УДК 343.14:004

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України
СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України

УДОСКОНАЛЕННЯ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ СПЕЦІАЛЬНИХ ПРОГРАМНИХ ЗАСОБІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *Стаття присвячена аналізу проблем експертного забезпечення правоохоронної діяльності у сфері протидії кіберзлочинності. В межах статті досліджуються проблемні питання розробки методичних матеріалів для проведення експертних досліджень спеціальних програмних засобів. Запропоновані перспективні напрями подальших наукових досліджень протидії кіберзлочинності, модернізації та вдосконалення методик проведення експертних досліджень спеціальних програмних засобів.*

Ключові слова: *кіберзлочинність, механізм слідоутворення, шкідливі програмні засоби, спеціальний програмний засіб негласного отримання інформації.*

Summary. *The article is devoted to the analysis of the problems of expert support for activities in law enforcement in the field of countering cyber crime. The article examines the problematic issues of the development of methodological materials for the conduct of expert studies of special software. Prospective directions for further research of the problem of countering cyber crime, upgrading and improving the methods of conducting expert studies of special software have been proposed.*

Keywords: *cyber security, tracing mechanism, harmful software, special software for covert obtaining of information.*

Аннотация. *Статья посвящена анализу проблем экспертного обеспечення правоохранительной деятельности в области противодействия киберпреступности. В рамках статьи исследуются проблемные вопросы разработки методических материалов для проведения экспертных исследований специальных программных средств. Предложены перспективные направления дальнейших научных исследований противодействия киберпреступности, модернизации и совершенствования методик проведения экспертных исследований специальных программных средств.*

Ключевые слова: *кибербезопасность, механизм следообразования, вредные програмные средства, специальное программное средство негласного получения информации.*

Постановка проблеми. Сьогодні стрімкий розвиток інформаційних технологій, масштаб застосування глобальних телекомунікаційних мереж, розробка новітніх телекомунікаційних пристроїв створює умови для зростання злочинності у сфері комп'ютерної інформації як в Україні, так і за її межами.

Кіберзлочинність, що пов'язана з використанням інформаційних технологій, комп'ютерних систем та мереж, здатна продукувати такі наслідки, які за масштабом наближаються до техногенної катастрофи чи економічної кризи. У 2008 році щорічна шкода від кіберзлочинності оцінювалася експертами ОБСЄ приблизно у 100 млрд. доларів [1]. Сьогодні ж збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн. на рік, а за негативним сценарієм у 2019 році вони сягатимуть $ 2 трлн. [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.

Отже, кіберзлочинність є сьогодні однією з найгостріших проблем інформаційної безпеки держави.

Результати аналізу наукових публікацій. Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська [3], Ю.М. Батурин [4], П.Д. Біленчук [5], О.В. Ботвінкін [6], В.Д. Гавловський [7], В.О. Голубєв [8], М.В. Карчевський [10; 11], В.В. Поляков [11], М.О. Кравцова, О.М. Литвинов [12], Ю.Ю. Нізовцев [13], Б.В. Романюк [14], О.Р. Росинська [15], Т.Л. Тропіна [16], О.М. Черкун, О.К. Юдін [17] та інші.

Вагомий внесок у розроблення методів, засобів і технологій ідентифікації та фіксації кіберзлочинів внесено дослідженнями, проведеними зарубіжними вченими. Це праці Д. Айкова, К. Сейгера, У. Фонсторха [18], К. Брайана [19] та С. Бренера [20].

Водночас, слід відзначити, що в більшості публікацій, присвячених питанням кіберзлочинності, мають місце неоднозначні судження, різні точки зору, істотні розбіжності між поглядами дослідників з питань методичного забезпечення розслідування комп'ютерних злочинів.

Незважаючи на значну кількість публікацій, що вийшли останнім часом, присвячених проблемам протидії комп'ютерній злочинності, більшість дослідників основну увагу приділяють загальним кримінально-правовим та криміналістичним аспектам цієї проблеми.

Практично не досліджена така важлива галузь теорії, як доведення ознак, обставин, способів вчинення злочинів у сфері комп'ютерної інформації для їх фіксації та ідентифікації, що має важливе значення для розробки методик забезпечення експертних досліджень кіберзлочинів [12, с. 210; 14].

Сьогодні масштаб та рівень кіберзлочинності, 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.

Метою статті є удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності.

Виклад основного матеріалу. Інформаційна зброя 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.

Підвищення результативності протидії кіберзлочинності безумовно потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях [7, 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, що охороняють інформацію в комп'ютерних системах та телекомунікаційних мережах.

Широкий спектр технологій вчинення кіберзлочинів відзначається різноманітністю механізмів слідоутворення з можливістю приховування або змін комп'ютерної інформації щодо слідів злочину, що, в кінцевому результаті, визначають їх високу латентність [17, с. 176].

Зазначені чинники, а також складність виявлення та фіксації комп'ютерної інформації щодо типових слідів здійснення злочинів, встановлення механізму слідоутворення, способу вчинення злочину ускладнюють процес формування криміналістичної характеристики кіберзлочинів та взагалі методів і технологій їх ідентифікації.

В сучасній криміналістиці дослідження застосовуваних засобів та технологій для вчинення кіберзлочинів, їх приховування не досягли практично значущих результатів, які б дозволили розробити як тактико-криміналістичні рекомендації з розслідування таких злочинів, так і методики експертних досліджень у цій сфері [11, с. 162].

Кіберзлочини завжди здійснюються з використанням засобів комп'ютерної техніки. До цих засобів відносяться комп'ютери в різноманітних варіантах їх виконання (ноутбуки, планшети, смартфони, тощо), комп'ютерні технології (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 [11, с. 162].

Слід зазначити, що важливу роль при вчиненні сучасних кіберзлочинів виконує саме спеціально розроблене програмне забезпечення.

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 спеціальне програмне забезпечення, наприклад, Dugu, Wiper, Flame, Gauss, Madi, Narilam [11, с. 164].

Зауважимо, що шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку є предметом злочину, передбаченого ст. 361-1 "Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут" КК України.

До речі, питання щодо співвідношення понять "предмет" і "засоби або знаряддя вчинення злочину" кримінально-правовою науковою не зовсім вирішене, оскільки матеріальні утворення, що не підпадають під поняття "предмет злочину", належать не до об'єкта, а до об'єктивної сторони складу злочину. Основним універсальним критерієм відмежування "предмет злочину" від поняття "знаряддя та інші засоби вчинення злочину" дослідники цієї проблеми визнають те, що засоби – це речі, за допомогою яких суб'єкт прагне досягти злочинного результату. Предмет сам піддається злочинному впливу [21, с. 137]. Обов'язковою ознакою предмету розглядуваного злочину є те, що за своїм призначенням шкідливі програмні засоби мають несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Відсутність цієї ознаки виключає можливість визнати вказані програмні чи технічні засоби як предмет злочину, передбаченого ст. 361-1 КК України [10].

Несанкціоноване втручання в роботу комп'ютерів, комп'ютерних систем чи мереж, слід розуміти, як проникнення до цих комп'ютерів, систем чи мереж, злом їх засобів програмно-апаратного захисту інформації, отримання доступу до управління

комп'ютером, комп'ютерної системи чи мережі, а також до комп'ютерної інформації, що може призвести до витоку, втрати, підробки, блокування цієї інформації, спотворення процесу обробки інформації в комп'ютері, комп'ютерних системах чи мережах, без дозволу (згоди) відповідного власника або уповноважених ним осіб [10].

Злочин, передбачений ч. 1 ст. 361-1 КК України, є злочином з формальним складом, тому для наявності його об'єктивної сторони не потрібно встановлювати настання суспільно небезпечних наслідків [10].

Наведені чинники, а також складність виявлення та фіксації слідів несанкціонованого проникнення до комп'ютерів, систем чи мереж, злому їх засобів програмно-апаратного захисту інформації ускладнюють формування методів ідентифікації шкідливих програмних засобів та методичного забезпечення їх експертних досліджень.

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 засобів [22 – 25]. Зазначені методики, а також методичні рекомендації зарубіжних вчених [18 – 20] передбачають єдиний методичний підхід до процесів огляду, фіксації стану речових доказів (збереження, копіювання даних, що знаходяться на наданих на дослідження носіях інформації) та дослідження цифрової інформації, що розміщується на них, оформлення матеріалів експертного дослідження. При цьому, рекомендовані методи дослідження комп'ютерної інформації та технології контролю активності досліджуваних програмних засобів (далі – ПЗ) можуть бути застосовані для виявлення слідів реалізації його функцій [25].

Встановлення та оцінка сукупності слідів дозволяє виявити функції шкідливого програмного засобу, що забезпечують здійснення несанкціонованого доступу до управління комп'ютером та комп'ютерної інформації [23; 25].

Такий підхід дозволяє вирішити діагностичну задачу при проведенні досліджень ПЗ, яка спрямована на встановлення загальної характеристики програмного засобу та визначення його недокументованих функцій, які забезпечують виконання злочинних дій.

На жаль, сьогодні практично не досліджено такий важливий розділ криміналістичної теорії, потенціал якого пояснює підходи щодо доведення ознак (типових слідів несанкціонованого втручання), способів несанкціонованого втручання в роботу комп'ютерів, комп'ютерних систем чи мереж (проникнення до цих комп'ютерів, систем чи мереж, злом їх засобів програмно-апаратного захисту інформації), що має важливе значення для визначення призначеності програмних засобів та їх належності до шкідливих програмних засобів.

Під час розробки методів ідентифікації та фіксації кіберзлочинів слід враховувати особливості функціональних можливостей різноманітних шкідливих програмних засобів (далі – ШПЗ) та їх класифікацію.

З точки зору криміналістики дослідження засобів вчинення кіберзлочинів, їх типізація та класифікація дозволять встановити причинові зв'язки між обставинами, що підлягають встановленню та доведенню під час слідчих дій та експертних досліджень [11, с. 162-163].

Сьогодні найбільш поширеною є розроблена на базі запропонованої "Лабораторією Касперського" класифікація, яка сформована з урахуванням особливостей функціональних можливостей ШПЗ, котрі визначають технологію їх застосування [10, с. 512].

Зазначена класифікація спрямована на забезпечення функціонування засобів програмно-апаратного захисту інформації, що циркулює в комп'ютерах, комп'ютерних системах, мережах та мережах електрозв'язку.

За технологією застосування виділяють такі види шкідливих програмних засобів: класичні комп'ютерні віруси; мережеві черв'яки; трояни; руткіти.

До окремого підвиду ШПЗ належить шпигунське програмне забезпечення (Spyware), яке призначене для незаконного віддаленого доступу до управління комп'ютером та комп'ютерної інформації.

За результатами аналізу шляхів еволюції їх застосування можна дійти висновку, що сучасні ШПЗ – це високотехнологічні програмні засоби, що спеціально розробляються для застосування іноземними спецслужбами, в якості кіберзброї, при проведенні спецоперацій за конкретними об'єктами посягання [13, с. 232].

При цьому вибір засобів для здійснення кіберзлочинів звичайно залежить від цілого ряду факторів: технологічної інфраструктури об'єкта посягання та прийнятого на ньому режиму охорони (застосовуваних технічних і організаційних засобів охорони, програмно-апаратного захисту інформації). Сучасні ШПЗ розробляються за цільовим призначенням як програмні комплекси, що складаються з взаємопов'язаних програмних додатків, які забезпечують виконання функціональних завдань на певних стадіях підготовки до вчинення злочину, безпосередньо при його здійсненні та при приховуванні злочину, наприклад, Stuxnet, BlackEnergy [11, с. 164].

Тому одним з пріоритетних напрямів протидії кіберзлочинності, зокрема запобігання застосуванню іноземними спецслужбами високотехнологічних програмних засобів, вважається здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на запобігання та припинення злочинної діяльності щодо створення, розповсюдження або збуту зазначеного спеціального програмного забезпечення.

Органи досудового розслідування, особливо на первісному етапі розслідування комп'ютерних злочинів, рідко мають вичерпні відомості про засоби, що використовуються під час вчинення злочину.

За відсутності такої інформації важливу роль для проведення розслідування має класифікація спеціальних програмних засобів, яка може бути сформована з урахуванням криміналістичної характеристики схожих злочинів. Її практичне значення, що проявляється в кореляційному взаємозв'язку між структурними елементами злочину, дає підстави для підготовки слідчих версій за наявності лише неповних отриманих даних [11, с. 163].

Отже, одним з актуальних досліджень нормативно-методичного забезпечення протидії кіберзлочинності є розробка класифікації спеціальних програмних засобів, яка сформована з використанням криміналістичної характеристики схожих злочинів.

Враховуючи актуальність питань протидії незаконному обігу спеціальних програмних засобів (так званих "шпигунських" програм), які дозволяють ефективно здійснювати дії з віддаленого доступу та негласного отримання інформації з абонентських та інших телекомунікаційних пристроїв телекомунікаційних мереж, в ІСТЕ СБ України було розроблено методичні рекомендації для проведення експертних досліджень програмних засобів, призначених для негласного отримання інформації (далі – ПЗ НОІ) [26].

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

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, з визначенням причинових зв'язків між виявленими діями з негласного отримання інформації та функціями ПЗ [26].

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 [19; 20; 22 – 25].

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 [26].

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

Аналіз результатів досліджень слідів реалізації функцій ПЗ, дій телекомунікаційного пристрою з негласного отримання інформації, на який встановлено ПЗ, та виявлених причинових 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 [26].

Під об'єктом експертних досліджень ПЗ слід розуміти прикладне програмне забезпечення, що знаходиться на наданих носіях інформації, або інстальоване на технічних засобах загального користування, а також інформаційні процеси, які обумовлені функціонуванням зазначених технічних засобів загального користування.

При цьому залишається задача дослідження ПЗ за відсутності вихідних кодів, що значно ускладнює роботу дослідника [25].

Як правило, при проведенні експертного дослідження вирішуються діагностичні та ситуаційні задачі, а також задачі групофікації ПЗ. При проведенні досліджень ПЗ діагностичні задачі спрямовані 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.

Серед ситуаційних задач виділяється 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).

Під час виявлення ознак функціонування спеціального програмного засобу на підставі аналізу процесів у режимі реального часу звертається увага на:

– 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 [26].

Для виявлення ознак функціонування спеціального програмного засобу, інстальованого на технічних засобах загального користування, 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) [25]. Найбільш часто застосовується метод контролю активності ПЗ HIPS, який має наступні переваги:

– низьке споживання системних ресурсів;

– невимогливі до апаратного забезпечення ПК (можуть працювати на різних платформах);

– можливість визначення загроз нульового дня;

– можливість визначення руткітів, які працюють в режимі користувача.

Технологія HIPS – це технологія контролю активності, заснована на перехопленні звернень до ядра ОС і блокуванні виконання потенційно небезпечних дій ПЗ, яке працює в режимі користувача, виконуваних без відома користувача [25]. За допомогою власного драйвера перехоплює всі звернення ПЗ до ядра ОС. У разі спроби здійснення потенційно небезпечної дії з боку ПЗ, HIPS-система блокує виконання даної дії і запитує користувача, який вирішує дозволити або заборонити виконання цієї дії.

При проведенні досліджень ПЗ на стадії експертного експерименту вирішення ситуаційної задачі полягає в оцінці можливостей виконання певних дій з негласного отримання інформації та виявлення необхідної сукупності функцій ПЗ, які є достатніми для визначення його функціонального призначення.

Дослідження програмного засобу в реальних умовах його функціонування може бути організовано 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.

Експертні задачі на стадії порівняльного дослідження ПЗ спрямовані на встановлення його групової належності до спеціальних програмних засобів, призначених для негласного отримання інформації (як різновиду спеціальних технічних засобів негласного отримання інформації).

Запропонована в методичних рекомендаціях процедура аналізу виявлених функцій ПЗ з урахуванням встановлених в методичних рекомендаціях суттєвих ознак (функціональних можливостей) ПЗ НОІ дозволяє з'ясувати спосіб функціонування ПЗ, його властивості з негласного отримання інформації, а також визначити, в кінцевому підсумку, призначеність програмного засобу [26].

Висновок щодо віднесення ПЗ до ПЗ НОІ формується відповідно до встановлених критеріїв, а саме – наявності загальних (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 [26; 27].

Висновки.

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

Проблема удосконалення методичного забезпечення правоохоронної та експертної діяльності в сфері боротьби з кіберзлочинністю зумовлює необхідність розробки класифікації кіберзлочинів, тактики проведення слідчих дій з їх розслідування та фіксації, методик та ефективних методів, спрямованих на удосконалення ідентифікації спеціального програмного забезпечення, що призначено для незаконного віддаленого доступу до управління комп'ютером та комп'ютерної інформації. 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.

Запропоновані рекомендації експертного дослідження програмних засобів, критерії їх віднесення до ПЗ НОІ можуть слугувати підґрунтям для розробки методик проведення судових експертиз спеціальних програмних засобів незаконного віддаленого доступу до управління комп'ютером, комп'ютерної системи чи мережі, негласного отримання інформації, а також удосконалення методів їх ідентифікації.

Використана література

1. Киберпреступность страшнее финансового кризиса. URL: https://www.crime-research.ru/news/03.12.2008/50 (дата звернення 03.05.2019).

2. Киберпреступники наживаются на самых бедных. URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief.html (дата звернення 19.02.2019).

3. Ахтирська Н. Форми протидії розслідуванню злочинів, вчинених у сфері комп'ютерних технологій. *Юридичний журнал*. 2002. № 3(9). С. 60-64.

4. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. Москва: Юридическая литература, 1991. 157 с.

5. Біленчук П.Д., Бут В.В., Гавловський В.Д., Гуцалюк М.В., Колпак Р.Л. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.

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

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

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

9. 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.

10. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.

11. 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.

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

13. Нізовцев Ю.Ю. Еволюція шкідливих програмних засобів та аналіз тенденцій небезпеки їх застосування: *зб. наукових праць Національної академії СБ України*. 2017. № 65. С. 230-238.

14. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій. Київ: Вид. Поливода А.В., 2004. 144 с.

15. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая експертиза. Москва: Право и закон, 2001. 416 с.

16. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т.Л. Тропина: дис. …канд. юрид. наук: спец. 12.00.08. Владивосток, 2005. 235 с.

17. Юдин О.К. Інформаційна безпека. Нормативно-правове забезпечення. Киів, 2010. 708 с.

18. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Москва: Мир, 1999. 351 с.

19. Для профессионалов криминалистический анализ файловых систем / под ред. Брайана Кэрриэ. С-Пб.: Питер, 2007. 480 с.

20. Brenner S. Cybercrime: criminal threats from cyberspace. Praeger, 2006. 281 p.

21. Кримінальне право України: заг. частина. гл. 7/ за ред. проф. В.В. Сташиса, В.Я. Тація. Харків: Право, 2010. 449 с.

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

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

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

25. 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.

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

27. Методика віднесення об'єктів до спеціальних технічних засобів негласного отримання інформації. Київ: ІСТЕ СБУ. 2011. 26 с.

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