УДК 343.14:004

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
головний науковий співробітник (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid/0000-0002-2488-7377.
СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.
ORCID: https://orcid/0000-0003-3302-1601.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАХОДІВ З КЛАСИФІКАЦІЇ, ІДЕНТИФІКАЦІЇ ТА ФІКСАЦІЇ КІБЕРЗЛОЧИНІВ

Анотація. *Стаття присвячена аналізу напрямів удосконалення методичного забезпечення експертних досліджень програмних засобів, призначених для негласного доступу до комп'ютерної інформації. В межах статті досліджуються актуальні питання методичного забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів на базі запропонованих методичних підходів у сфері протидії кіберзлочинності.*

Ключові слова*: інформаційна безпека, кібербезпека, кіберзлочинність, комп'ютерний злочин, механізм слідоутворення, шкідливі програмні засоби, спеціальний програмний засіб негласного отримання інформації.*

Summary*. The article is devoted to the analysis of directions of improvement of methodical maintenance of expert researches of the software intended for obtaining covert access to the computer information. Within the limits of the article the topical questions of methodical support of measures on classification, identification and fixing of cybercrimes on the basis of the offered methodical approaches in the field of counteraction to cybercrime are investigated. The approach proposed in the article on the study of software involves the integrated application of various research methods, including methods of monitoring the activity of software and the implementation of appropriate types of expert tasks in computer technical expertise and area of expertise of special technical means of covert access to information. It is noted that one of the important areas of improving the methodological support for combating cybercrime is the introduction of methodological materials to ensure the conduct of expert research on special software designed for obtaining covert access to information. The article concludes that the proposed approaches can serve as a methodological basis for the development of methods, tools and identification technology, fixation of cybercrime in the field of combating cybercrime*

Keywords*: information security, cybersecurity, cybercrime, computer crime, tracing mechanism, harmful software, special software for covert access to information.*

Аннотация*. Статья посвящена анализу направлений усовершенствования методического обеспечения экспертных иследований програмных средств, предназначеных для негласного доступа к компьютерной информации. В рамках статьи исследуются актуальные вопросы методического обеспечения мер по класификации, идентификации и фиксации киберпреступлений на основе предложенных методических подходов в сфере противодействия киберпреступности.*

Ключевые слова*: информационная безопасность, кибербезопасность, киберпреступность, компьютерное преступление, механизм следообразования, вредные програмные средства, специальное программное средство негласного получения информации.*

Постановка проблеми. Кіберзлочинність є сьогодні однією з найгостріших проблем захисту інформаційної безпеки держави. Глибокі зміни, спричинені переходом на цифрові технології, триваюча глобалізація комп'ютерних мереж, розробка новітніх телекомунікаційних пристроїв створюють умови для зростання кіберзлочинності як в Україні, так і за її межами.

Сьогодні більшість фахівців у сфері інформаційних технологій визнають, що ситуація з кіберзлочинністю у світі погіршується. У 2008 році щорічна шкода від кіберзлочинності оцінювалася експертами ОБСЕ приблизно у 100 млрд. доларів [1]. У 2020 році збитки світової економіки від кіберзлочинності оцінювались у $ 1 трлн., що складає понад один відсоток світового ВВП [2].

Революційне зростання кіберзлочинності з використанням сучасних інформаційних технологій на початку XXI століття можна порівняти з появою ядерної зброї, небезпечний руйнівний потенціал якої обумовив впровадження правових підстав її застосування. Масштаб та поява нових способів і методів кіберзлочинів зумовлює потребу подальших досліджень цієї тематики, спрямованих на удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності [3, с. 99].

Актуальність проблем протидії кіберзлочинності в умовах сьогодення потребує розробки криміналістичної теорії стосовно тактики проведення слідчих дій, методик та результативних методів, що спрямовані на збирання та дослідження криміналістичної значимої комп'ютерної інформації [4; 5].

Результати аналізу наукових публікацій. Основи криміналістичної теорії досліджень злочинів у сфері комп'ютерної інформації були закладені відносно недавно (наприкінці 1990-х – початку 2000-х років) у роботах Ю.М. Батурина, О.В. Ботвінкіна [4], В.Б. Вехова, О.П. Войтовича, В.Д. Гавловського [5], В.В. Голубєва [6], В.В. Крилова, С.А. Лапина, В.А. Мещерякова, В.В. Полякова, Н.А. Селиванова, Е.Р. Росинска, А.І. Усов, О.М. Черкуна, О.К. Юдіна та ін.

Особливе значення для криміналістичної теорії й практики мало запровадження в науковий обіг таких нових понять, як віртуальні сліди, електронні докази, формулювання базових принципів слідчих дій [6, с. 64]. При цьому широкий спектр комп'ютерних злочинів відзначається різноманітністю механізмів слідоутворення з можливістю приховання або змін комп'ютерної інформації щодо слідів злочину.

У дослідженні судової комп'ютерно-технічної експертизи значну роль відіграли праці таких вчених, як Е.Р. Росинска та А.І. Усов. У той же час, малодослідженою залишається така важлива окрема криміналістична теорія, як доведення ознак, обставин, способів здійснення злочинів у сфері комп'ютерної інформації.

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 15 березня 2016 року № 96, зазначається, що боротьба з кіберзлочинністю повинна передбачати, зокрема, здійснення заходів з удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень [7]. Це обумовлює актуальність проведення досліджень криміналістичної характеристики злочинів у сфері комп'ютерної інформації, техніко-криміналістичних засобів і методів, тактико-криміналістичних та організаційно-криміналістичних прийомів слідчих дій [4; 8].

Слід підкреслити, що дослідження з позицій криміналістичної теорії зустрічаються зі значними труднощами, обумовленими як складністю цих високотехнологічних злочинів, високим рівнем їх латентності, так і відносно незначною кількістю їх судового

розгляду, що ускладнюють узагальнення слідчої, судової та експертної практики [6]. Є численні невирішені питання в сфері криміналістичної характеристики злочинів, пов'язаних з неправомірним доступом до комп'ютерної інформації, тактики проведення слідчих дій та методики їх експертного дослідження.

Метою статті є удосконалення методичного забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів.

Виклад основного матеріалу. Кіберзброя як інструмент кіберзлочинності характеризується такими ознаками, як цілеспрямованість, вибірковість, розосередженість, швидкість доставки, масштабність та досяжність впливу, комплексність впливу на технічні засоби, системи і людей, регулювання (дозування) "потужності" впливу, що зближує її зі зброєю масового ураження [3, с. 99].

Підвищення результативності протидії кіберзлочинності безумовно потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях [5, с. 110].

Одним із важливих напрямів забезпечення діяльності правоохоронних органів з розслідування кіберзлочинів є удосконалення нормативно-методичного забезпечення слідчих дій та експертних досліджень стосовно кіберзлочинів, зокрема удосконалення методів і технологій ідентифікації та фіксації кіберзлочинів за результатами практики застосування кримінально-правових норм та результатів експертних досліджень у цій сфері [3, с. 99].

Кіберзлочини завжди здійснюються з використанням засобів комп'ютерної техніки. До цих засобів відносяться комп'ютери в різноманітних варіантах їх виконання (ноутбуки, планшети, смартфони, тощо) з використанням телекомунікаційних технологій (бездротові Wi-Fi, Bluetooth, WiMAX тощо), а також комп'ютерне програмне забезпечення як загального використання, наприклад, Opera, Mozilla Firefox, так і програмне забезпечення, використання якого заборонено, наприклад, SpyEye, Zeus, Carberp тощо [9, с. 162].

Як свідчить сучасна практика слідчих дій, в переважній більшості випадків кіберзлочини (кібертероризм, кібершпигунство) здійснюються шляхом віддаленого несанкціонованого доступу до комп'ютерів, комп'ютерних систем, комп'ютерних мереж та мереж електрозв'язку за допомогою комп'ютерної техніки загального використання, на яку встановлюється спеціально розроблене програмне забезпечення, наприклад, Dugu, Wiper, Flame, Gauss, Madi, Narilam [9 с. 164].

Для визначення напрямків напрямків боротьби з кіберзлочинністю слід з'ясувати визначення поняття "кіберзлочинність", появу якого обґрунтовано пов'язують, перш за все, з рівнем її суспільно небезпечних загроз, що пов'язана з розширенням технічної бази інформатизації.

Кіберзлочинність як сукупність кіберзлочинів – суспільно небезпечних винних діянь у кіберпросторі та (або) з його використанням, відповідальність за які передбачена законом України про кримінальну відповідальність та (або) які визнані злочинами міжнародними договорами України [10], є відносно новим антисоціальним явищем, яке швидко прогресує, але його характер і особливості в різних країнах практично не мають істотних відмінностей; етапи та зміст процесу становлення кримінально-правової системи боротьби з кіберзлочинністю в різних країнах практично повторюються [11].

Найбільш поширеним у вітчизняній юридичній літературі є підхід, згідно з яким до кола комп'ютерних злочинів слід відносити всі суспільно небезпечні посягання, при вчиненні яких комп'ютери використовуються як технічні засоби [12; 13]. Звідси випливає, що в основу такої класифікації злочинів покладено ознаки, що

характеризують засоби, які використовуються при їх вчиненні.

Визначення комп'ютерних злочинів як групи посягань, які характеризуються загальними ознаками способу, засобу чи знаряддя, може бути цілком затребуване з позиції криміналістики [13, с. 13]. В межах останньої йдеться про встановлення особливостей методики виявлення, розслідування злочинів цієї категорії, фіксації їх слідів тощо.

Сьогодні в спеціалізованих експертних установах України впроваджені методичні матеріали для забезпечення проведення досліджень носіїв цифрової інформації та комп'ютерної інформації, які використовуються у тому числі й для методичного забезпечення дослідження програмних продуктів, як засобів здійснення комп'ютерних злочинів [14 – 16].

Рекомендовані методи дослідження комп'ютерної інформації та технології контролю активності досліджуваних програмних засобів (далі – ПЗ) можуть бути застосовані для виявлення слідів реалізації його функцій. Встановлення та оцінка сукупності слідів дозволяє відтворити, тобто змоделювати, дії при здійсненні комп'ютерного злочину [17, с. 4].

Враховуючи актуальність питань протидії незаконному обігу спеціальних програмних засобів, призначених для негласного доступу до комп'ютерної інформації (так званих "шпигунських" програм) в ІСТЕ СБ України було розроблено методичні рекомендації для проведення експертних досліджень програмних засобів, призначених для негласного отримання інформації (далі – ПЗ НОІ) [18].

Слід підкреслити, що віднесення програмного засобу до предмету злочину потребує встановлення за результатами дослідження необхідної сукупності ознак та властивостей, які є достатніми для визначення його призначеності для негласного отримання інформації [3, с. 102].

На відміну від вказаних методів дослідження комп'ютерної інформації, дослідження ПЗ НОІ повинно передбачати як аналіз слідів (ознак) реалізації функціоналу програмного засобу, так і безпосереднє дослідження дій комп'ютера чи телекомунікаційного пристрою, на який встановлено програмний засіб, зі визначенням причино-наслідкових зв'язків між виявленими діями з негласного отримання інформації та функціями ПЗ [18].

Розроблення методичних рекомендацій "Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації" базується на критеріях віднесення технічних та програмних засобів до спеціальних технічних засобів негласного отримання інформації та методичних матеріалів зарубіжних і вітчизняних фахівців у сфері комп'ютерно-технічної експертизи [14 – 18].

Новизною методичних рекомендацій є запропонований підхід щодо дослідження ПЗ, який передбачає комплексне застосування різних методів досліджень, зокрема методів контролю активності ПЗ та виконання відповідних видів експертних задач як в галузі комп'ютерно-технічної експертизи, так і в галузі експертизи СТЗ [18].

Предметом експертних досліджень ПЗ є факти й обставини, встановлені при дослідженні використання програмних засобів, що встановлені на технічні засоби загального користування (комп'ютери, телекомунікаційні пристрої тощо), та забезпечують реалізацію інформаційних процесів [8, с. 113].

Аналіз результатів досліджень слідів реалізації функцій ПЗ, дій телекомунікаційного пристрою з негласного отримання інформації, на який встановлено ПЗ, та виявлених причино-наслідкових зв'язків між ними, дає підстави для:

– визначення можливості здійснення негласного отримання інформації з використанням наданого на дослідження програмного засобу;

– віднесення програмного засобу до ПЗ НОІ [18].

Як правило, при проведенні експертного дослідження вирішуються діагностичні та ситуаційні задачі, а також задачі групофікації ПЗ [15; 18].

Вирішення діагностичної задачі спрямовано на:

– встановлення загальної характеристики програмного засобу, з яких файлів та каталогів він складається, їх параметрів (обсяг, атрибути тощо);

– визначення функцій програмного засобу, які забезпечують виконання певних дій з негласного отримання інформації;

– встановлення типів апаратно-програмних платформ, що підтримують функціонування програмного засобу[3, с. 103].

При вирішенні ситуаційної задачі здійснюється зняття процесів (одномоментних станів) у режимі реального часу, встановлення й сприйняття яких можливо тільки з використанням спеціалізованих програмних засобів або в певних умовах (наприклад, у складі певної конфігурації технологічного устаткування, у складі комп'ютерної системи або мережі тощо) [9, с. 113].

Під час аналізу процесів у режимі реального часу виявляються ознаки функціонування спеціального ПЗ: читання/запис даних у файловій системі – створення, видалення, редагування файлів, каталогів; дописування інформації в файл; модифікації пам'яті – створення чи завершення процесів, створення прихованих процесів; зміни реєстру – створення нових записів в реєстрі, редагування або видалення існуючих; зовнішню мережеву активність – отримання чи відсилання інформації через мережу; внутрішню мережеву активність – отримання чи відсилання інформації через localhost; перехоплення хуків клавіатури; відкриття портів; запуск файлів в операційній системі; встановлення чи заміну драйверів [18].

Для виявлення ознак функціонування спеціального програмного засобу використовується спеціалізоване програмне забезпечення, наприклад, ThreatExpert, Process Monitor, Defense Wall HIPS, SafenSoft SysWatch Deluxe. При використанні зазначеного програмного забезпечення застосовується один з трьох основних методів контролю активності ПЗ: HIPS, VIPS та Пісочниця (sandbox) [17].

Проведення досліджень ПЗ в реальних умовах на стадії експертного експерименту спрямовано на визначення оцінки можливостей забезпечення виконання певних дій з негласного отримання інформації та виявлення необхідної сукупності функцій ПЗ, яка є достатньою для застосування його за призначенням.

При цьому дослідження ПЗ може організовуватися на базі технології "клієнт-сервер" телекомунікаційно-інформаційної системи, яка включає пункт управління об'єднаний телекомунікаційною мережею з абонентськими пристроями, на яких здійснюється перехоплення та передача дистанційно встановлених видів інформації [3, с. 104].

Висновок щодо віднесення ПЗ до ПЗ НОІ формується відповідно до встановлених критеріїв, а саме – наявності критеріальних ознак програмного засобу: придатності програмного засобу для негласного отримання інформації та призначеності програмного засобу для його застосування у прихований спосіб, який характерний для оперативно-розшукових заходів [18].

Запропонований в рекомендаціях метод аналізу виявлених слідів реалізації функцій ПЗ дозволяє з'ясувати спосіб функціонування ПЗ, його властивості з негласного

отримання інформації, а також визначити, в кінцевому підсумку, призначеність програмного засобу [18].

У свою чергу, аналіз та узагальнення результатів експертних досліджень надає можливість визначення ключових елементів криміналістичної характеристики кіберзлочинів, що здійснюються із застосуванням спеціальних програмних засобів, призначених для негласного доступу до комп'ютерної інформації, а саме: значущі ознаки ПЗ, спосіб його використання, механізм слідоутворення та типові сліди реалізації функцій ПЗ.

Висновки.

Актуальність проблеми протидії кіберзлочинності в умовах сьогодення потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях.

Одним із важливих напрямів удосконалення методичного забезпечення протидії кіберзлочинності є впровадження методичних матеріалів для забезпечення проведення експертних досліджень спеціальних програмних засобів, призначених для негласного отримання інформації [9, с. 114].

Аналіз та узагальнення результатів експертних досліджень можуть бути використані для визначення криміналістичної характеристики кіберзлочинів, що здійснюються із застосуванням спеціальних програмних засобів, призначених для негласного доступу до комп'ютерної інформації.

Запропоновані підходи можуть слугувати методичним підґрунтям для розробки методів, засобів і технологій ідентифікації, фіксації кіберзлочинів у сфері протидії кіберзлочинності.

Використана література

1. Киберпреступность страшнее финансового кризиса. URL: https://www.crime-research.ru/news/03.12.2008/50 (дата звернення: 03.01.2021).

2. Кіберзлочинці у 2020 році завдали у світі збитків на трильйон доларів – дослідження. URL: https://www.unn.com.ua/uk/news/1906706-kiberzlochintsi-u-2020-rotsi-zavdali-u-sviti-zbitkiv-na-trilyon-dolariv-doslidzhennya (дата звернення: 19.02.2021).

3. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. *Інформація і право*. № 4(31)/2019. С. 98-106.

4. Ботвінкін О.В. Проблеми забезпечення національної безпеки в інформаційній сфері. *Юридичний журнал.* 2007. № 2. С. 59-60.

5. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. № 1(28)/2019. С. 108-117.

6. Голубєв В.О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту.* 1997. № 2. С. 35-40.

7. Стратегія кібербезпеки України: Указ Президента України від 15.03.16 р. № 96. URL: https://www.president.gov.ua/documents/962016-19836. (дата звернення: 21.02.2020).

8. Серьогін В.С., Леонов Б.Д. Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов'язаних з неправомірним дистанційним доступом до комп'ютерної інформації. *Інформація і право*. № 2(21)/2017. С. 108-115.

9. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений: доклады ТУСУРа. 2014. № 2(32). Барнаул: Изд-во Алт. ун-та, 2014. С. 162-165.

10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.

11. Баранов О.А. Кримінологічні проблеми комп'ютерної злочинності. URL: http://www.bezpeka.com/ru/lib/spec/crim/art71.html

12. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні: монографія. Харків: Панов, 2016. 212 с.

13. Карчевский Н.В. "Киберпреступление" или преступление в сфере использования информационных технологий?: матеріали всеукр. наук.-практ. конф. *Кібербезпека в Україні: правові та організаційні питання,* м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. С. 10-14.

14. Дослідження інформації на цифрових носіях (методика): звіт про науково-досліду роботу / С.М. Бобрицький, О.В. Чишкало та ін. Харків. ХНДІСЕ. 2009. 2009. 34 с.

15. Методика дослідження комп'ютерної інформації / К.Ю. Усков, О.М. Пешехонова, Ю.М. Бєляк, В.А. Кореньок, А.О. Ружинський. Київ: КНДІСЕ. 2005. 37 с.

16. Розробка спеціальних програмних засобів для проведення судових експертиз комп'ютерних мереж / О. Башкатов, Г. Дружинін та ін. Донецьк: ДНДІСЕ. 2010. 179 с.

17. Войтович О.П., Вітюк В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. *Інформаційні технології та комп'ютерна інженерія*. 2013. № 3. С. 4-9.

18. Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації: методичні рекомендації. Київ: ІСТЕ СБУ. 2016. 31 с.

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