УДК 341.24(477+100):[341.48:004]

МІЖНАРОДНО-ПРАВОВІ ПРОБЛЕМИ ВИЗНАЧЕННЯ ТА КЛАСИФІКАЦІЇ «КІБЕРЗЛОЧИНІВ»

Оксана СТОЛЯР,
аспірант кафедри міжнародного права
Львівського національного університету імені Івана Франка

SUMMARY

The article deals with the international legal problems of the definition and classification of cybercrime. The main approaches of domestic and foreign scientists to understanding the concept of cybercrime both from the standpoint of international criminal law and from the standpoint of national criminal law are analyzed. The main criteria for classifying cybercrime are determined through the prism of scientific doctrine and international legal acts. A critical analysis of existing approaches is being carried out and suggestions are made to improve these issues.

Key words: cybercrime, computer crimes, definition, classification, scientific doctrine, international criminal law.

АНОТАЦІЯ

У статті досліджуються міжнародно-правові проблеми визначення та класифікації кіберзлочинів. Аналізуються основні підходи вітчизняних і зарубіжних вчених щодо розуміння поняття «кіберзлочинність» як з позицій міжнародного кримінального права, так і з позицій національного кримінального права. Визначаються основні критерії класифікації кіберзлочинів через призму наукової доктрини та міжнародно-правових актів. Здійснюється критичний аналіз наявних підходів і наводяться пропозиції щодо вдосконалення досліджуваних проблем.

Ключові слова: кіберзлочини, комп'ютерні злочини, дефініція, класифікація, наукова доктрина, міжнародне кримінальне право.

Постановка проблеми. Сучасний підхід до постановки проблеми теми наукової статті полягає тому, що в теорії як міжнародного, так і національного права досі відсутній загальноприйнятний підхід як щодо міжнародного кримінально-правового визначення поняття злочинів, які вчиняються за допомогою комп'ютерів, так і визначення єдиних чітких критеріїв щодо їх класифікації. Внаслідок чого в науковій доктрині можна зустріти цілу низку понять («комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «кіберзлочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин»), які здебільшого мають на увазі той самий вид злочинної діяльності. Така ситуація і визначає необхідність у науковому вивченні проблеми.

Метою статті є дослідження міжнародно-правових проблем визначення та класифікації кіберзлочинів. Аналіз основних підходів вітчизняних і зарубіжних вчених щодо розуміння поняття «кіберзлочинність» як із позицій міжнародного кримінального права, так і з позицій національного кримінального права. Визначення основних критеріїв класифікації кіберзлочинів через призму наукової доктрини та міжнародно-правових актів. Здійснення критичного аналізу наявних підходів та наведення пропозицій щодо вдосконалення зазначених питань.

Виклад основного матеріалу дослідження. Насамперед варто звернути увагу на те, що сьогодні термін «комп'ютерні злочини» вживають доволі часто. Проте більшість вчених надають перевагу терміну тертер«кіберзлочини» [1, с. 52]. Однак саме поняття тлумачиться науковцями по-різному, єдиного визначення поняття «комп'ютерна злочинність» або «кіберзлочинність» немає, проте, зважаючи на їхню суть, можна обидва терміни певною мірою вважати синонімами. Так, деякі автори зазначають, що до комп'ютерної злочинності належать усі протизаконні дії, для яких електронне опрацювання інформації є знаряддям їх вчинення і (чи) засобом [2, с. 14], або всі протизаконні діяння, предметом і засобом здійснення яких є процедури й методи, а також процес комп'ютерного опрацювання даних [3, с. 72].

Водночас сам термін «кіберзлочинність» з'явився в американській доктрині на початку 60-х рр., коли були виявлені перші випадки злочинів, здійснених із використанням комп'ютерів. Він став широко вживатися практичними працівниками правоохоронних органів і вченими, хоча спочатку для цього не було ні кримінологічних, ні правових підстав [4, с.17] .

Перший злочин, здійснений із використанням комп'ютера в колишньому Союзі Радянських Соціалістичних Республік (далі – СРСР), був зареєстрований 1979 р. у Вільнюсі: ним стало розкрадання, збитки від якого складали 78 584 крб. Цей факт був занесений у міжнародноий реєстр правопорушень подібного роду і став своєрідним початком розвитку нового виду злочинів у колишньому СРСР [5, с. 126].

Передусім варто зауважити, що в теорії досі відсутня загальноприйнята кримінально-правова дефініція поняття злочинів, які вчиняються з використанням електронно-обчислювальної машини (далі – ЕОМ). У науковій доктрині можна зустріти цілу низку понять («комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «кіберзлочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин»), що здебільшого мають на увазі ті самі різновиди злочинної діяльності. Зарубіжними дослідниками частіше вживаються поняття "high-tech crime", "cyber crime", "network crime", які відповідно перекладаються як «злочини у сфері високих технологій», «кіберзлочини», «злочини в комп'ютерних мережах» [6, с. 58].

З приводу зазначеного цікавою є думка А.А. Музики і Д.С. Азарова [7], що найбільш дискусійним є питання формулювання теоретичного поняття злочинів у сфері комп'ютерної інформації. Значна кількість вчених відмовилася від його розробки. Так, фахівці у сфері кримінального права Ради Європи під час розробки низки рекомендацій із протидії комп'ютерним злочинам обмежуються тільки переліком таких посягань, прямо посилаючись на непереборні труднощі, які унеможливлюють таке визначення [8, с. 121].

Окрім згаданих, до кіберзлочинів відносять «злочини,

що пов'язані з втручанням у роботу комп'ютерів, і злочини, що використовують комп'ютери як необхідні технічні засоби» [9, с. 11]. Поширене і таке визначення кіберзлочинів: «усі протизаконні дії, під час яких електронне опрацювання інформації є засобом їх вчинення або їх об'єктом» [10, с.65].

Деякі вчені під терміном «кіберзлочин» розуміють злочинне діяння, здійснене в інтернеті, під час якого комп'ютер є або знаряддям, або предметом посягань у віртуальному просторі. Із цього випливає безліч типів кібернетичних злочинів: онлайн-шахрайство, наклеп, зневага, екстремізм у мережі, DoS-атаки, дефейс, поширення шкідливих програм, кардерство, фішинг, комп'ютерне шпигунство та ін. [11, с. 77]. Деякі вчені дають більш широке визначення терміну. Так, П.Д. Біленчук і М.А. Зубань [12, с. 6] вважають, що кіберзлочинність – це «суспільно небезпечна діяльність або бездіяльність, яка здійснюється з використанням сучасних технологій і засобів комп'ютерної техніки з метою завдання шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи» [13, с. 32–37]. В.В. Крилов як альтернативу пропонує ширше поняття «інформаційні злочини», яке дозволяє абстрагуватися від конкретних технічних засобів [14, с. 11]. А.Н. Карахан'ян розуміє комп'ютерні злочини як протизаконні дії, об'єктом або знаряддям вчинення яких є ЕОМ [15, с. 77]. В.В. Лісовий вважає, що основною кваліфікуючою ознакою належності злочинів до розряду комп'ютерних є «електронна обробка інформації», незалежно від того, на якій стадії злочину вона застосовувалася [16, с. 87]. В.О. Голубєв визначає таку ознаку інакше – це «використання засобів комп'ютерної техніки» [17, с. 39]. Є.А. Бідашко і Н.Л. Волкова пропонують і таке визначення кіберзлочинів, як «передбачені кримінальним законом суспільно небезпечні діяння, в яких машинна інформація є або засобом, або об'єктом злочинного посягання» [18, с. 161].

Попри різні підходи до розуміння поняття кіберзлочинності потрібно зауважити, що основною її характеристикою є переважно здебільздзтранснаціональний характер. Тобто той факт, що клієнтами деяких популярних провайдерів, які надають поштові послуги безкоштовно, є мільйони людей на всій планеті, доводить транснаціональні масштаби кіберзлочинності [19].

Оскільки кіберзлочинність є новим видом суспільно небезпечних діянь, то для визначення її особливостей необхідно дослідити основні підходи щодо їх класифікації. Як відомо, класифікація – це розподіл предметів будь-якого роду на взаємопов'язані класи згідно з найістотнішими ознаками, що є властивими для предметів даного роду. Як слушно зазначає М.В. Салтевський, «у кримінальному праві та криміналістиці вид злочину називають не за засобом (знаряддям) вчинення злочину, а за видом злочинної діяльності» [20, с. 4.]. Отже, можна стверджувати, що найважливішою ознакою таких злочинів є їхній об'єкт. Тому визначення видів кіберзлочинів має конструюватися на основі специфічних ознак їхнього родового об'єкта. Оскільки класифікація за родовим об'єктом – це системоутворюючий чинник сукупності норм Особливої частини Кримінального кодексу (далі – КК).

Зважаючи на вищезазначене, деякі вчені виділяють такі види кіберзлочинів і протиправних дій у сфері комп'ютерної інформації:

– насильницькі або інші потенційно небезпечні дії, що посягають на фізичну безпеку, життя та здоров'я людини;

– дії, що порушують конфіденційність даних, циркулюючих в інформаційних і телекомунікаційних системах управління різними об'єктами (такі злочини спрямовані на розкриття важливої інформації без її руйнування, модифікації, знищення, переупорядковування);

– дії, що порушують цілісність даних, їхню доступність для адміністраторів і легальних користувачів (відмова в обслуговуванні), що здатне порушити штатні режими функціонування інформаційних і телекомунікаційних систем різного призначення (такі злочини можуть заподіяти майновий збиток, проте вони не пов'язані з розкраданням інформації, грошових засобів);

– дії, що посягають на майно, майнові права, а також на право власності на інформацію й авторські права;

– дії, що посягають на громадську моральність;

– дії, що посягають на громадську безпеку;

– інші [21,с. 72].

До останніх належать традиційні злочини, які посягають на різні об'єкти, що охороняються законом, але здійснюються з використанням інформаційних і телекомунікаційних систем. До такої групи входять злочини, які могли б бути вчинені і без застосування інформаційних і телекомунікаційних технологій.

Так, в інструктивних матеріалах Інтерполу вживається термін «цифрові злочини» ("digital crime"), які поділяються на три групи: 1) власне комп'ютерні злочини (порушення авторських прав на програмне забезпечення, розкрадання даних, порушення роботи обчислювальних систем, розкрадання комп'ютерного часу тощо); 2) злочини, «пов'язані з комп'ютерами» (переважно фінансове шахрайство); 3) мережева злочинність (використання мереж для здійснення незаконних угод – поширення порнографії, торгівлі наркотиками, ухилення від митних зборів, відмивання грошей тощо) [6, с. 57].

Окрім цього, в одній із наявних класифікацій кіберзлочинів, яка була розроблена на основі міжнародної взаємодії в боротьбі з комп'ютерними злочинами, є кодифікатор робочої групи Інтерпол, що був покладений в основу автоматизованої інформаційно-пошукової системи, створеної на початку 90-х рр. [22, с. 53–54]. Згідно з таким кодифікатором, усі кіберзлочини класифіковані таким чином:

QA – несанкціонований доступ і перехоплення:

QAH – комп'ютерний абордаж (несанкціонований доступ);

QAI – перехоплення за допомогою спеціальних технічних засобів;

QAT – крадіжка часу (ухилення від плати за користування);

QAZ – інші види несанкціонованого доступу та перехоплення;

QD – зміна комп'ютерних даних:

QDL – логічна бомба;

QDT – троянський кінь;

QDV – комп'ютерний вірус;

QDW – комп'ютерний черв'як;

QDZ – інші види зміни даних;

QF – комп'ютерне шахрайство:

QFC – шахрайство з банкоматами;

QFF – комп'ютерна підробка;

QFG – шахрайство з ігровими автоматами;

QFM – маніпуляції з програмами введення-виведення;

QFP – шахрайства з платіжними засобами;

QFT – телефонне шахрайство;

QFZ – інші комп'ютерні шахрайства.

QR – незаконне копіювання:

QRG – комп'ютерні ігри;

QRS – інше програмне забезпечення;

QRT – топологія напівпровідникових пристроїв;

QRZ – інше незаконне копіювання.

QS – комп'ютерний саботаж:

QSH – з апаратним забезпеченням (порушення роботи ЕОМ);

QSS – із програмним забезпеченням (знищення, блокування інформації);

QSZ – інші види саботажу.

QZ – інші комп'ютерні злочини:

QZB – із використанням комп'ютерних дошок оголошень;

QZE – розкрадання інформації, що становить комерційну таємницю;

QZS – передача інформації, що підлягає судовому розгляду;

QZZ – інші комп'ютерні злочини [4 , с. 19–20].

Такий кодифікатор, який використовує під час відправки запитів або повідомлень про комп'ютерні злочини телекомунікаційною мережею Інтерпол, свідчить про широкий спектр скоюваних у сфері комп'ютерної інформації злочинів.

Цікавою є класифікація кіберзлочинів за способами втручання у процес передачі даних: 1) переривання (блокування процесу передачі); 2) перехоплення (неправомірний доступ до передаваних даних); 3) модифікація (неправомірна зміна даних); 4) виготовлення (організація сфальсифікованого сеансу зв'язку) [23, с. 7].

Різні підходи до класифікації кіберзлочинів характерні і для робіт інших вчених. Так, В.Н. Черкасов вказує на чотири основні види таких злочинів: маніпуляції з інформаційною технікою; незаконне використання машинного часу; крадіжка програм; комп'ютерний саботаж [24, с. 34].

В.Є. Козлов виділяє чотири види кіберзлочинів: несанкціонований доступ; зловмисна вірусна модифікація; перехоплення інформації; комбіноване використання. Кожен вид розподіляється на підвиди [25, с. 129].

Зарубіжні вчені намагаються класифікувати всі кіберзлочини за наслідками, спричиненими їх здійсненням, і відповідно до можливих форм уразливості комп'ютерної інформації, таких, як схильність до фізичного знищення, можливість несанкціонованої модифікації, небезпека несанкціонованого отримання інформації особами, для яких вона не призначалася. Виділяються три групи наслідків: 1) спотворення (неправомочна модифікація) даних, 2) просочування інформації, 3) відмова в обслуговуванні (порушення доступу до мережевих послуг) [26, с. 55]. Під час таких злочинних дій порушується цілісність, конфіденційність і доступність інформації [27, с. 75].

Інші іноземні вчені визначають сім груп, які найімовірніше можна віднести до використовуваних способів скоєння злочину: перехоплення паролів інших користувачів; «соціальна інженерія»; використання помилок програмного забезпечення та програмних закладок; використання помилок механізмів ідентифікації користувачів; використання недосконалості протоколів передачі даних; отримання інформації про користувачів стандартними засобами операційних систем; блокування сервісних функцій системи, що атакується [28, с. 159].

Згідно з Конвенцією Ради Європи по боротьбі з кіберзлочинністю, виділяється чотири основні типи кіберзлочинів:

1. Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

– несанкціонований доступ до інформаційного середовища – протиправний навмисний доступ до комп'ютерної системи або її частини, вченений в обхід систем безпеки;

– незаконне перехоплення – здійснене з використанням технічних засобів в обхід заходів безпеки протиправне навмисне перехоплення не призначених для загального доступу комп'ютерних даних, які передаються комп'ютерними системами;

– втручання в дані – протиправна зміна, ушкодження, видалення, спотворення або блокування комп'ютерних даних;

– втручання в роботу системи – протиправне порушення або створення перешкод функціонуванню комп'ютерної системи;

– незаконне використання комп'ютерного і телекомунікаційного устаткування – виготовлення, придбання для використання, поширення або надання доступу в інший спосіб: а) пристрої (зокрема комп'ютерні програми), розроблені або пристосовані для здійснення будь-якого із злочинів першої групи; б) комп'ютерні паролі, коди доступу, інші дані, які забезпечують доступ до комп'ютерної системи або її частини (при наявності намірів використання їх з метою здійснення будь-якого із злочинів першої групи); а також володіння одним із перелічених предметів із наміром використати його для здійснення будь-якого зі злочинів.

2. Шахрайство та підробка, що пов'язані з використанням комп'ютерів:

– підробка документів із застосуванням комп'ютерних засобів – протиправне умисне внесення, зміна, видалення або блокування комп'ютерних даних, що призводить до зниження їхньої достовірності, припускає, що згодом вони розглядатимуться як достовірні;

– шахрайство із застосуванням комп'ютерних засобів – втручання у функціонування комп'ютерної системи з обманним або нечесним наміром умисного протиправного отримання економічної вигоди для себе або для інших осіб.

3. Злочини, пов'язані з розміщенням у мережах протиправної інформації:

– злочини, пов'язані з дитячою порнографією, – поширення дитячої порнографії за допомогою глобальних мереж, пропозиція або надання доступу до неї, отримання для себе або інших осіб за допомогою комп'ютерної системи, зберігання дитячої порнографії в комп'ютерній системі.

4. Злочини щодо авторських і суміжних прав:

– злочини, що порушують авторські та суміжні права – здійснені навмисно, в комерційному масштабі і з використанням комп'ютерної системи злочини щодо прав, передбачених низкою відповідних міжнародних актів [29].

Комітет, який розробляв проект Конвенції по боротьбі з кіберзлочинністю, обговорював можливість включення до типології й інших порушень, пов'язаних із використанням глобальних мереж, таких, наприклад, як пропаганда расизму в Інтернеті. Проте через різні позиції учасники Ради Європи не дійшли згоди щодо питань криміналізації зазначених діянь.

Насамкінець варто погодитись із думкою О.Г. Волеводза, який стверджує, що всі кіберзлочини можна поділити на такі види:

– злочини у сфері комп'ютерної інформації, які посягають на інформаційні комп'ютерні відносини, тобто стосунки, що виникають із приводу здійснення інформаційних процесів виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, поширення та споживання комп'ютерної інформації, створення і використання комп'ютерних технологій і засобів їх забезпечення, а також захисту комп'ютерної інформації, прав суб'єктів, що беруть участь в інформаційних процесах та інформатизації;

– злочини в інформаційному комп'ютерному просторі, які посягають на відносини реалізації прав на інформаційні ресурси (власності та ін.), інформаційну інфраструктуру та її складники (ЕОМ, системи і мережі ЕОМ, програми для ЕОМ тощо);

– інші злочини, для яких характерне використання комп'ютерної інформації або складових її елементів, інформаційного простору під час вчинення діянь, які посягають на інші правовідносини (власності, громадської безпеки та ін.), що охороняються кримінальним законом [4, с. 49–50].

Висновки. Отже, можна стверджувати, що доктринальні підходи вчених до розуміння поняття «кіберзлочин» є різними, не всім імпонує саме цей термін. Проте варто зазначити,

що попри наявні альтернативні дефініції («комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин») саме термін «кіберзлочин» найбільшою мірою відображає суть зазначеного явища.

Щодо класифікації кіберзлочинів можна дійти висновку, що більшість дослідників, які вивчають проблему кіберзлочинності, пропонують поділяти кіберзлочини на види залежно від об'єкту та предмета посягання. Найпоширеніший варіант – це поділ на комп'ютерні злочини та злочини, здійснені за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв для доступу до кіберпростору. Таку класифікацію використовує Організація Об'єднаних Націй, поділяючи згаданий вид злочинної діяльності на кіберзлочини в «широкому» і «вузькому» сенсі. У зазначеному контексті кіберзлочини – це злочини, основним об'єктом посягання яких є конфіденційність, цілісність, доступність і безпечне функціонування комп'ютерних даних і систем. Інші кіберзлочини, окрім комп'ютерних систем, посягають на інші об'єкти (як основні): безпеку суспільства і людини (кібертероризм), майно і майнові права (крадіжки, шахрайства, здійснені за допомогою комп'ютерних систем або в кіберпросторі), авторські права (піратство).

Особливістю Конвенції Ради Європи про кіберзлочинність є те, що вона спочатку поділяла кіберзлочини на чотири групи. Потім, на початку 2002 р. на додаток до Конвенції ухвалили протокол, який доповнює перелік злочинів поширенням інформації расистського й іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що грунтуються на расовій, національній, релігійній або етнічній приналежності. Проте наведена в Конвенції класифікація, на думку низки західних і вітчизняних дослідників, не є всеосяжною: із розвитком науково-технічного потенціалу і громадських відносин в кіберпросторі згаданий список буде, на жаль, розширюватися. До того ж зазначені в Конвенції злочини, пов'язані з деякими, але не з усіма діями, які посягають на громадську безпеку.

Список використаної літератури:

1. Голубєв В.О. Теоретично-правові проблеми боротьби з комп'ютерною злочинністю / В.О. Голубєв // Вісник Запорізького юридичного інституту. – 1999. – № 3. – С. 52–60.
2. Калюжный Р.А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект): автореф. дис. ... д. юрид. наук : спец. 12.00.02 «Конституционное право; муниципальное право» / Р.А. Калюжный ; Институт государства и права имени В.М. Корецкого Академии наук Украины. – К., 1992. – С. 14.
3. Азаров Д.С. Порушення роботи автоматизованих систем – злочини у сфері комп'ютерної інформації / Д.С. Азаров // Право України. – 2000. – № 12. – С. 72.
4. Волеводз А.Г. Противодействие компьютерным преступлениям : правовые основы международного сотрудничества / А.Г. Волеводз. – М. : ООО Издательство «Юрлитинформ», 2001. – 496 с.
5. Батурин Ю.М. Проблемы компьютерного права / Ю.М. Батурин. – М. : Юридическая литература, 1991. – с. 126.
6. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт : [монография] / А.Л. Осипенко. – М. : Норма, 2004. – 432.
7. Музика А.А., Азаров Д.С. Про поняття злочинів у сфері комп'ютерної інформації [Електронний ресурс]. – Режим доступу : http://vvww.crime-research.ru/library/Muzika.html.
8. Голубєв В.О. Організаційно-правові аспекти протидії комп'ютерному терроризму / В.О. Голубєв // Підприємництво, господарство і право. – 2004. – № 7. – С. 121–124
9. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М. : Юридическая литература, 1991. – С. 11.
10. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С та ін. Комп'ютерна злочинність : [навчальний посібник] / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. – К. : Атіка, 2002. – С. 65.
11. Кривогін М.С. Міжнародно-правові аспекти боротьби з кібернетичними злочинами / М.С. Кривогін // Держава і право : теорія і практика : матеріали II междунар. науч. конф. (м. Чита, березень 2013 р.). – Чита: «Молодий вчений», 2013. – С. 77–79.
12. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти : [навчальний посібник] / П.Д. Біленчук, М.А. Зубань. – К. : Українська академія внутрішніх справ, 1994. – С. 6.
13. М.В. Карчевський. Злочини у сфері використання комп'ютерної техніки : [навч. посібн.] / М.В. Карчевський. – К. : Атіка. – 2010. – С. 32–37.
14. Крылов В.В. Информационные компьютерные преступления / В.В Крылов. – М., 1997. – С. 11.
15. Полевой Н.С. и др. Правовая информатика и кибернетика : [учебник] / Н.С. Полевой и др. – М. : Юридическая литература, 1993. – С. 243.
16. Лісовий В.В. «Комп'ютерні» злочини: питання кваліфікації / В.В. Лісовий // Право України. – 2002. – № 2. – С 87.
17. Голубєв В.О. Правові проблеми захисту інформаційних технологій / В.О. Голубев // Вісник Запорізького юридичного інституту. – 1997. – № 2 – С. 39–40.
18. Бидашко Е.А., Волкова Н.Л. Компьютерные преступления: миф или реальность? / Е.А. Бидашко, Н.Л. Волкова // Науковий вісник Дніпропетровського юридичного інституту Міністерства внутрішніх справ України. – 2001. – № 1(14). – С 161.
19. Дванадцятий Конгрес Організації Об'єднаних Націй з попередження злочинності і кримінального правосуддя // Distr. : General 22 February 2009 Russian // Original : English // Сальвадор, Бразилія, 12–19 квітня 2010 р.
20. Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : [навчальний посібник] / М.В. Салтевський. – Х.: Національна юридична академія України, 2000. – С. 4.
21. Казарин О.В., Сальников А.А. Нові актори і безпека в кіберпросторі / О.В. Казарин, А.А. Сальників, // Вісник Московського університету : Політичні науки. – 2010 . – № 2. – С. 71–84
22.Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность / В.Д. Курушин, В.А. Минаев. – М. : Новый Юрист, 1998. – С. 53 – 54.
23. Stallings W. Network and Internetwork Security Principles and Practice. – Prentice Hall, Englewood Cliffs, NJ, 1995. – P. 7.
24. Черкасов В.Н. Борьба с экономической преступностью в условиях применения компьютерных технологий / В.Н. Черкасов. – Саратов, 1995. – С. 34.
25. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью / В.Е Козлов – М. : Горячая линия-Телеком, 2002. – С. 129–143.
26. Cohen F. Protection and Security on the Information Superhighway. – John Wiley &Sons, New York, 1995. – P. 55.
27. Методологические основы обеспечения информационной безопасности объекта // Защита информации. Конфидент. – 2000. – № 1. – С. 75.
28. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security : Repelling the Wily Hacker. – Addison. – Wesley Publishing Company, 1994. – P. 159–166.
29. Конвенція про кіберзлочинність від 23 листопада 2001 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575