УДК 343.14:004

ЛЕОНОВ Борис Дмитрович
СЕРЬОГІН Валерій Сергійович

ПРОБЛЕМИ ПРАВОВОГО ТА ЕКСПЕРТНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Постановка проблеми. На стан комп'ютерної або кіберзлочинності істотно впливає бурхливий розвиток інформаційних технологій і розширення сфери їх застосування.

На думку експертів ОБСЄ, кіберзлочинність, пов'язана з використанням інформаційних технологій, комп'ютерних систем і мереж, здатна створити такий хаос, який за масштабом наближується до економічної кризи. У 2008 році щорічна шкода від кіберзлочинності оцінювалася приблизно у 100 млрд доларів [1]. Сьогодні збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн на рік, а за негативним сценарієм у 2019 році вони сягатимуть $ 2 трлн [2].

Революційний стрибок у сучасних інформаційних технологіях на початку XXI століття можна порівняти з появою у 1945 році ядерної зброї, небезпечний руйнівний потенціал якої зумовив впровадження правових підстав її застосування.

Масштаб та рівень суспільно небезпечних наслідків кіберзлочинності зумовлюють необхідність впровадження адекватних підходів щодо вдосконалення кримінально-правового забезпечення протидії кіберзлочинності.

В Україні, на жаль, відсутня офіційна державна статистика, яка б містила відомості про кіберзлочини, що негативно позначається на запобіжних заходах, які мають фрагментарний характер, зумовлюючи труднощі у протидії та боротьбі з таким видом суспільно небезпечних діянь. Згідно зі статистичними даними Генеральної прокуратури України протягом 2018 року обліковано 2 017 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Їх питома вага ще незначна і становить усього 0,5 % від усіх облікованих кримінальних правопорушень у 2018 році, але за останні п'ять років зросла в 5,6 раза (у 2014 році становила – 0,09 %) [3, с. 108, 110].

Отже, як на міжнародному, так і національному рівні кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед правоохоронними органами. До цього часу не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці.

Вважається, що на міжнародному рівні кримінально-правовому реагуванню на прояви кіберзлочинності приділена достатня увага. Серед основних міжнародних нормативно-правових актів щодо протидії кіберзлочинності виділяються Конвенція ООН проти транснаціональної злочинності 2001 року (ратифікована із застереженнями і заявами Законом України від 04.02.2004 № 1433-IV), Європейська конвенція про взаємну правову допомогу у кримінальних справах 1959 року (ратифікована із застереженнями і заявами Законом України від 16.01.1998 № 4498-ВР), Конвенція про кіберзлочинність 2001 року (ратифікована із застереженнями і заявами Законом України від 07.09.2005 № 2824-IV).

З урахуванням міжнародних зобов'язань нашої держави та під впливом світових тенденцій склалася і практика боротьби з кіберзлочинністю в Україні. Особливу гостроту проблематика забезпечення кібербезпеки набуває в сучасних умовах фактичної гібридної війни, яка ведеться проти України. Про це свідчить низка прийнятих останнім часом нормативно-правових актів, серед яких Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія кібербезпеки, затверджена Указом Президента України від 15.03.2016 № 96, Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 № 92, Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 06.06.2016 № 240, Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.2016 № 242, Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений Постановою Кабінету Міністрів України від 23.08.2016 № 563.

Аналіз останніх досліджень і публікацій. Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н. М. Ахтирська, Ю. М. Батурин, П. Д. Біленчук, О. В. Ботвінкін, В. О. Голубєв, В. Д. Гавловський, М. В. Гуцалюк, М. В. Карчевський, М. О. Кравцова, О. М. Литвинов, Ю. Ю. Нізовцев, О. А. Парфило, Б. В. Романюк, О. Р. Росинська, Т. Л. Тропіна, В. С. Цимбалюк, О. М. Черкун, О. К. Юдін та інші.

Серед закордонних досліджень заслуговують на увагу праці Д. Айкова, К. Сейгера, У. Фонстроха, К. Брайана та С. Бреннера.

Водночас, незважаючи на значну кількість наукових публікацій, присвячених проблемам протидії кіберзлочинності, стрімкий розвиток інформаційних технологій, поява нових способів і методів кіберзлочинів зумовлює потребу подальших досліджень цієї тематики.

Отже, **метою статті** є аналіз правових основ забезпечення кібербезпеки та виявлення недоліків у правоохоронній діяльності з протидії кіберзлочинності, а також визначення шляхів її удосконалення.

Виклад основного матеріалу. Перш ніж перейти до розгляду правового та експертного забезпечення протидії кіберзлочинності слід уточнити

визначення поняття «кіберзлочинність», появу якого обґрунтовано пов'язують з рівнем суспільно небезпечних загроз та з розширенням технічної бази інформатизації.

Останнім часом у теорії кримінального права загострилася дискусія щодо формулювання проблеми кіберзлочинності. З'ясування цього питання має велике значення для визначення напрямків кримінально-правової боротьби з кіберзлочинністю в цілому та комп'ютерними злочинами зокрема.

О. В. Ботвінкін вважає, що до комп'ютерних злочинів слід відносити: комп'ютерне шпигунство; комп'ютерні диверсії (у тому числі руйнування операційних систем, створення та використання комп'ютерних вірусів); комп'ютерний тероризм; крадіжку комп'ютерних послуг (зокрема обчислювальних ресурсів); махінації та маніпулювання системою обробки даних, а також крадіжку фінансових засобів і підробку документів; порушення приватної або державної таємниці; протиправне копіювання програмних продуктів, яке порушує авторське та інші права, тощо [7, с. 59, 60]. Таке розуміння істотно розширює коло комп'ютерних злочинів, оскільки деякі із згаданих злочинів мають інший об'єкт кримінально-правової охорони, зміст якої не охоплюється статтями 361–362-3 Кримінального кодексу України (далі – КК України).

М. О. Кравцова та О. М. Литвинов під кіберзлочинністю пропонують розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [12, с. 19].

Доречно зазначити, що завдяки широкому розповсюдженню так званих «комуникаторів» та «смартфонів», які поєднують властивості мобільних телефонів і комп'ютерів, кіберзлочинність набула значного поширення, зміст якої охоплює весь спектр суспільно небезпечних діянь у сфері використання інформаційних технологій.

Однак нормативні визначення обчислювальної машини та електронної обчислювальної машини не дозволяють тлумачити поняття «комп'ютер» настільки обмежено.

Отже, можна погодитись з тим, що поняття «комп'ютерний злочин» та «кіберзлочин» є тотожними [10, с. 12]. Такий висновок підтверджується результатами наукових досліджень зарубіжних вчених. Так, С. Бреннер розглядає три категорії кіберзлочинів: 1) злочини, в яких комп'ютер є метою злочину; 2) злочини, в яких комп'ютер використовується як засіб вчинення злочину; 3) злочини, в яких комп'ютер грає незначну роль у вчиненні злочину [21].

Законом України «Про основні засади забезпечення кібербезпеки України» «кіберзлочин» (комп'ютерний злочин) визначається як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, від-

повідальність за яке передбачена законом України про кримінальну відповідальність, та/або яке визнано злочином міжнародними договорами України [22].

На думку фахівців ГНЕУ Апарату Голови Верховної Ради України, цей термін має бути узгоджений із КК України, який містить окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», де використовується термін «комп'ютерний злочин» [23].

Схожої точки зору додержуються фахівці Головного юридичного управління Апарату Голови Верховної Ради України, які дійшли висновку, що наведене в законопроєкті «Про основні засади забезпечення кібербезпеки України» (реєстр. № 2126а) визначення кіберзлочинності як сукупності кіберзлочинів є яскравим прикладом порушення базових правил формальної логіки, що мають застосовуватися при формулюванні визначень, оскільки дефініція кіберзлочинності містить у собі так зване «коло» – визначаюче поняття, фактично, буквально повторює визначуване поняття. Запропонована редакція поняття «кіберзлочин» насправді складається з дефініцій, відповідно, злочину, яке вже використовується в чинних нормативно-правових актах, з додаванням словосполучення «в кіберпросторі» [24].

На помилковість застосування категорії «кіберпростір» у визначенні кіберзлочину звертає увагу М. В. Карчевський, на думку якого зміст інформаційного середовища не може розглядатися як вид певного простору чи території у класичному розумінні [9, с. 12].

Т. Л. Тропіна пропонує визначати кіберзлочинність як винне вчинене суспільно небезпечне кримінальне каране втручання у роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, вчинені за допомогою комп'ютерів, комп'ютерних програм, комп'ютерних мереж, а також за допомогою інших засобів доступу [16, с. 38].

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 [5; 6; 25]. Тобто в основу такої класифікації злочинів покладено ознаки, що характеризують засоби, які використовуються при їх вчиненні. Але самі по собі засоби не змінюють сутності злочину. Отже, такий підхід не позбавлений недоліків з огляду на його невідповідність головному принципу структурування національного законодавства про кримінальну відповідальність – систематизації кримінального закону на підставі класифікації злочинних посягань за об'єктом. Визначення нової групи злочинів має проводитися з урахуванням ознак, що характеризують об'єкт злочинного посягання. Саме тому у межах національного кримінально-правового дискурсу необґрунтованим вбачається виділяти певні групи злочинів на основі ознак,

що характеризують спосіб, знаряддя чи засоби злочину [5, с. 11; 25, с. 22].

Між тим, визначення комп'ютерних злочинів як групи посягань, які характеризуються загальними ознаками способу, засобу чи знаряддя, може бути цілком затребуване з позиції криміналістики [9, с. 13]. В межах останньої йдеться про встановлення особливостей методики виявлення, розслідування злочинів цієї категорії, фіксації їх слідів тощо. До речі, у вітчизняній юридичній літературі термін «комп'ютерний злочин» спочатку застосовувався в криміналістичному аспекті. Під цими злочинами пропонувалося розуміти передбачені кримінальним законом суспільно небезпечні діяння, в яких машинна інформація є засобом або об'єктом злочинного посягання [25, с. 167].

З нашої точки зору, термін «машинна інформація» є застарілим й таким, що не узгоджується з вимогами національного та міжнародного законодавства, адже Конвенція про кіберзлочинність 2001 року і додаткові протоколи до неї оперують поняттями «комп'ютерна система», «комп'ютерні дані». Тому предметом злочинних посягань, відповідальність за які передбачена розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України, є саме комп'ютерна інформація.

Конвенція про кіберзлочинність 2001 року передбачає встановлення відповідальності за «правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп'ютерної системи» тощо.

Ми приєднуємося до позиції вчених, на думку яких кримінально-правовий обсяг поняття «кіберзлочинність», що визначається рівнем суспільно небезпечних загроз, складають як правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних, навмисне перехоплення технічними засобами, без права на це передач комп'ютерних даних, так і кримінальне каране втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, навмисне серйозне перешкоджання їх функціонуванню.

Водночас слід зазначити, що поряд з поняттям «кіберзлочинність» в кримінально-правовому аспекті вживається поняття «злочини у сфері використання інформаційних технологій». Забезпечення кримінально-правового стимулювання позитивних та мінімізації негативних соціальних наслідків інформатизації передбачає визначення як самостійного об'єкта кримінально-правової охорони системи суспільних відносин, які забезпечують реалізацію інформаційної потреби. Для позначення цієї системи використовують термін «інформаційна безпека», її структуру складають відносини у сфері формування інформаційного ресурсу, забезпечення дос-

тупу до інформації, а також відносини у сфері використання інформаційних технологій [9, с. 11; 10]. Суспільна небезпечність злочинів у сфері використання інформаційних технологій головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це і визначає суспільну небезпечність конкретного посягання у сфері використання інформаційних технологій [11].

З огляду на викладене вважаємо більш перспективним закладений у законопроєкті про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки (реєстр. № 9575 від 09.12.2011) підхід, згідно з яким родовим об'єктом злочинів, що розглядаються, є суспільні відносини у сфері інформаційної безпеки, що, на думку його розробників, зумовлює зміну назви розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України на «Злочини у сфері інформаційної безпеки» [26].

Водночас слід зазначити, що злочини, які передбачені розділом XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України не охоплюють весь спектр злочинів у сфері інформаційної безпеки. Тому більш прийнятною вважається зміна назви розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України на «Злочини у сфері використання інформаційних технологій».

Крім того, з урахуванням міжнародних зобов'язань України вважаємо за доцільне доповнити згаданий розділ КК України нормами про злочини проти конфіденційності, цілісності та доступності комп'ютерних даних, в яких як обтяжуючі обставини мають визнаватися використання спеціальних програмних засобів негласного отримання інформації та інформаційних технологій.

Слід підкреслити, що широкий спектр таких технологій відзначається різноманітністю механізмів слідоутворення з можливістю приховання або змін комп'ютерної інформації щодо слідів злочину.

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 15.03.2016 № 96, визначається, 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 [27].

Сьогодні в спеціалізованих експертних установах України впроваджені методичні матеріали для забезпечення проведення досліджень но-

сіїв комп'ютерної інформації, які використовуються, у тому числі й для методичного забезпечення дослідження програмних продуктів як засобів здійснення комп'ютерних злочинів [28–31].

Рекомендовані методи дослідження комп'ютерної інформації та технології контролю активності досліджуваних програмних засобів (далі – ПЗ) можуть бути застосовані для виявлення слідів реалізації його (ПЗ) функцій. Встановлення та оцінка сукупності слідів дозволяє відтворити, тобто змоделювати, дії при здійсненні комп'ютерного злочину й ототожнити слідоутворюючий об'єкт (програму) як засіб злочину при вирішенні діагностичної задачі [32, с. 4].

Враховуючи актуальність питань протидії незаконному обігу спеціальних програмних засобів (так званих «шпигунських» програм), в ІСТЕ СБ України було розроблено низку методичних рекомендацій для проведення експертних досліджень програмних засобів, використання яких завдає шкоди конфіденційності, цілісності та доступності комп'ютерної інформації, а саме дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем [33] шкідливих програмних засобів [34], а також дослідження програмних засобів, призначених для негласного отримання інформації (далі – ПЗ НОІ) [35].

Слід підкреслити, що віднесення програмного засобу до предмета злочину потребує встановлення за результатами дослідження необхідної сукупності ознак та властивостей, достатніх для визначення його призначеності для негласного отримання інформації.

Новизною методичних рекомендацій є запропонований підхід щодо дослідження ПЗ, який передбачає комплексне застосування різних методів досліджень та виконання експертних задач (діагностичної, ситуаційної та задачі групофікації) як в галузі комп'ютерно-технічної експертизи, так і в галузі експертизи СТЗ [20, с. 4].

Висновки. Кримінально-правова політика у сфері забезпечення інформаційної безпеки в основному здійснюється за напрямками, що випливають з міжнародних зобов'язань України. Втім, боротьба з кіберзлочинністю недостатньо ефективна. Це свідчить про необхідність удосконалення всієї системи кримінально-правового забезпечення охорони інформаційної безпеки України, а не тільки критичної інформаційної інфраструктури.

Під час удосконалення законодавства України про кримінальну відповідальність назву розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України доцільно змінити на «Злочини у сфері використання інформаційних технологій», а його зміст доповнити нормами про злочини проти конфіденційності, цілісності та доступності комп'ютерних даних.

Успішній протидії незаконному обігу спеціальних програмних засобів (так званих «шпигунських» програм) сприятиме запропонована в методичних рекомендаціях процедура

аналізу виявлених функцій ПЗ з урахуванням встановлених в цих рекомендаціях суттєвих ознак (функціональних можливостей) ПЗ НОІ, що дозволяє з'ясувати спосіб функціонування ПЗ, його властивості з негласного отримання інформації та визначити, в кінцевому результаті, призначеність програмного засобу [35].

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

Список використаних джерел

1. Киберпреступность страшнее финансового кризиса [Електронний ресурс]. – Режим доступу : https:www.crime-research.ru/news/03.12.2008/50.

2. Киберпреступники наживаются на самых бедных [Електронний ресурс]. – Режим доступу : https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief.

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

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

5. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М. : Юридическая литература, 1991. – 157 с.

6. Біленчук П. Д. Комп'ютерна злочинність : навчальний посібник / П. Д. Біленчук, В. В. Бут, В. Д. Гавловський, М. В. Гуцалюк, Р. Л. Колпак. – К. : Атіка, 2002. – 240 с.

7. Ботвінкін О. В. Проблеми забезпечення національної безпеки в інформаційній сфері / О. В. Ботвінкін // Юридичний журнал. – 2007. – № 2. – С. 59–60.

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

9. Карчевский Н. В. «Киберпреступление» или преступление в сфере использования информационных технологий? / Н. В. Карчевский // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовтня 2016 р.). – Одеса : ОДУВС, 2016. – С. 10–14.

10. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України / М. В. Карчевський. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 512 с.

11. Карчевський М. В. Дослідження практики використання національними судами норм про кримінальну відповідальність за злочини у сфері використання комп'ютерної техніки та мереж електрозв'язку. Злочини у сфері використання ІТ [Електронний ресурс]. – Режим доступу : http//www.it-crime.at.ua.

12. Кравцова М. О. Запобігання кіберзлочинності в Україні / М. О. Кравцова, О. М. Литвинов. – Харків : Панов, 2016. – 210 с.

13. Парфило О. А. Актуальні питання судово-експертного дослідження шкідливих програмних засобів у межах протидії кібертероризму / О. А. Парфило, Ю. Ю. Нізовцев // Криміналістичний вісник. – 2016. – № 1(25). – С. 78–84.

14. Романюк Б. В. 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.

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

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

17. Цимбалюк В. С. Латентність комп'ютерної злочинності / В. С. Цимбалюк // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2001. – № 3. – С. 176–182.

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

19. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонстрох. – М. : Мир, 1999. – 351 с.

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

21. Brenner S. Cybercrime: criminal threats from cyberspace / S. Brenner. – Praeger, 2006. – 281 p.

22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/2163-19.

23. Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

24. Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

25. Геллер А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета : дис. ... канд. юрид. наук : спец. 12.00.08 / А. В. Геллер. – М., 2006. – 219 с.

26. Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=42065.

27. Стратегія кібербезпеки України : затвердж. Указом Президента України від 15.03.2016 № 96 [Електронний ресурс]. – Режим доступу : https://www.president.gov.ua/documents/962016-19836.

28. Звіт про науково-дослідну роботу дослідження інформації на цифрових носіях (методика) / С. М. Бобрицький, О. В. Чишкало та ін. – Харків : ХНДІСЕ, 2009. – 34 с.

29. 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.

30. Guidelines for best practice in the forensic examination of digital technology [Електронний ресурс]. – Режим доступу : http://ioce.org/fileadmin/user_up-load/2002.

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

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

33. Нізовцев Ю. Ю. Судово-експертне дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні : методичні рекомендації / Ю. Ю. Нізовцев. – Київ : Видавничий дім «АртЕк», 2016. – 118 с.

34. Нізовцев Ю. Ю. Судово-експертне дослідження шкідливих програмних засобів : методичні рекомендації / Ю. Ю. Нізовцев. – К. : ІСТЕ СБУ, 2018. – 119 с.

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

Аннотация. Статья посвящена анализу проблем правового и экспертного обеспечения правоохранительной деятельности в области противодействия киберпреступности. В статье рассматриваются вопросы уголовно-правовой охраны информационной безопасности в контексте имплементации международных договоров в национальное законодательство. Проанализировано законодательство в области обеспечения кибербезопасности, современная доктрина его толкования, а также внесены отдельные предложения по его усовершенствованию.

Ключевые слова: кибербезопасность, киберпреступность, компьютерное преступление, вредные программные средства, специальное программное средство негласного получения информации.

Abstract. The article is devoted to the analysis of the problems of legal and expert support of law enforcement activities in the field of cybercrime counteraction. The article deals with the issues of criminal and legal protection of information security in the context of the implementation of international treaties into the field of national legislation. The authors both analyzed legislation in the field of cybersecurity provision; the modern doctrine devoted to its interpretation and made some suggestions for its improvement.

Key words: cybersecurity, cybercrime, computer crime, harmful software, special software for secretly obtaining information.

УДК 343.148

НАДІЖКО Марина Миколаївна

ДЕЯКІ ПИТАННЯ НАУКОВО-МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ СУДОВО-ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ В СИСТЕМІ СБ УКРАЇНИ (НА ПРИКЛАДІ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ДОСЛІДЖЕНЬ)

Постановка проблеми. Відповідно до п. 1 ч. 5 ст. 69 Кримінального процесуального кодексу України експерт зобов'язаний особисто провести повне дослідження і дати обґрунтований та об'єктивний письмовий висновок на поставлені йому запитання, а в разі необхідності – роз'яснити його [1]. Зрозуміло, що обґрунтованість та об'єктивність висновку експерта можлива лише у випадку, якщо в процесі збирання речових доказів (об'єктів) та їх подальшого експертного дослідження застосовуються науково обґрунтовані методи і методики, що дозволяють отримати достовірні