Normative-legal field in the field of fight against the crimes accomplished with the use of crime scene cyberspace

Нормативно-правове поле у сфері боротьби зі злочинами, вчиненими із використанням обстановки кіберпростору

Olena Samoilenko

Ключові слова:

боротьба зі злочинами, кіберпростір, кіберзлочин, нормативно-правове поле, криміналізація.

Key words:

fight against, crimes scene cyberspace, ciber crime, normative-legal field, criminalizatsiya.

Постановка проблеми. Відправною точкою для розуміння базових нормативно-правових засад у сфері боротьби зі злочинами, вчиненими в обстановці кіберпростору, є норми міжнародного права, які імплементуються у національне законодавство з міжнародно-правових договорів. Для України це стосується чисельних універсальних та регіональних договорів, які зачіпають питання боротьби зі злочинами у кіберпросторі. Через безмежні можливості використання обстановки кіберпростору з метою вчинення злочинів різної кваліфікації, що призводить до складнощів їх розслідування, постає питання нормативно-правового регулювання сфери боротьби з такими злочинами через призму зв'язку відповідного міжнародного та національного законодавства.

Стан дослідження. Проблемні питання нормативно-правового поля у сфері боротьби зі злочинами, вчиненими з використанням обстановки кіберпростору, висвітлювались у наукових працях багатьох правників (Д.С. Азаров, А.С. Білоусов, В.М. Бутузов, В.Д. Гавловський, В.О. Голубєв, М.В. Карчевський, О.І. Мотлях, Л.П. Паламарчук, Н.А. Розенфельд, Б.В. Романюк, В.П. Шеломенцева та ін.). Втім, для встановлення сучасного світового правопорядку, здійснення розслідування та співробітництва у сфері боротьби з такими злочинами важливим є визначення чинників формування національного нормативно-правового поля у сфері боротьби зі злочинами, вчиненими з використанням обстановки кіберпростору.

Метою статті є дослідження на прикладі України стану національного нормативно-правового поля у сфері боротьби зі злочинами, вчиненими з використанням обстановки кіберпростору.

Виклад основного матеріалу. Системоутворюючим міжнародним актом у сфері боротьби зі злочинами, вчиненими із використанням обстановки кіберпростору, можна вважати прийняту 23 листопада 2001 р. Конвенцію Ради Європи про кіберзлочинність, до якої Україна приєдналась із застереженнями шляхом ратифікації 7 вересня 2005 р. Ця Конвенція стала, по суті, основним моментом у встановленні сучасного світового правопорядку та співробітництва у сфері боротьби з такими злочинами, адже станом на листопад 2017 р. була ратифікована 58 державами, серед яких є всі держави–члени Ради Європи (за виключенням Російської Федерації) та такі, що не входять до європейської спільноти, зокрема Канада, Ізраїль, США, Японія та країни Південної Америки[1]. Конвенція про кіберзлочинність – це договір, за яким держави, що до неї приєднались, зобов'язалися щодо кіберзлочинів зблизити внутрішньодержавні положення кримінального права та створити можливості для застосування ефективних засобів розслідування таких правопорушень. Тому в Конвенції прямо передбачені заходи, що мають здійснюватися на національному рівні в матеріальному кримінальному праві (ч. 1 розділ 2) та кримінально-процесуальному (так званому «процедурному») праві (ч. 2 розділ 2), система міжнародного співробітництва (розділ 3) та питання юрисдикційного характеру (ч. 3 розділ 2).

Зміст міжнародного акта свідчить, що автори Конвенції зважали на необхідність уніфікації національних кримінальних законів, що дасть змогу не просто декларувати у світовій спільноті боротьбу зі злочи-

[1] Таблица подписей и ратификации договора Совета Европы № 185 «Convention on Cybercrime» / [Електронний ресурс]. – Режим доступу : https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dfS8PM6Z.

нами, що вчинені з використанням обстановки кіберпростору, а й вдатися до реального міжнародного переслідування злочинців та розслідування кіберзлочинів. Підтвердженням цього є докладний поділ кіберзлочинів у Конвенції, враховуючи прийнятий в 2003 р. додатковий до неї Протокол, на п'ять груп[2]. Втім, незважаючи на докладний опис на міжрегіональному рівні конкретних складів кіберзлочинів, сутність та перелік правопорушень, що пов'язані з обстановкою кіберпростору, в національних правових системах відрізняються. Не є виключенням й Україна, що вимагає порівняння відповідних норм Конвенції з чинними нормами Кримінального кодексу України (далі – КК).

По-перше, з огляду на те, що Конвенція була ратифікована із застереженнями, в Україні не визнаються кримінально караними окремі конвенційні види злочинів, що стосуються таких діянь: 1) виготовлення, придбання з метою використання, надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створених або адаптованих із метою вчинення будь-якого зі злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (ст. 6); 2) виготовлення і придбання з метою використання предметів комп'ютерних паролів, кодів доступу або таких даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи (ст. 6); 3) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації (п. d, e, ч.1 ст. 9).

По-друге, зважаючи на зміст Конвенції, всі інші запропоновані нею склади кримінальних правопорушень, втілені у КК, враховуючи особливості національної кримінальної політики. Так, окрема частка правопорушень, визначених у Конвенції, отримала закріплення в спеціальних нормах, що об'єднані у Розділі XVI «Злочини у сфері використання ЕОМ (комп'ютерів), систем (далі – АС) та комп'ютерних мереж і мереж електрозв'язку». У ст. 361 КК «Несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» криміналізована більшість конвенційних правопорушень – проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, зокрема незаконний доступ (ст. 2); незаконне перехоплення (ст. 3); втручання в дані (ст. 4); втручання в систему (ст. 5). У ст. 362-1 КК «Створення з метою використання, поширення або збуту шкідливих програмних чи технічних засобів, а також їх поширення або збут» була втілена конвенційна норма щодо зловживання пристроями в частині поширення або збуту шкідливих програмних чи технічних засобів (ст. 6). Варто підкреслити, що, незважаючи на термінологічну відмінність під час формулювання вказаних національних та міжнародних норм, їх семантичний зміст повністю збігається. Відмінність полягає в тому, що автори Конвенції під час формулювання об'єктивної сторони складів правопорушень акцентують на процесі вчинення злочину, а вітчизняний законодавець – на його наслідках, прописуючи в диспозиції певний злочинний результат («призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації»).

Інша ж частина конвенційних правопорушень прописана в традиційних статтях КК, де регламентується використання для вчинення злочину електронно-обчислювальної техніки, мереж, систем, інших апаратних та програмних засобів, таких як: елемент об'єктивної сторони (ст. 200 КК – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима; ст. 176 – порушення авторського права і суміжних прав; ст. 300 – ввезення, виготовлення або поширення творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію) та її кваліфікуюча ознака (ч. 3 ст. 190 – шахрайство із використання електронно-обчислювальної техніки; ч. 4 ст. 301 – ввезення, виготовлення, збут і поширення порнографічних предметів у частині щодо творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію). У цьому контексті акцентуємо, що передбачені Додатковим протоколом до Конвенції дії расистського та ксенофобного характеру, вчинені через комп'ютерні системи, не визначаються у КК України з прямою вказівкою на використання для їх вчинення обстановки кіберпростору. При цьому щодо злочинів расистського та ксенофобного характеру передбачені склади доволі широкої інтерпретації об'єктивної сторони, зокрема: ст. 161 – порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками; ч. 2 ст. 129 – погроза вбивством у частині вчинення з мотивів расової, національної та релігійної нетерпимості; ч. 2 ст. 442 – геноцид у частині публічних закликів до геноциду, а також виготовлення матеріалів із закликами до нього з метою їх поширення. Це дає змогу вбачати наявність криміналізації в національному законодавстві й вказаної групи конвенційних кіберзлочинів.

[2] Конвенції про кіберзлочинність : Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 р. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find=1&text=%F7%E0%F1&x=0&y=4#w11.

По-третє, КК містить кримінальні правопорушення, які є альтернативними до правопорушень, визнаних Конвенцією, тобто, про які в цьому акті не йдеться. До таких спеціальних норм належать правопорушення, визначені у Розділі XVI КК: 1) несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362); 2) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію (ст. 363); 3) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1). До інших альтернативних Конвенції злочинів, що можуть бути вчинені із використанням комп'ютерних технологій, можна віднести порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163); зайняття гральним бізнесом (ст. 203-2); втручання в роботу автоматизованої системи документообігу суду (ст. 376) та інші злочини, у диспозиції яких є пряма вказівка на використання комп'ютерів, систем та мереж для вчинення злочину.

Через наведені позиції можна поставити під сумнів досконалість самої Конвенції про кіберзлочинність. Так, у Конвенції Організації Об'єднаних Націй (далі – ООН) проти транснаціональної організованої злочинності державам рекомендується криміналізація злочинів проти принципів суверенної рівності та територіальної цілісності держав і принципу невтручання у внутрішні справи інших держав, відмивання доходів від злочинів, участі в організованій злочинній групі, корупції, перешкоджання здійсненню правосуддя, вчинених за таких умов: 1) у більш ніж одній державі; 2) в одній державі, але істотна частина його підготовки, планування, керівництва або контролю має місце в іншій державі; 3) в одній державі, але за участю організованої злочинної групи, яка здійснює злочинну діяльність у більш ніж одній державі; 4) в одній державі, але його істотні наслідки мають місце в іншій державі. У п. 29 цієї Конвенції йдеться про програми підготовки персоналу правоохоронних органів в аспекті «методів, які використовуються в боротьбі з транснаціональними організованими злочинами, які вчиняються з використанням комп'ютерів, телекомунікаційних мереж та інших видів сучасної технології». Наприклад, із появою технології криптографічних валют, так званих електронних грошей, створення та обіг яких базується на методах криптографічного захисту інформації, корупційні дії, відмивання доходів від злочинів шляхом застосування такої валюти стали невідслідковуваними для правоохоронних органів. Адже під час обігу таких валют немає єдиного керуючого суб'єкта, ця технологія дає змогу зберігати інформацію про обіг валюти розрізнено на комп'ютерах по всьому світі[3]. Це лише один із прикладів можливостей, що надає кіберпростір для вчинення вказаних злочинів. Тому в Конвенції про кіберзлочинність можна було б вести мову про використання технологій кіберпростору з метою вчинення публічних закликів чи поширення матеріалів із закликами посягання на територіальну цілісність і недоторканність держави, фінансування дій, вчинених із метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону, державної зради, диверсії, шпигунства, легалізації доходів від злочину та інших транснаціональних організованих видів кримінальних правопорушень.

На окрему увагу заслуговує питання про можливість використання кіберпростору з метою вчинення терористичного акту та інших злочинів, що пов'язані з ним, відповідного віднесення універсальним міжнародним актом наведених правопорушень до категорії «кіберзлочини». Кібертероризм як явище та способи протидії йому стали предметом дослідження багатьох науковців (В.М. Бутузов, С.Б. Гавриш, С.О. Гнатюк, В.А. Голубєв, Д.В. Дубов, О.Г. Корченко, В.А. Ліпкан, В.П. Шеломенцев, С. Хилдрет тощо). Проте широке обговорення проблем кібертероризму в міжнародному законодавчому полі знайшло окреме відображення поки у вигляді проектів актів або локальних, двосторонніх міжнародних договорів із питань процедурного права. Країнами Європейського Союзу обговорюється міжрегіональний проект Clean IT, метою якого є організація оперативного реагування у разі загрози акту кібернетичного тероризму[4]. В Україні зачіпають цю сферу боротьби з тероризмом двосторонні договори, укладені з США, Республікою Словенія, Чорногорією, Королівством Бельгія, Королівством Нідерланди.

---

[3] Мащенко П.Л., Пилипенко М.О. Технология Блокчейн и ее практическое применение / П.Л. Мащенко, М.О. Пилипенко // Наука, техника, образование. – 2017. – № 32. – С. 61–64.

[4] Clean IT – Leak shows plans for large-scale, undemocratic surveillance of all communications, 21 sep. 2012 [Електронний ресурс]. – Режим доступу: https://edri.org/cleanit/.

У результаті аналізу положень Конвенції про кіберзлочинність та українського кримінально-правового законодавства ми дійшли висновку, що більшість конвенційних кіберзлочинів в Україні криміналізовані, однак сам процес формування національного нормативно-правового поля у досліджуваній сфері характеризується певними чинниками.

Перший чинник полягає в тому, що національна кримінально-правова охорона тих чи інших прав і свобод людини залежить від наявності суспільної потреби в цьому. Так, в Україні переведення коштів із банківських рахунків клієнтів банку на рахунки комерційних структур або фізичних осіб із подальшим їх зняттям готівкою досить поширено вчиняє оператор банку чи інша службова особа[5]. Тому доцільним було запровадження норм кримінального закону України, які описують склади кіберзлочинів зі спеціальним суб'єктом – особою, яка має право доступу до інформацією, яка оброблюється у кіберпросторі (ст. 362); особою, яка відповідає за експлуатацію комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363).

Другий чинник стосується визнання Україною обов'язковості норм не тільки Конвенції про кіберзлочинність, а й інших багатосторонніх міжнародних договорів, що пов'язані з питанням боротьби зі злочинами, вчиненими із використанням обстановки кіберпростору. Так, на п'ятому пленарному засіданні 12 грудня 2003 р. Всесвітньої зустріч на вищому рівні з питань інформаційного суспільства, відповідно до рішення Ради Міжнародного союзу електрозв'язку (МСЕ) і резолюцій 56/183 і 57/238 Генеральної Асамблеї ООН, вповноваженими від 103 держав, включно й України, одноголосно було прийнято Декларацію принципів[6]. У п. 37 визнано: «Спам становить для користувачів, мереж і загалом для інтернету серйозну проблему, масштаби якої зростають. Питання, що стосуються спаму і кібербезпеки, варто розглядати на відповідному національному і міжнародному рівнях». Відповідно 23 грудня 2004 р., КК був доповнений ст. 363-1 «Перешкоджання роботі ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку», яка, по суті, передбачала кримінальну відповідальність за розсилку спаму, що стало причиною порушення або припинення роботи комп'ютерів, АС, комп'ютерних мереж чи мереж електрозв'язку. За ст. 3 Правил надання та отримання телекомунікаційних послуг, під терміном «спам» розуміють електронні, текстові та/або мультимедійні повідомлення, які без попередньої згоди (замовлення) споживача умисно масово надсилаються на його електронну адресу або кінцеве обладнання абонента, крім повідомлень оператора, провайдера щодо надання послуг[7]. Спам-повідомлення злочинцями досить вдало використовуються з метою несанкціонованого проникнення до електронної системи користувача, викрадення або модифікації інформації, поширення вірусів із різною злочинною метою.

Третій чинник формування національного нормативно-правового поля у сфері боротьби зі злочинами, вчиненими із використанням обстановки кіберпростору, визначається через формування національного галузевого законодавства у сфері забезпечення національної безпеки. Одну з загроз національної безпеки становить саме кіберзагроза. У березні 2016 р. Указом Президента України було введено в дію Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Визначальними позиціями у Стратегії стали шляхи вирішення питань консолідації зусиль у розслідуванні та запобіганні кіберзлочинам різних суб'єктів забезпечення кібербезпеки, зокрема Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції та Національного банку України, розвідувальних органів.

Ми дійшли певних висновків. По-перше, нормативно-правове поле України у сфері боротьби зі злочинами, вчиненими з використанням обстановки кіберпростору, можна вважати доволі сформованим. Питання боротьби зі злочинами, вчиненими з використанням обстановки кіберпростору, в основному врегульоване нормами кримінального та міжнародного права, окремі аспекти боротьби з такими злочинами перебуваютьу нормативно-правовому полі забезпечення національної безпеки.

---

[5] Самойленко О.А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій: [монографія] / О.А. Самойленко. – К.: КНТ, 2009. – С. 54–57.

[6] Письмо Постоянного представителя Швейцарии при ООН от 7 октября 2004 года на имя Генерального секретаря с Приложением Отчета о Женевском этапе всемирной встречи на высшем уровне по вопросам информационного общества, Женева – Palexpo, 10–12 декабря 2003 г. [Електронний ресурс]. – Режим доступу : http://www.un.org/ru/documents/ods.asp?m=%20A/C.2/59/3.

[7] Про затвердження Правил надання та отримання телекомунікаційних послуг : Постанова Кабінету Міністрів від 11 квітня 2012 р. за № 295 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF/page?text=%F1%EF%E0%EC#w11.

По-друге, ефективність української кримінально-правової політики у сфері боротьби зі злочинами, вчиненими в обстановці кіберпростору, можна вважати середньої якості, що загалом відповідає стану законодавства у цій сфері на міжнародному рівні. Таке міжнародне законодавство, як й національне, вимагає уніфікації та гармонізації.

По-третє, порівняльне дослідження українського та міжнародного сегмента кримінально-правових норм, що регламентують відповідальність за кіберзлочин та злочини, вчинені з комп'ютерів, АС та мереж, дають змогу визначити у КК України альтернативні конвенції про кіберзлочинність кримінальні правопорушення, що можуть бути вчинені з використанням обстановки кіберпростору. Зважаючи на зміст диспозицій статей КК України, до таких злочинів належать: дії, спрямовані на насильницьку зміну, повалення конституційного ладу або на захоплення державної влади (ст. 109); посягання на територіальну цілісність і недоторканність України (ст. 110); фінансування дій, учинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110-1); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114); доведення до самогубства (ст. 120); погроза вбивством (ст. 129); вербування людини, вчинене з метою її експлуатації (ст. 149); розбещення неповнолітніх (ст. 156); злочини проти виборчих прав і свобод (ст. ст. 157, 158, 159, 159-1); крадіжка (ст. 185); вимагання (ст. 189); привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем (ст. 191); протидія законній господарській діяльності (ст. 206); легалізація (відмивання) доходів, одержаних злочинним шляхом (ст. 209); незаконне збирання з метою використання відомостей, що становлять комерційну чи банківську таємницю (ст. 231); розголошення комерційної або банківської таємниці (ст. 232); терористичний акт (ст. 258); публічні заклики до вчинення терористичного акту (ст. 258-2) ;створення терористичної групи чи терористичної організації (ст. 258-3); фінансування тероризму (ст. 258-5); придбання чи збут зброї, бойових припасів або вибухових речовин (ст. 263); незаконне придбання, збут наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів (ст. ст. 307, 311); злочини у сфері охорони державної таємниці (ст. ст. 328, 330); незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359); незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376); пропаганда війни й поширення комуністичної, нацистської символіки та пропаганда комуністичного і націонал-соціалістичного (нацистського) тоталітарних режимів (ст. ст. 436, 436-1). Цей перелік не вичерпний через постійний розвиток науково-технічного потенціалу та суспільних відносин у кіберпросторі. Злочини, передбачені Конвенцією про кіберзлочинність та альтернативні ним, що можуть бути вчинені із використанням обстановки кіберпростору, що фактично різні за кримінально-правовими ознаками, утворюють самостійну категорію – злочини, вчинені із використанням обстановки кіберпростору. За неврегульованості цього питання в кримінально-правовому законодавстві, у боротьбі з цією категорією злочинів особливого значення набувають теоретико-методичні засади їх розслідування, що дасть змогу мінімізувати труднощі збирання, дослідження, оцінки та використання доказів, організувати розслідування, враховуючи технологічний та організований транснаціональний характер такої злочинної діяльності.

Анотація

У статті проаналізовано нормативно-правове поле у сфері боротьби зі злочинами, вчиненими із використанням обстановки кіберпростору. Проведено порівняльне дослідження положень Конвенції про кіберзлочинність та положень Кримінального кодексу України. Запропоновано перелік альтернативних конвенційним кримінальних правопорушень у сегменті національного кримінального законодавства.

Summary

In the article the normative-legal field is analysed in the field of borotbi with, by the crimes accomplished with the use of situation of kiberprostranstva. Comparative research of positions of Convention about kiberprestupleniyah and positions of the Criminal code of Ukraine is conducted. The list of criminal offences alternative for Convention in the segment of national criminal statute is offered.

Використана література:

1. Конвенції про кіберзлочинність: Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 г. [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find=1&text=%F7%E0%F1&x=0&y=4#w11.
2. Мащенко П.Л., Пилипенко М.О. Технология Блокчейн и ее практическое применение / П.Л. Мащенко, М.О. Пилипенко // Наука, техника, образование. – 2017. – № 32. – С. 61–64.
3. Письмо Постоянного представителя Швейцарии при ООН от 7 октября 2004 г. на имя Генерального секретаря с Приложением Отчета о Женевском этапе всемирной встречи на высшем уровне по вопросам информацыионного общества, Женева – Palexpo, 10–12 декабря 2003 г. [Електронний ресурс]. – Режим доступу : http://www.un.org/ru/documents/ods.asp?m=%20A/C.2/59/3.
4. Про затвердження Правил надання та отримання телекомунікаційних послуг : Постанова Кабінету Міністрів від 11 квітня 2012 р. № 295 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF/page?text=%F1%EF%E0%EC#w11.
5. Самойленко О.А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій: [монографія] / О.А. Самойленко. – К.: КНТ, 2009. – 328 с.
6. Таблица подписей и ратификации договора Совета Европы № 185 "Convention on Cybercrime" [Електронний ресурс]. – Режим доступу : https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dfS8PM6Z.
7. Clean IT – Leak shows plans for large-scale, undemocratic surveillance of all communications, 21 sep. 2012 [Електронний ресурс]. – Режим доступу : https://edri.org/cleanit.

Olena Samoilenko,
Candidate of Law Sciences, Associate Professor,
Department of Criminalistics,
National University "Odessa law academy"