

УДК 343.98.06

СПІВВІДНОШЕННЯ ТЕРМІНІВ, ЩО ЗАСТОСОВУЮТЬСЯ ДЛЯ ПОЗНАЧЕННЯ ЗЛОЧИНІВ, УЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ ОБСТАНОВКИ КІБЕРПРОСТОРУ

Самойленко О.А., к. ю. н.,
доцент кафедри криміналістики
Національний університет «Одеська юридична академія»

Стаття присвячена порівняльному аналізу термінів і терміносполучень, що використовуються для позначення злочинів, учинених із використанням обстановки кіберпростору.

Ключові слова: інформаційні технології, кіберпростір, кіберзлочин, комп'ютерний злочин, комп'ютерні технології, обстановка злочину.

Статья посвящена сравнительному анализу терминов и их словосочетаний, которые используются для обозначения преступлений, совершенных с использованием обстановки киберпространства.

Ключевые слова: информационные технологии, киберпространство, киберпреступление, компьютерное преступление, компьютерные технологии, обстановка преступления.

Samoilenko O.A. CORRELATION OF TERMS, WHICH ARE USED FOR VALUE OF THE CRIME ACCOMPLISHED WITH THE USE OF CRIME SCENE CYBERSPACE

The article is devoted to a comparative analysis of terms and their word combinations, which are used to describe crimes, committed using the environment of cyberspace.

Key words: information technologies, cyberspace, kibercrime, computer crime, computer technologies, situation of crime.

Постановка проблеми. Кіберпростір сьогодні створює специфічну обстановку вчинення злочинів різних видів, що, безперечно, зумовлює необхідність звернення уваги в криміналістичних дослідженнях на комплекс таких злочинів. Проблема різноманіття використовуваних термінів і терміносполучень для позначення такого явища призводить до суттєвої плутанини в понятійному апараті, що під час наукових досліджень відвертає увагу науковців від прикладного характеру досліджень із подібної тематики, призводить до необґрунтованої підміни чи об'єднання понять.

Ступінь розробленості проблеми. Проблемі багатозначності терміносполучень, що позначають злочини, учинені із використанням обстановки кіберпростору, піднімали В.П. Беленький, В.О. Голубев, О.І. Мотлях, Н.А. Розенфельд, К.В. Тітуніна, В.С. Цимбалюк, В.П. Шеломенцев і багато інших науковців. Здавалося б, надання визначення конкретному терміну мало вирішити таку проблему, але визначення понять зводить останні до інших, не визначених основних понять [1, с. 18].

Метою статті є визначення змісту та співвідношення термінів і терміносполучень, що використовуються для позначення злочинів, учинених із використанням обстановки кіберпростору.

Виклад основного матеріалу. Для позначення вказаного соціально-правового явища використовуються такі терміни та терміносполучення: «комп'ютерний злочин», «кіберзлочин», «інформаційний злочин», «злочини у сфері високих інформаційних технологій», «злочини у сфері комп'ютерної інформації». Розмежування змісту таких понять має здійснюватися з урахуванням вітчизняних, міжнародних і закордонних теоретико-прикладних досліджень у науках кримінального блоку.

Проаналізувавши публікації з тематики змісту терміна «комп'ютерні злочини», резюмуємо, що зміст терміна залежить від пред-

метної сфери конкретної науки. На цьому справедливо наголошують також В.В. Вехов, М.В. Карчевський і багато інших науковців, що пропонують давати різні визначення комп'ютерних злочинів із погляду кримінально-правової охорони й криміналістичної науки [2].

У кримінальному праві, на думку М.В. Карчевського, визначення комп'ютерних злочинів має конструюватися на основі специфічних ознак їх родового об'єкта, адже системоутворюючим фактором сукупності норм Особливої частини Кримінального кодексу України (далі – КК України) є саме родовий об'єкт [3, с. 42]. Тож традиційним у кримінально-правових дослідженнях стало ототожнення комп'ютерного злочину зі злочинами у сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку, передбаченими винятково нормами однойменного розділу XVI КК України. У кримінально-правовому значенні комп'ютерні злочини є передбаченими кримінальним законом суспільно небезпечними діяннями, в яких комп'ютерна (машинна) інформація є об'єктом злочинного посягання [4, с. 14; 5, с. 38; 3, с. 42]. Про підтримання більшістю науковців такої позиції свідчать результати аналізу тематики дисертаційних досліджень подібного напрямку, адже теми дисертацій формулюються в контексті викладення конкретної статті розділу XVI КК України. Утім, сам термін «комп'ютерний злочин» використовується з метою скорочення громіздких терміносполучень цієї тематики (Д. Айков, Ю.М. Батурич, А.Г. Волеводз, В.О. Голубев, Р.А. Калюжний, М.В. Карчевський, Н.А. Розенфельд, К. Сейгер, У. Фонсторх та ін.) [4; 6–10].

У криміналістиці термін «комп'ютерний злочин» має розширене тлумачення, під ним розуміють діяння, в яких комп'ютер є предметом, знаряддям або засобом скоєння злочину. Це пов'язано з переважанням діяльнісного підходу в криміналістичних дослі-



дженнях [11, с. 8]. М.В. Салтевський, пояснюючи використання терміна «комп'ютерні злочини», писав, що на відміну від кримінального права, у криміналістиці вид злочину називають навіть не за засобом (знаряддям) учинення злочину, а за видом злочинної діяльності [12, с. 4]. Дійсно, одним з основних об'єктів дослідження в криміналістиці є діяльність зі скоєння злочинів (злочинна діяльність) [13, с. 14]. Використання комп'ютера розглядається як обов'язкова умова вчинення таких злочинів, що з погляду спільності механізмів учинення злочинів зумовлює відповідний механізм слідоутворення, а тому можна розробити єдиний напрям організації й тактики розслідування таких злочинів. На зламі XX і XXI століть виходить ціла низка робіт, присвячених комп'ютерному злочину в подібній трактовці, зокрема криміналістів (П.Д. Біленчук, А.С. Білоусов, В.Б. Вехов, М.А. Зубань, Б.В. Романюк, В.С. Цимбалюк) [2; 5; 14; 15], кримінологів (Р.І. Дрімлюга, Д.В. Добровольський, М.О. Кравцов) [16; 17].

Окремої уваги заслуговує терміносполучення «злочини у сфері комп'ютерної інформації», що окреслюється в Україні на рівні дисертаційного дослідження в 2002 р. Д.С. Азаровим. Цей вислів, на думку автора, зумовлений важливістю та значенням об'єкта посягання (комп'ютерна інформація) [18, с. 19]. До таких злочинів відносять злочини, передбачені розділом XVI КК України, а також ч. 3 ст. 190 КК (шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки) і ст. 200 КК (використання підроблених електронних засобів доступу до банківських рахунків) [18; 19]. Наразі саме ці категорії злочинів у диспозиції статей КК України мають указівку на використання для їх учинення комп'ютерної техніки, а значить, додатковим предметом посягання стає інформація. У цьому аспекті В.В. Крилов у криміналістичних дослідженнях уживає поняття «інформаційні злочини», розуміючи їх як суспільно небезпечні діяння, що заборонені кримінальним законом під загрозою покарання, учинені в галузі інформаційних правовідносин [20, с. 11]. Відзначимо, що в такому розумінні злочини у сфері комп'ютерної інформації (інформаційні злочини) близькі за змістом до поняття «комп'ютерні злочини» в криміналістичних дослідженнях.

Тож терміносполучення «комп'ютерний злочин», «злочини у сфері комп'ютерної інформації» й «інформаційні злочини» пов'язуються з позицій кримінально-правового змісту цих понять. Вони розглядаються в аспекті «діянь, учинених у сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку», кримінальна відповідальність за які передбачена однойменним розділом XVI КК України, і злочинних діянь, учинених за допомогою комп'ютера (ст. ст. 190, 200 КК України).

Варто зазначити, що жодне з розглянутих терміносполучень не тлумачиться в законодавстві України. У Законі України «Про основи національної безпеки України» [21] використовується лише вислів «комп'ютерна злочинність і комп'ютерний тероризм» в якості визначених у ст. 7 основних загроз національній безпеці України.

Поява в криміналістичних дослідженнях терміносполучень «злочини у сфері високих інформаційних технологій» або «злочини у сфері комп'ютерних технологій» була пов'язана з розвитком наукового знання у сфері високих інформаційних технологій і комп'ютерних технологій зокрема.

Сьогодні абсолютну більшість технологічних і соціальних процесів у державі, галузях виробництва від енергетики до засобів масової інформації вивели на інший наукоємний рівень саме високі інформаційні технології, що засновані на автоматичному обробленні інформації в процесі розв'язання обчислювальних та інформаційних завдань. Комп'ютерні технології є сукупністю систематичних і масових засобів і прийомів автоматичного оброблення інформації, заснованих на перетворенні інформації в числову форму, що забезпечує високу швидкість оброблення даних, пошуку інформації, розосередження доступу до джерел інформації незалежно від місця розташування [22, с. 18]. Комп'ютер є лише одним з апаратних засобів комп'ютерних технологій. Тому помилковими стають посилення криміналістів лише на його використання під час учинення злочинів.

Застосування всіх апаратних і програмних засобів комп'ютерних технологій під час учинення злочину призводить до утворення специфічних слідів – змін в інформаційному середовищі, що в ході розслідування зумовлює необхідність використання відповідних (спеціальних) прийомів і методів їх виявлення й дослідження [22, с. 19]. На межі першого та другого десятиріч XXI століття наукові теми, окремі та комплексні методики розслідування злочинів розробляються саме з огляду на цю специфіку злочинної діяльності, зокрема щодо викрадень майна, шахрайств, незаконних дій у кредитно-фінансовій сфері тощо [22–25]. Але проблема визначення єдиного терміна, що має змістовно охоплювати всі схожі за електронною природою види злочинної діяльності, не вирішувалася.

Довготривала наукова та законодавча невизначеність наведеного соціально-правового явища призвела в країнах СНД до запозичення з міжнародної й закордонної практик боротьби зі злочинами терміна «кіберзлочин» («cybercrime»). Аналіз сучасних публікацій, тем дисертаційних досліджень та інших джерел інформації дозволяє нам упевнено говорити про сучасне загальне визнання українською науковою спільнотою терміна «кіберзлочин» [26–28]. На нашу думку, запозичення з англійської лексики терміна «кіберзлочин» можна розглядати з двох різнопланових позицій. По-перше, запозичена конструкція є вдалою з позицій предметної сторони криміналістичної науки, сформульована в змістовному плані коротко, легка для розуміння навіть нефахівцем із права. Термін із префіксом «кібер-» дає однозначну відповідь на обстановку вчинення конкретного злочинного явища – це кіберпростір як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої,

обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача. По-друге, проблема недостатньої аргументованості та хаотичного представлення змісту поняття «кіберзлочин», наявна в закордонних роботах і правових актах, перейшла в наукове поле України.

Для розуміння міжнародного процесу розвитку наукової думки щодо змісту терміна «кіберзлочин» потрібно вдаватися до аналізу результатів багаторічної роботи Конгресу ООН із попередження злочинності та поведіння з правопорушниками як консультативного органу відповідно до Програми ООН у сфері попередження злочинності та кримінального судочинства, пункту 29 Декларації принципів [29]. Починаючи з десятого форуму Конгресу у Відні у 2000 р., жодний форум не проходить без акценту на боротьбі з кіберзлочинами.

На Десятому форумі Конгресу термін «кіберзлочин» був розкритий у двох розуміннях. Кіберзлочин у вузькому розумінні (синонім – «комп'ютерний злочин», використовувався в такому значенні в окремих доповідях форуму) є будь-яким протиправним діянням, здійснюваним за допомогою електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних. Кіберзлочини в широкому сенсі (синонім – «злочини, пов'язані з використанням комп'ютерів», також використовувався на форумі) – це будь-яке протиправне діяння, вчинене у зв'язку з комп'ютерною системою чи мережею або за її допомогою, включаючи такі злочини, як незаконне зберігання, пропозиція або поширення інформації за допомогою комп'ютерної системи чи мережі.

На одинадцятому форумі Конгресу була прийнята так звана Бангкокська декларація про взаємодію й відповідні заходи: стратегічні союзи в галузі попередження злочинності й кримінального правосуддя, у пункті 16 Декларації йдеться про активізацію та розширення співробітництва в галузі попередження та розслідування злочинності, пов'язаної з використанням високих технологій і комп'ютерів. В інших пунктах йдеться про тероризм і транснаціональну організовану злочинність.

У центрі уваги дванадцятого форуму Конгресу знаходилися проблеми кіберзлочинності, її транснаціональний і організаційний аспекти, організаційні відмінності підходів у національному законодавстві й інші важливі питання.

Останній форум Конгресу, що проходив 2015 р., є дуже важливим із позицій практичного роз'яснення проблем і шляхів їх вирішення щодо розслідування кіберзлочинів [30]. Наведемо основні тези, що допомагають визначити міжнародний погляд на зміст терміна «кіберзлочин».

По-перше, визнано, що межа між кіберзлочинністю та звичайною злочинністю стає все більш розмитою. Дійсно, у річному звіті про результати роботи за 2016 р. Управління ООН із наркотиків і злочинності містяться конкретизовані напрями протидії кіберзлочинам (для країн Західної й Центральної Азії), зокрема створення спеціалізованих підрозділів по боротьбі з кіберзлочинами; зміцнення регіональної співпраці між правоохоронними й судовими органами в питаннях переслідування кіберзлочинців, проведення розслідувань у «тішовій мережі» (DarkNet); боротьба з проблемою незаконного використання віртуальних валют; збір і використання електронних доказів [31].

По-друге, до категорії «кіберзлочинність» включають такі діяння, за яких об'єктом злочину є комп'ютерні дані або системи, а також діяння, за яких використання комп'ютерних або інформаційних систем є невід'ємною частиною способу вчинення злочину. В якості першої групи називають отримання незаконного доступу до комп'ютерних даних або систем (іноді іменовані «основними» кіберзлочинами). В якості другої групи – використання комп'ютерних даних або систем для шахрайства, розкрадання чи спричинення шкоди іншим особам, злочини, пов'язані з використанням комп'ютерів та інтернет-контенту, включаючи пропаганду ненависті, дитячу порнографію, злочини з використанням особистих даних і продаж заборонених товарів у режимі он-лайн.

По-третє, міжнародна спільнота резюмувала, що у внутрішньому (національному) законодавстві про кіберзлочинність відповідальність за такі злочини встановлюється на основі поєднання положень, що стосуються як виключно кіберзлочинів, так і в цілому загальнокримінальних злочинів. Наводимо чіткий фрагмент офіційної публікації результатів форуму: «Кримінальна відповідальність за здійснення «основних» злочинів, таких, як отримання незаконного доступу до комп'ютерних даних і систем, може встановлюватися шляхом ухвалення спеціального законодавчого положення, тоді як діяння, пов'язані із застосуванням комп'ютерів для отримання особистої або фінансової допомоги чи спричинення особистої або фінансової шкоди, частіше за все можуть визнаватися кримінальними на основі положень, що стосуються здійснення загальнокримінальних (не пов'язаних із застосуванням комп'ютерів) злочинів. У деяких випадках внутрішні нормативно-правові основи приймаються у виконання з урахуванням багатосторонніх документів, які можуть бути обов'язковими або необов'язковими для сторін» [30].

Вважаємо, що термін «кіберзлочин» на міжнародній арені обґрунтовано розширений до розуміння під ним усіх традиційних злочинів, учинених із застосуванням телекомунікаційних мереж, комп'ютерних систем і пристроїв, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача. Однак розкриття змісту через конкретний перелік таких злочинів ми сьогодні не побачимо в жодному нормативному акті або теоретичному розробленні питання класифікації кіберзлочинів. Це пов'язано з відсутністю універсального міжнародного документа щодо боротьби з кіберзлочинами. Більшість науковців спираються в цьому питанні на міжрегіональні нормативні акти, до яких приєдналась їхня держава.



Конвенція Ради Європи про кіберзлочини, яка діє в правовому полі України, далека від досконалості щодо визначення змісту та видів кіберзлочинів в європейському регіоні. Тому, використовуючи дефініцію «кіберзлочин», вітчизняні науковці-правники не виправдано звужують зміст соціально-правового явища – злочину, учиненого з використанням обстановки кіберпростору, обмежуючи його діями, які визначені злочинними відповідно до Конвенції. У криміналістичній науці це призводить до неповноти розроблених методик розслідування, відсутності практичної значущості рекомендацій з організації й тактики розслідування злочинів, адресованих практичним працівникам правоохоронних органів.

Висновки. Таким чином, у реаліях міжнародного та національного, правового й теоретичного забезпечення процесу боротьби з новим соціально-правовим явищем – злочином, учиненим із використанням обстановки кіберпростору, – немає терміна чи терміносполучення, що їх можна було б безпеліційно використовувати в наукових дослідженнях. Вважаємо, що в основу такого поняття повинна бути покладена сутність кіберпростору, зумовлена його подвійною природою, чинниками соціального та технічного характеру як специфічної обстановки вчинення кримінального правопорушення. Тому до моменту розроблення на міжнародному рівні універсального нормативного акта у сфері боротьби зі злочинами, учиненими з використанням обстановки кіберпростору, вважаємо можливим використовувати наведене нами терміносполучення, намагаючись не звужувати предмет дослідження в контексті транснаціонального характеру такої злочинної діяльності.

ЛІТЕРАТУРА:

1. Бауэр Ф.Л. Информатика : в 2 ч. – Ч. 1: Вводный курс / Ф.Л. Бауэр, Г. Гооз. – Москва : Мир, 1990. – 336 с.
2. Вехов В.В. Компьютерные преступления. Способы совершения и раскрытия / В.В. Вехов, под ред. акад. Б.П. Смагоринского. – М. : Право и Закон, 1996. – 182 с.
3. Карчевський М.В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж: аналіз складу злочину : дис... канд. юрид. наук : 12.00.08 / М.В. Карчевський. – Луганськ, 2003. – 175 с.
4. Калужный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. ... докт. юрид. наук : спец. 12.00.02 «Конституционное право; муниципальное право» / Р.А. Калужный; Институт государства и права имени В.М. Корецкого Академии наук Украины. – К., 1992. – 23 с.
5. Білоусов А.С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. ... канд. юрид. наук : 12.00.09 / А.С. Білоусов. – Запоріжжя, 2008. – 245 с.
6. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх (пер. с англ.). – М. : Мир, 1999. – 351 с.
7. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзишский. – М. : Юрид. лит., 1991. – 157 с.
8. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с.
9. Вертузаев М.С. Безопасность компьютерных систем. Комп'ютерна злочинність та її попередження / М.С. Верту-

заев, В.О. Голубев, О.І. Котляревський, О.М. Юрченко / За ред. О.П. Снегірьова. – З. : Павел, 1998. – 316 с.

10. Розенфельд Н.А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж : дис. ... канд. юрид. наук : 12.00.08 / Н.А. Розенфельд. – Київ, 2003. – 222 с.
11. Тіщенко В.В. Теоретичні і практичні основи методик розслідування злочинів : [монографія] / В.В. Тіщенко ; Одеська національна юридична академія. – О. : Фенікс, 2007. – 260 с.
12. Салтєвський М.В. Основи методики розслідування злочинів, скоєних із використанням ЕОМ : [навч. посібник] / М.В. Салтєвський. – Х. : Нац. юрид. акад. України, 2000. – 35 с.
13. Криміналістика : [навч. посібник] / А.Ф. Волобуєв, О.О. Волобуєва, О.А. Самойленко та ін.; за ред. А.Ф. Волобуєва. – К. : КНТ, 2011. – 504 с.
14. Біленчук П.Д. Комп'ютерні злочини: соціально-правові й кримінологічно-криміналістичні аспекти : [навч. посібник] / П.Д. Біленчук, М.А. Зубань. – К. : Укр. акад. внутрішніх справ, 1994. – 72 с.
15. Біленчук П.Д. Комп'ютерна злочинність : [навчальний посібник] / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.
16. Дримлюга Р.І. Інтернет-преступность : автореф. дис. ... канд. юрид. наук : спец. 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» / Р.І. Дримлюга ; Байкальский государственный университет экономики и права. – Владивосток, 2007. – 23 с.
17. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08 «Кримінальне право та криминологія; кримінально-виконавче право» / М.О. Кравцова ; Харківський національний університет внутрішніх справ. – Харків, 2016. – 16 с.
18. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. ... канд. юрид. наук : спец. 12.00.08 «Кримінальне право та криминологія; кримінально-виконавче право» / Д.С. Азаров ; Інститут держави та права ім. В.М. Корецького НАН України. – К., 2002. – 18 с.
19. Голубев В.О. Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту / В.О. Голубев, О.М. Юрченко; під ред. О.П. Снегірьова, М.С. Вертузаєва. – Запоріжжя : Павел, 1998. – 140 с.
20. Крылов В.В. Информационные компьютерные преступления : [учеб. и практ. пособие] / В.В. Крылов. – М. : Инфра-М-НОРМА, 1997. – 285 с.
21. Про основи національної безпеки України : Закон України від 19 червня 2003 р. № 964-IV [Електронний ресурс]. – Режим доступу : <http://zakon2.rada.gov.ua/laws/show/964-15>.
22. Самойленко О.А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : [монографія] / О.А. Самойленко. – К. : КНТ, 2009. – 328 с.
23. Реуцький А.В. Методика розслідування злочинів у сфері виготовлення й обігу платіжних карток : автореф. дис. ... канд. юрид. наук : спец. 12.00.09 «Кримінальний процес і криміналістика; судова експертиза; оперативно-розшукова діяльність» / А.В. Реуцький ; Національна юридична академія імені Ярослава Мудрого. – Х., 2009. – 22 с.
24. Мотлях О.І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : спец. 12.00.09 «Кримінальний процес і криміналістика; судова експертиза; оперативно-розшукова діяльність» / О.І. Мотлях ; Академія праці та соціальних відносин Федерації профспілок України. – Київ, 2005. – 20 с.
25. Анапольська А.І. Розслідування шахрайств, пов'язаних із ними злочинів, учинених у сфері функціонування електронних розрахунків : автореф. дис. ... канд. юрид. наук : спец. 12.00.09 «Кримінальний процес і криміналістика; судова експертиза; оперативно-розшукова діяльність» / А.І. Анапольська ; Луганський університет внутрішніх справ імені Е.О. Дідоренка. – Луганськ, 2008. – 20 с.

26. Біленький В.П. Відповідальність за кіберзлочини за кримінальним правом США, Великобританії й України (порівняльно-правове дослідження) : дис. ... канд. юрид. наук : 12.00.08 / В.П. Беленький. – Одеса, 2015. – 230 с.

27. Голубев В.А. Аналіз кіберзлочинності у сфері економічної безпеки / В.А. Голубев // Information Technology and Security. – 2013. – № 1. – С. 26–32.

28. Літвінов М.Ю. Світова й українська практика боротьби з кіберзлочинністю / М.Ю. Літвінов // Право й безпека. – 2014. – № 1. – С. 85–89.

29. Создание эффективной программы ООН в области предупреждения преступности и уголовного правосудия : Резолюция Генеральной Ассамблеи ООН от 18 декабря 1991 г. № 46/152 [Електронний ресурс]. – Режим доступу : <http://base.garant.ru/2565318/#ixzz4xKtuj3dP>.

30. Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие, как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничество : Справочный документ / 13 Конгресс ООН по предупреждению преступности и уголовному правосудию, Доха, 12–19 апреля 2015 г. (A/CONF.222/12) [Електронний ресурс]. – Режим доступу : http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf.

31. Звіт про результати роботи за 2016 р. Управління ООН із наркотиків і злочинності щодо кіберзлочинності [Електронний ресурс]. – режим доступу : http://www.unodc.org/documents/rpanc/RP_Annual_Report_RU_31.05.17_low.pdf.