи охорони державної таємниці: Монографія. О.Є. Архипов, І.Т. Бородавко, В.П. Ворожко. Київ. Вид-во НА СБ України, 2007. 62 с.

8. Пашков А.С. Загальні принципи охорони державної таємниці / Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. Вип. №17. 2009.[Електронний ресурс]. Режим доступу: http://www.nbuv.gov.ua/portal/natural/Znpviknu/ 2009_17/vip17-29.pdf.

9. Кримінальний кодекс України від 05.04.2001 р. № 2341-III / Відомості Верховної Ради України, 2001, № 25, ст. 131.

Матвієнко Є.І., *здобувач вищої освіти факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ*

Науковий керівник:
Телійчук В. Г.*, доцент кафедри оперативно-розшукової діяльності факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, старший науковий співробітник, доцент*

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ОНЛАЙН-ОБШУКУ ЯК РІЗНОВИДУ СЛІДЧИХ ДІЙ В РАМКАХ ЗНЯТТЯ ІНФОРМАЦІЇ З ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Таємне проникнення до електронних інформаційних систем становить собою окремий вид негласних слідчих (розшукових) дій. Спеціальний статус цієї слідчої дії обумовлений тим, що завжди відбувається з втручанням у приватне спілкування, а тому вимагає додаткового обґрунтування при його

здійсненні, яке аргументує неможливість отримання в інший спосіб відомостей про злочин та особу, яка його вчинила.

Правовою підставою для проведення цієї дії в кримінальному процесі є ст. 264 КПК України, в якій закріплено, що пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування [1].

Для врегулювання загальних процедур організації проведення негласних слідчих дій та використання їх результатів у кримінальному провадженні, забезпечення додержання конституційних прав та законних інтересів учасників досудового розслідування, швидкого, повного та неупередженого розслідування злочинів спільним наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Міністерства юстиції України, Міністерства фінансів України, Адміністрації Державної прикордонної служби України No 114/1042/516/1199/936/1687/5 від 16.11.2012 затверджена Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні [2].

Пунктом 1.11.6 Інструкції [2] визначено, що зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача (ст. 264 КПК України) полягає в одержанні інформації, в тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.

Кримінальне процесуальне законодавство прямо не визначає спосіб отримання інформації з електронних цифрових систем, але він може здійснюватися як через фізичний доступ працівника правоохоронних органів, так і через програмне проникнення, тобто, як зазначено нами, онлайн-обшук. Саме зняття інформації з електронних інформаційних систем за допомогою таємного програмного проникнення є набагато складнішою процедурою як із точки зору її виконання, так із точки зору її фіксації.

Слід звернути увагу, що даний вид слідчої дії в тому чи іншому вигляді використовується і в інших країнах Європи. Наприклад, у Франції подібні заходи відображені в кримінальному процесуальному кодексі, але застосовуються лише для розслідування злочинів, які вчинені злочинною організацією, або тяжких злочинів, таких як вбивства, торгівля зброєю, збут наркотичних речовин, педофілія. Дозвіл на застосування даного виду слідчих дій та нагляд здійснює слідчий суддя.

У Німеччині online-обшук не відображений у положеннях кримінального процесуального кодексу, а правовою підставою для його

застосування є лише Закон «Про боротьбу з тероризмом». Компетенція застосування даного виду слідчої діє належить Федеральному відомству кримінальної поліції.

Австрія саме в цьому виді слідчих дій не має жодної регламентаційної норми. Але земельний суд із розгляду кримінальних справ Відня висловив позицію, якою дозволив таємне програмне проникнення, хоча й не в абсолютній мірі. Суд вирішив, що спеціальне програмне забезпечення на комп'ютері особи, по відношенню до якої проводяться відповідні слідчі дії, може робити знімки екрана з певним проміжком часу, які автоматично направляються для аналізу даних співробітникам правоохоронних органів [4].

Але, як уже було зазначено вище, саме фіксація та відображення результатів негласної слідчої дії робить вразливим доказ, отриманий у ході такої слідчої дії. Вимоги до фіксації ходу і результатів негласних слідчих (розшукових) дій закріплені у ст. 252 КПК України. Процесуальними документами щодо проведення негласних слідчих (розшукових) дій є постанови, клопотання, доручення, протоколи уповноваженого співробітника (працівника) оперативного підрозділу, слідчого, прокурора, а також ухвали слідчого судді [1]. Фіксація результатів негласної слідчої (розшукової) дії повинна здійснюватися таким чином, щоб завжди була можливість експертним шляхом встановити достовірність цих результатів. При виявленні відомостей, що мають значення для досудового розслідування й судового розгляду, слідчий негайно складає протокол, в якому відтворює відповідну частину інформації. Хоча нормативно це не передбачено, але правознавці в своїх наукових роботах рекомендують, окрім стандартних процесуальних реквізитів протоколу про проведення слідчої дії, визначених у ст. 104 КПК України [1], зазначати відомості про використане спеціальне програмне забезпечення, за допомогою якого проводилися такі дії.

Серед таких відомостей можуть бути: 1) найменування, виробник та серійний номер програмного забезпечення, за допомогою якого проводилася слідча дія; 2) реквізити та строк дії ліцензійної угоди на використання спеціального програмного забезпечення, за допомогою якого проводилася слідча дія, а також відомості про його сертифікацію в разі наявності; 3) копія спеціального програмного забезпечення, за допомогою якого проводилася слідча дія. Саме ці дані дозволяють у подальшому експертним шляхом встановити достовірність отриманих у ході слідчої дії результатів.

При цьому слід мати на увазі, що згідно зі ст. 62 Конституції України обвинувачення не може ґрунтуватися на припущеннях, а також на доказах, одержаних незаконним шляхом. Докази повинні визнаватися такими, що одержані незаконним шляхом, наприклад, тоді, коли їх збирання й закріплення здійснено або з порушенням гарантованих Конституцією України прав людини і громадянина, встановленого кримінально-процесуальним законодавством порядку, або не уповноваженою на це

особою чи органом, або за допомогою дій, не передбачених процесуальними нормами [3].

У випадку відсутності в протоколі інформації про спеціальне програмне забезпечення, яке використовувалося для проведення відповідних слідчих дій, є підстави для визнання такого доказу недопустимим, а тому він не може бути в подальшому використаний при прийнятті процесуальних рішень і на нього не зможе посилатися суд при ухваленні судового рішення [4].

Таким чином, як ми бачимо правовою підставою для проведення цієї дії в кримінальному процесі є ст. 264 КПК України. Зняття інформації з електронних інформаційних систем за допомогою таємного програмного проникнення є набагато складнішою процедурою як із точки зору її виконання, так із точки зору її фіксації. Зокрема, спираючись на досвід зарубіжнних країни, нами було визначено, що чимало країн застосовують такий вид обшуку, повязаний із зняттям інформаціїї з електронних інформаційних систем.

---

1. Кримінальний процесуальний кодекс України. Редакція від 25.09.2019, URL: https://zakon.rada.gov.ua/laws/show/4651-17.

2. Наказ від 16.11.2012 № 114/1042/516/1199/936/1687/5 «Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні». URL: https://zakon.rada.gov.ua/laws/show/v0114900-12.

3. Конституція України від 07.02.2019, ВВР, 2019, № 9, ст.50.URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

4. Особливості проведення online-обшуку як різновиду слідчих дій // Юридичний вісник України. – 2019. URL: https://lexinform.com.ua/dumka-eksperta/osoblyvosti-provedennya-online-obshuku-yak-riznovydu-slidchyh-dij/.