УДК 343.14: 004

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

ОКРЕМІ ПРОБЛЕМИ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ’ЯЗАНИХ З НЕПРАВОМІРНИМ ДИСТАНЦІЙНИМ ДОСТУПОМ ДО КОМП’ЮТЕРНОЇ ІНФОРМАЦІЇ

***Анотація**. У статті розглядаються аспекти криміналістичної характеристики комп’ютерних злочинів та проблемні питання розробки методичних матеріалів для проведення експертних досліджень спеціальних програмних засобів, призначених для негласного отримання комп’ютерної інформації.*

***Ключові слова:** комп’ютерна інформація, комп’ютерні злочини, розслідування.*

***Аннотация.** В статье освещаются аспекты криминалистической характеристики компьютерных преступлений и проблемные вопросы разработки методических материалов для проведения экспертных исследований специальных программных средств, предназначенных для негласного получения компьютерной информации.*

***Ключевые слова:** компьютерная информация, компьютерные преступления, расследование.*

***Summary.** The article considers aspects of the forensic characteristics of computer crimes and the problematic issues of developing methodological materials for conducting expert studies of special software intended for covert obtaining computer information.*

***Keywords:** computer information, computer crime, investigation.*

Постановка проблеми. На сьогодні одночасно з стрімкими процесами інформатизації суспільства спостерігається суттєве підвищення рівня та масштабів загроз інформаційній безпеці держави. Радикальні зміни в інформаційних стосунках у всіх сферах діяльності людини, суспільства та держави передусім пов’язані із застосуванням глобальних телекомунікаційно-інформаційних мереж, в першу чергу, мережі Інтернет.

Результати аналізу наукових публікацій. Мережа Інтернет, як принципово відкрита система, забезпечує вільний і анонімний доступ до інформаційних ресурсів, що надає різноманітні можливості правопорушень, пов’язаних з неправомірним доступом до комп’ютерної інформації [1 – 2]. Злочинність у цій сфері отримала назву “комп’ютерна”, а останнім часом поширюється термін “кіберзлочинність”, що повніше охоплює об’єкти посягання цього виду злочинів. Останні швидкими темпами поширюються, у звязку з розповсюдженням багатофункціональних апаратно-програмних засобів, що можуть бути використані для несанкціонованого доступу до телекомунікаційних та комп’ютерних мереж. Поряд із застосуванням традиційних засобів здійснення комп’ютерних злочинів спостерігається стала тенденція розповсюдження спеціальних програмних засобів, призначених для неправомірного дистанційного доступу та негласного отримання інформації з абонентських пристроїв телекомунікаційних мереж, комп’ютерних систем [1; 6].

За даними Інтерполу, у 2000 р. доходи злочинців, в основному організованих злочинних груп, пов’язані з використанням новітніх технологій, посіли третє місце у світі після доходів від торгівлі наркотиками і зброєю [3]. Ці обставини призвели до різкого загострення кримінальної обстановки в інформаційній сфері. У зв’язку з цим Рада Європи 23 листопада 2001 р. схвалила Конвенцію “Про кіберзлочинність”, у якій передбачені основні засади та напрями міжнародної співпраці у цій діяльності, а саме: збереження протягом визначеного терміну комп’ютерних даних, у т.ч. на території інших країн – можливих їх користувачів, термінове розкриття за необхідності збереження даних, взаємна допомога у збиранні даних про рух інформації, її перехоплення тощо. В ЄС, а також в провідних європейських країнах (Австрія, Іспанія, Нідерланди, Польща, Угорщина, Фінляндія) прийняті стратегії кібербезпеки.

Складність інформаційних технологій та безмежна сфера їх використання при здійснені комп’ютерних злочинів зумовлюють подальшу потребу дослідження криміналістичної характеристики комп’ютерних злочинів, вдосконалення існуючого механізму захисту інформаційних ресурсів в кіберпросторі, забезпечення відповідної профілактичної діяльності [2, с. 257; 4].

Основи криміналістичної теорії досліджень злочинів у сфері комп’ютерної інформації були закладені відносно недавно (наприкінці 90-х – початку 2000-х років) у роботах Н.М. Ахтирської, Ю.М. Батурина, П.Д. Біленчука, В.Б. Вехова, В.Д. Гавловського, В.О. Голубєва, М.В. Гуцалюка, В.Е. Козлова, В.В. Крилова, В.А. Мещерякова, А.Л. Осипенко, В.Ю. Рогозіна, О.Р. Росинської, Н.А. Селиванова, О.М. Черкуна, О.К. Юдіна й інших авторів.

Серед закордонних досліджень потрібно згадати методичні матеріали з розслідування комп’ютерних злочинів Д. Айкова, К. Сейгера, У. Фонсторха та К. Брайана.

Важливий внесок зробили Е.Р. Россинска і А.І. Усова, які заклали наукові основи для проведення такого нового виду інженерно-технічних експертиз, як комп’ютерно-технічні експертизи. Особливе значення для криміналістичної теорії й практики мало введення таких нових понять, як віртуальні сліди, електронні докази, формулювання базових принципів слідчих дій [5, с. 64].

Водночас, серед дослідників немає єдності поглядів з питань розслідування комп’ютерних злочинів. Це стосується як тлумачення термінів, визначення криміналістичної характеристики злочинів у сфері комп’ютерної інформації, так і вироблення техніко-криміналістичних засобів і методів, тактико-криміналістичних і організаційно-криміналістичних прийомів та формулювання рекомендацій з розслідування цих злочинів.

Не применшуючи теоретичну та практичну значимість проведених досліджень цієї теми, варто зазначити, що вони не вичерпують усіх криміналістичних аспектів розслідування злочинів, пов’язаних з неправомірним дистанційним доступом до комп’ютерної інформації.

Метою статті є удосконалення методичного забезпечення розслідування комп’ютерних злочинів.

Виклад основного матеріалу. Комп’ютерні технології та міжнародні інформаційно-комунікаційні мережі створили нові умови, які сприяють вчиненню злочинів як на національному, так і на міжнародному рівні. Організовані злочинні утворення у повному обсязі використовують нові технології для відмивання коштів, отриманих злочинним шляхом, поширення неправдивої інформації, несанкціонованого доступу до інформаційних систем, вчинення інших правопорушень в цій сфері. Загроза комп’ютерної злочинності полягає і в тому, що вона надає значну матеріальну

підтримку організованій злочинності для вчинення насильницьких злочинів, зокрема, терористичних актів. На окрему увагу заслуговують злочинні посягання, що здійснюються за допомогою спеціальних програмних засобів, так званих “шпигунських” програм, призначених для негласного віддаленого доступу до інформаційно-телекомунікаційних мереж і отримання комп’ютерної інформації. Ці злочинні дії в останні роки стали домінуючими серед інших категорій комп’ютерних злочинів [8].

Розслідування комп’ютерних злочинів стикається зі значними труднощами, зумовленими складністю виявлення цих високотехнологічних злочинів, високим рівнем їх латентності, недосконалістю статистичного обліку комп’ютерних злочинів, що ускладнюють узагальнення слідчої, судової та експертної практики [6].

Зауважимо, що високий рівень латентності цих злочинів викликає серйозні негативні наслідки. Вона створює сприятливу психологічну обстановку для вчинення нових злочинів, сприяє формуванню стійких злочинних утворень, порушує принцип невідворотності покарання, знижує превентивну функцію кримінального закону, погіршує моральний клімат в державі.

Серед шляхів подолання латентності комп’ютерної злочинності виділяють розробку криміналістичної характеристики злочинів у сфері високих технологій, а також подальшу роботу з вироблення методичних рекомендацій з виявлення, розкриття злочинів у сфері високих технологій [3].

Існують численні невирішені питання в сфері криміналістичної характеристики комп’ютерних злочинів, тактики проведення слідчих дій. Практично не досліджена така важлива галузь теорії, як доведення ознак, обставин, способів здійснення злочинів у сфері комп’ютерної інформації, що має важливе значення для розробки методик забезпечення експертних досліджень комп’ютерних злочинів. Як наслідок, недостатня розробленість криміналістичної теорії не дозволяє створити надійну наукову основу для методичного забезпечення криміналістичної діяльності правоохоронних органів [2; 3].

Особливе значення при цьому має формування поняття “криміналістична характеристика комп’ютерних злочинів”, зміст якого має враховувати положення криміналістичної теорії та її методики. Доречно зазначити, що криміналістична характеристика комп’ютерних злочинів є сукупністю криміналістичної, найбільш характерної, значущої та взаємопов’язаної інформації про ознаки і властивості такого виду злочинів, здатної слугувати підставою для висування версій про подію злочину і особистість злочинця [4 – 5; 7; 9 – 11]. Водночас, серед дослідників немає єдності поглядів щодо визначення змісту криміналістичної характеристики.

Так, М.П. Яблоков визначає зміст криміналістичної характеристики, як такий, що складається з трьох елементів: криміналістичних рис способу вчинення злочину; типових слідчих ситуацій; характеру інформації, яка підлягає з’ясуванню [5, с. 64].

І.Ф. Герасимов до структури криміналістичної характеристики включає поширеність злочинного діяння, особливості виявлення та розкриття даних злочинів, типові риси злочинної події та обстановки вчинення злочину, механізм слідоутворення, спосіб вчинення злочину, особливості особистості і поведінки обвинувачених [5, с. 65].

Р.С. Бєлкін вважає, що криміналістична характеристика окремого виду злочинів охоплює характеристику вихідної інформації, системи даних про спосіб вчинення і приховання злочину і типових наслідках його застосування, особистість вірогідного злочинця, вірогідних мотивах і цілях злочину [5, с. 64].

Порівнюючи різні визначення криміналістичної характеристики, можна дійти висновку, що більшість дослідників-криміналістів відзначають наступні елементи криміналістичної характеристики: типові слідчі ситуації; спосіб вчинення та

приховання злочину; типові матеріальні сліди злочину та механізм слідоутворення; характеристика особистості обвинуваченого й потерпілого; обстановка злочину. Водночас слід підкреслити, що широкий спектр технологій комп’ютерних злочинів відзначається різноманітністю механізмів слідоутворення з можливістю приховання або змін комп’ютерної інформації щодо слідів злочину, що суттєво перешкоджає встановленню типових слідів злочину. Зазначені чинники, а також труднощі виявлення та фіксації комп’ютерної інформації щодо слідів здійснення злочинів, збору доказів не сприяють чіткому уявленню щодо всіх компонентів криміналістичної характеристики, що, в кінцевому підсумку, ускладнює процес розслідування комп’ютерних злочинів.

З огляду на значну роль предмету у механізмі шкідливого впливу на об’єкт злочинного посягання вбачається за доцільне розглянути це питання в контексті криміналістичної характеристики злочинів, що розглядаються. Справді, без дослідження предмета злочину складно правильно кваліфікувати злочинне діяння, розмежувати його від суміжних злочинів.

Визначення поняття “предмет злочину” охоплює змістовні та функціональні аспекти, які у теорії кримінального права досліджені під обома кутами зору. У функціональному аспекті предмет злочину – це те, діючи на що суб’єкт посягає на охоронювані законом відносини. До таких предметів належать лише ті з них, на які суб’єкт злочину безпосередньо впливає, вилучаючи їх, знищуючи, створюючи, змінюючи їх вигляд або правовий режим тощо. Наприклад, предметом злочину, передбаченого ст. 361-1 КК України, є шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку [9]. Але в разі несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку (ст. 361 КК України) комп’ютерні віруси, програмні та технічні засоби, призначені для незаконного проникнення в АОЕМ, їх системи та комп’ютерні мережі, є знаряддям вчинення злочину. У першому прикладі злочинець безпосередньо створює з метою використання, розповсюдження або збуту шкідливі програмні чи технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. У другому – суб’єкт злочинних дій посягає на комп’ютерну інформацію, що використовується в АЕОМ, не впливаючи на предмет, а використовуючи його для здійснення злочинного наміру. До речі, питання про співвідношення понять “предмет” і “засоби або знаряддя вчинення злочину” наукою досі не вирішене.

Викладене вище, а також невизначеність питань щодо з’ясування криміналістично значущих ознак та критеріїв віднесення об’єктів дослідження до шкідливих програмних засобів, в свою чергу, зумовлює певні проблеми при розробці методів експертних досліджень шкідливих програмних засобів, що спрямовані на встановлення криміналістично значимої інформації на підставі аналізу комп’ютерної інформації [8].

На окрему увагу заслуговує робота з розроблення методик експертних досліджень комп’ютерних злочинів як важливої складової методичного забезпечення розслідування цих злочинів, оскільки вміння їх розкривати та розслідувати створює підґрунтя для доказової бази та сприяє підвищенню ефективності протидії цим злочинам.

На сьогоднішній день 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 [13 – 14; 16 – 17]. Зазначені методичні матеріали, в тому числі методики, 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 [12 – 14; 16 – 17]. 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 [15]. Встановлення та оцінка сукупності слідів дозволяє відтворити, тобто змоделювати, дії при здійсненні комп’ютерного злочину й ототожнити слідоутворюючий об’єкт (програму) як засіб злочину [11 – 12; 15].

Такий підхід дозволяє вирішити діагностичну задачу при проведенні досліджень ПЗ, що спрямована на встановлення загальної характеристики програмного засобу та визначення його недокументованих функцій, які забезпечують виконання певних дій [11 – 12].

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 зазначених ПЗ, 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, достатньої для визначення, чи призначений він для негласного отримання інформації.

Тому, 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 встановленням причинного зв’язку 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” базувалось на основних положеннях загальної методики проведення судової експертизи “Віднесення об’єктів до спеціальних технічних засобів негласного отримання інформації” та методичних матеріалів зарубіжних і вітчизняних фахівців у сфері комп’ютерно-технічної експертизи [11 – 19].

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

Методичні рекомендації “Дослідження програмних засобів призначених для негласного отримання інформації” (далі – методичні рекомендації) визначають загальні засади щодо порядку проведення експертних досліджень та встановлює послідовність застосування методів дослідження з питань віднесення програмних засобів до ПЗ НОІ.

Експертне дослідження ПЗ здійснюється шляхом послідовного проведення взаємопов’язаних стадій, до яких відносяться: попереднє дослідження, роздільне дослідження, експертний експеримент, порівняльне дослідження, оцінка результатів проведених досліджень та формулювання висновків, оформлення результатів

проведеного дослідження. На кожній стадії дослідження на підставі оцінки отриманих результатів надаються проміжні висновки [18 – 19].

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.

Аналіз результатів досліджень слідів реалізації функцій ПЗ, дій телекомунікаційного пристрою з негласного отримання інформації, на який встановлено ПЗ, та виявлених причинно-наслідкових зв’язків між ними спрямовано на:

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

– віднесення програмного засобу до ПЗ НОІ [18].

Під об’єктом експертних досліджень ПЗ слід розуміти прикладне програмне забезпечення, що знаходиться на наданих носіях інформації та інформаційні процеси, які обумовлені функціонуванням технічних засобів загального користування, на яких встановлено зазначені ПЗ.

При проведенні експертного дослідження вирішуються, як правило, діагностична, ситуаційна задача, а також задача групофікації ПЗ [11; 14; 18].

Діагностична задача при проведенні досліджень ПЗ спрямована на вирішення наступних питань:

– 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.

Ситуаційна задача – зняття процесів у режимі реального часу, одномоментних станів, встановлення й сприйняття яких можливо тільки в певних умовах (наприклад, у складі певної конфігурації технологічного устаткування, у складі комп’ютерної мережі тощо).

Вирішення ситуаційної задачі при проведенні досліджень ПЗ на стадії експертного експерименту спрямовано на оцінку можливостей виконання певних дій з негласного отримання інформації в реальних умовах його функціонування, встановлення способу використання програмного засобу та з’ясування функціонального призначення програмного засобу.

Для дослідження програмного засобу в реальних умовах його функціонування організується на базі технології “клієнт-сервер” електронно-інформаційна система, яка включає пункт управління об’єднаний телекомунікаційною мережею з абонентськими пристроями, на яких здійснюється перехоплення та передача дистанційно встановлених видів інформації.

Експертна задача на стадії порівняльного дослідження ПЗ спрямована 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, прихованості застосування та визначити, в кінцевому результаті, призначеність програмного засобу [18].

Вирішення завдання експертного дослідження ПЗ здійснюється з урахуванням проміжних висновків та на підставі узагальненої оцінки результатів досліджень. 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;

– призначеності програмного засобу для його застосування у прихований спосіб, характерний для оперативно-розшукових заходів [18 – 19].

Висновки.

Зважаючи на вищевикладене, можливо зазначити, що актуальність проблеми виявлення та розслідування комп’ютерної злочинності в умовах сьогодення потребує удосконалення тактики проведення слідчих дій з розслідування комп’ютерних злочинів, методик та ефективних методів, спрямованих на збирання й аналіз криміналістичної значимої інформації, що дозволять у подальшому оперувати новими специфічними видами доказів (електронними доказами).

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 методичні рекомендації, які регламентують процедуру аналізу ознак реалізації функцій ПЗ та дій комп’ютера чи телекомунікаційного пристрою, на який встановлено ПЗ, з урахуванням встановленого критерію можуть слугувати підґрунтям для розробки методик проведення судових експертиз спеціальних програмних засобів.

Використана література

1. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій / [Б.В. Романюк, В.Д. Гавловський, М.В. Гуцалюк, В.М. Бутузов]. – К. : Вид. Поливода А.В., 2004. – 144 с.

2. Козюра В.Д., Хорошко В.О. Комп’ютерні технології та злочинність : матер. наук.-практ. конф. [“Актуальні проблеми управління інформаційною безпекою держави”], (Київ, 2016 р.) : у 2 ч. – Ч. 1. – К. : Нац. академія СБУ, 2016. – С. 257-261.

3. Виктор Сабадаш. Проблемы латентности компьютерной преступности. – Режим доступу : www crime-research.ru/article/sabodash06. – Назва з екрана.

4. Ботвінкін О.В. Проблеми забезпечення національної безпеки в інформаційній сфері // Юридичний журнал. – 2007. – № 2. – С. 58-63.

5. Голубєв В.О. Розслідування комп’ютерних злочинів : монографія / В.О. Голубєв. – Запоріжжя : Гуманітарний університет “ЗІДМУ”, 2003. – 296 с.

6. Латентність комп’ютерної злочинності // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 3. – С. 176-182.

7. Юдин О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдин. – К., 2010. – 708 с.

8. Кузьменко Б.В., Заїка Ю.О. Типи сучасного особливо небезпечного (шкідливого) програмного забезпечення: правові та технічні аспекти // Юридична наука. – 2013. – № 7. – С. 29-35.

9. Особливості кваліфікації злочину зі створення, розповсюдження і збуту програмних чи технічних засобів (ст. 361-1 КК України). – Режим доступу : http://lib-net.com/content/9471_Osoblivosti_kvalifikacii_zlochiny_zi_stvorennya_rozpovsudjennya_i_zbyty programnih_chi_tehnichnih_zasobiv_st_361_KK_Ykraini.html. – Назва з екрана.

10. Шкідливе програмне забезпечення. – Режим доступу : http://wiki.tntu.edu.ua/Шкідливе_програмне_забезпечення. – Назва з екрана.

11. Россинская Е.Р. Судебная компьютерно-техническая експертиза / Е.Р. Россинская, А.И. Усов. – М. : Право и закон, 2001. – 416 с.

12. Для профессионалов криминалистический анализ файловых систем ; под ред. Брайана Кэрриэ. – СПб. : Питер, 2007. – 480 с.

13. Звіт про науково-досліду роботу дослідження інформації на цифрових носіях : методика / [С. М. Бобрицький, О. В. Чишкало та ін.]. – Х. : ХНДІСЕ, 2009. – 34 с.

14. Методика дослідження комп’ютерної інформації / [К.Ю. Усков, О.М. Пешехонова, Ю.М. Бєляк, В.А. Кореньок, А.О. Ружинський]. – К. : КНДІСЕ, 2005. – 37 с.

15. 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. 4-7.

16. Guidelines for best practice in the forensic examination of digital technology. – Режим доступу : http:// ioce.org/fileadmin/ user_up-load/ 2002. – Назва з екрана.

17. Розробка спеціальних програмних засобів для проведення судових експертиз комп’ютерних мереж / [О. Башкатов, Г. Дружинін та ін.]. – Донецьк : ДНДІСЕ, 2010. – 179 с.

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

19. Методика віднесення об’єктів до спеціальних технічних засобів негласного отримання інформації. – К. : ІСТЕ СБУ, 2011. – 26 с.

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