Солдатова Валерія Дмитрівна,
кандидат юридичних наук
(Харківський національний університет внутрішніх справ)

УДК 343.9.3 (477)

ОКРЕМІ ЗАХОДИ ПОПЕРЕДЖЕННЯ І БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

У статті розглядається характеристика сучасної української кіберзлочинності, дається кримінологічна оцінка її основних показників, визначаються окремі кримінально-правові та кримінологічні заходи попередження і боротьби з кіберзлочинністю.
Ключові слова: мережа Інтернет, кіберзлочинність, заходи попередження та боротьби.
В статье рассматривается характеристика современной украинской киберпреступности, дается криминологическая оценка ее основных показателей, определяются отдельные уголовно-правовые и криминологические меры предупреждения и борьбы с киберпреступностью.
Ключевые слова: сеть Интернет, киберпреступность, меры предупреждения и борьбы.
The article considers the characteristics of modern Ukrainian cybercrime, given criminological assessment of its basic parameters, determined by the individual criminal and criminological measures to prevent and combat cybercrime.
Key words: Internet, cyber crime, measures to prevent and combat.

Постановка проблеми. Стрімке впровадження цифрових технологій в усі сфери людського життя в кінці XX – початку XXI ст. зумовило виникнення нових суспільних відносин. Найбільшу значущість і поширеність здобула технологія Інтернет, яка з'єднала людей по всій земній кулі, зробила комунікації дешевими і безперешкодними, а також відкрила нові горизонти для всього світового співтовариства. Інтернет, останнім часом, дав людині безмежні можливості в області передачі, поширення та розсилки інформації, дозволив виконувати фінансово-банківські операції, незважаючи на відстань і кордони.

В Україні за попередніми оцінками кількість користувачів Інтернету досягла 16,9 млн. і це складає 48 % жителів нашої держави, при тому, що в дослідженні не брали участі мешканці України яким не виповнилося 15 років. Саме тому, можна сказати, що Інтернет став не просто технологією, а унікальним нововведенням, що змінив світ. Інтернет – це місце проведення дозвілля, можливість отримувати різноманітну інформацію та свіжі новини зі всього світу, засіб здійснення трудової діяльності, спосіб знайти однодумця у самому віддаленому куточку земної кулі.

Однак слід зауважити, що крім позитивного ефекту Інтернет містить ряд негативних моментів, зокрема, може завдавати певну шкоду. Деякі особливості даної технології, які допомогли їй поширитися по всьому світу, в той же час створюють сприятливі умови для багатьох видів злочинної діяльності. Новизна суспільних відносин, що виникли в результаті появи Інтернету, і відсутність відповідного правового поля, що стосується даної технології, привели до безлічі проблем, що негативно впливають на становлення відносин у світовій комп'ютерній мережі, заснованих на законі.

Викликає побоювання те, що величезний технічний потенціал і безмежні можливості Інтернет все частіше використовуються в злочинних цілях. До того ж Інтернет, з одного боку, дозволив більш ефективно і безкарно здійснювати раніше існуючі традиційні злочини, а з іншого – породив нові, невідомі світовій спільноті види суспільно небезпечних посягань. Глобальна мережа в останні роки стала використовуватися не тільки для здійснення загальнокримінальних злочинів, але і вкрай небезпечних діянь міжнародного значення – таких як «Мережева-війна», «Інтернет-тероризм», «Інтернет-страйк», що створює загрозу безпеки цілих держав і всього світового співтовариства.

Якщо ще кілька років тому кіберзлочини в Україні здійснювалися рідко, а кіберзлочинність як негативне соціальне явище представляло реальну загрозу лише в майбутньому, то в даний час слід констатувати, що частка мережевої злочинності в структурі українського кримінального світу істотно збільшилася.

Аналіз останніх досліджень і публікацій. Висока латентність, відсутність офіційної статистки та комплексних досліджень кіберзлочинності в Україні призводять до неефективності вироблених заходів попередження, які носять фрагментарний та суперечливий характер, зумовлюючи труднощі у протидії та боротьби з даним видом суспільно небезпечних діянь.

Вважаємо, що за сучасних мінливих умов виникає необхідність у системному і послідовному дослідженні кіберзлочинності в цілому, так і її окремих найбільш поширених видів, а розробка ефективних заходів боротьби та попередження злочинів у Глобальній мережі сприятиме розвитку мережевих технологій в нашій країні.

Питання правових відносин в мережі Інтернет, а також розвиток законодавства в даній області висвітлили у своїх роботах С. А. Бабкін, Ю. М. Батурин, М. С. Вертузаєв, В. О. Голубєв, О. І. Котляревський, В. М. Кравець, В. Г. Лукашевич, Ю. Ю. Орлов, О. І. Сергач, О. П. Снігерьов, Т. Л. Тропіна, В. П. Шеломенцев, О. М. Юрченко.

Кримінологічні дослідження комп'ютерної злочинності проводилися такими російськими вченими, як В. Б. Вехов, М. С. Гаджієв, Д. В. Добровольський, Д. А. Зиков, Р. М. Кашапов, В. В. Колмиков, М. М. Менжег, С. С. Наумов, Л. Н. Соловйов, Є. В. Старостін, Д. Б. Фролов.

За кордоном проблему злочинності в Інтернет розглядали у своїх дослідженнях Б. Уорлі (B. Worly), Д. Л. Шайндер (D. L. Shinder), Д. Чірілло (J. Chirillo), Т. Харді (T. Hardjono), Д. Шрейн та ін. При цьому слід зазначити, що в роботах зарубіжних дослідників кримінологічна та кримінально-правова характеристика кіберзлочинності в Україні взагалі не розглядалася.

Метою статті є виявлення детермінуючих факторів і особливостей характеристики сучасної української кіберзлочинності, кримінологічна оцінка її основних показників, розробка системи кримінально-правових та кримінологічних заходів профілактики і протидії.

Виклад основного матеріалу. Підхід до злочинності як до соціально-негативного явища передбачає відповідну стратегію боротьби з нею в рамках державної кримінальної політики, головними напрямками якої є запобігання вчиненню протиправних посягань, протидія злочинності та формування чітких засобів впливу на злочинність.

У кримінології попередженням злочинності прийнято вважати багаторівневу систему державних і суспільних заходів, спрямованих на виявлення, усунення, послаблення або нейтралізацію причин і умов злочинності, її окремих видів і конкретних діянь, а також на утримання від переходу або повернення на злочинний шлях людей, умови життя і (або) поведінка яких вказує на таку можливість [1, с. 185]. Загальним об'єктом попередження злочинності є умови і причини злочинів і злочинності, а саме криміногенні соціальні явища, що обумовлюють види, стан і динаміку злочинності, а також негативні впливи на мікрорівні.

За спрямованістю та змістом фахівці виділяють такі заходи профілактики на всіх її рівнях: соціально-економічні, організаційно-управлінські, ідеологічні, соціально-психологічні, медичні, психолого-педагогічні, технічні, правові, культурно-виховні та інші (наприклад, екологічного, демографічного характеру) [2, с. 182–183; 3, с. 286–288; 4, с. 119; 5, с. 18; 6, с. 59–64]. Враховуючи детермінуючи чинники та умови кіберзлочинності, ми докладно зупинимося лише на організаційних, технічних, економічних та ідеологічних заходах і окремо – правових заходах попередження і боротьби з кіберзлочинністю.

Організаційні заходи попередження кіберзлочинів прийма-

ються для структурування роботи та взаємодії органів державної влади, прийняття різних рішень з нагляду за діяльністю мережі Інтернет та інформацією, що розповсюджується на її порталах. Виділення питання загальної організації попередження злочинів у Глобальній мережі служить передумовою для вирішення питань про визначення кола суб'єктів, що займаються цією діяльністю, механізму їх взаємодії, повноважень тощо.

Так, відповідно до наказу МВС України «Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС» від 31 травня 2012 року № 494 [7] було створено Управління боротьби з кіберзлочинністю МВС України, котре виступає самостійним структурним підрозділом Міністерства внутрішніх справ України, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, у тому числі організовує та здійснює оперативно-розшукову діяльність. Основними завданнями Управління є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим злочинам та правопорушенням, учиненим з їх використанням. У тому числі: 1) злочинам і правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; 2) злочинам і правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (у сферах платіжних систем; обігу інформації протиправного характеру із використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидія забороненим видам господарської діяльності у цій сфері; надання телекомунікаційних послуг; а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище злочинів) [7, п. 2.1].

Створення єдиної структури, яка контролювала б діяльність і поширення інформації в Інтернет, в даний час просто необхідно. Адже крім боротьби з кіберзлочинністю, яку здійснює Управління боротьби з кіберзлочинністю МВС України, важливо усунути

такий криміногенний фактор, як поширення інформації, що ідеологічно сприяє вчиненню злочинних акцій терористичної, екстремістської, наркотичної, аморальної спрямованості.

Незважаючи на те, що суспільство вимагає державного контролю, необхідно враховувати, що можливості держрегулювання, на думку фахівців, малоперспективні і вельми дорогі, до того ж ще сполучені із значним обмеженням прав і свобод [8, с. 125–127]. Тому в інших державах значна частина боротьби з кіберзлочинністю покладається на комерційні організації. Так, у Китаї, наприклад, за розміщення протиправної інформації несуть відповідальність, перш за все, адміністратори сайтів і провайдери (компанії, які надають доступ в Інтернет), що змушує їх самих стежити за інформацією, розміщеною у них на сайтах.

До *технічних заходів* попередження кіберзлочинів відносять різні засоби і пристосування, що ускладнюють вчинення злочинів. Ці заходи досить докладно викладені в спеціальній літературі. Існують різні класифікації методів технічної протидії кіберзлочинності. Наприклад, А. А. Жмихов ділить технічні заходи попередження комп'ютерної злочинності на три види [9, с. 138–139], по відношенню до кіберзлочинності ці заходи несуть більш спеціалізований характер.

По-перше, апаратні, тобто ті, які безпосередньо захищають технічні пристрої передачі даних від фізичних впливів сторонніх сил, наприклад, перехоплення сигналу в дротяних лініях Інтернет, захоплення переданого бездротовим шляхом сигналу і т. п. Питання безпеки циркуляції сигналів у Інтернет-мережах це не тільки питання боротьби зі злочинністю, але також питання національної безпеки. Оскільки, перехоплення сигналу може погрожувати не тільки обороноздатності, а й також і політичній, і економічній безпеці країни. Практична реалізація даних методів здійснюється за допомогою різних технічних рішень. До них, наприклад, відносяться пристрої екранування апаратури та ліній зв'язку, засоби захисту портів Інтернет-пристроїв та комп'ютерів, підключених до Інтернету. По-друге, програмні заходи попередження призначені для безпосереднього захисту інформації та комунікацій Інтернет. Крім цього за допомогою програмних засобів можна обмежити доступ до тієї чи іншої злочинної інформації, що знаходиться у Інтернет.

Починати необхідно з програмних заходів попередження злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розділ 16 КК України), що здійснюються за допомогою Інтернету, оскільки такі злочини частіше за все виступають пер-

шим та необхідним кроком для здійснення подальших тяжчих злочинів і займають найбільшу частку в структурі зареєстрованих кіберзлочинів. За результатами проведення фахових досліджень, переважна більшість жертв несанкціонованого втручання це ті користувачі Інтернет, які не забезпечені взагалі жодними засобами захисту [10, с. 11–12].

Найчастіше за все несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів) окремих користувачів (ст. 361 КК України) здійснюється, через те, що представник послуг Інтернет (провайдер) не відповідає за безпеку каналу зв'язку, хоча і зобов'язаний це робити. До того ж, більшість користувачів використовує неліцензійне програмне забезпечення, а, отже, і не може звернутися до служби технічної підтримки з питань безпеки. Хоча, в мережі Інтернет завжди можна знайти безкоштовно поширювані (freeware) засоби захисту, за використання яких не треба платити. На жаль, не існує ефективних неліцензійних програмних і безкоштовних засобів захисту від такого виду чисто комп'ютерних злочинів, як поширення шкодоносних програм.

До комплексних програмно-апаратних засобів можна віднести системи логування і відстеження транзакцій за допомогою Інтернет. Часто така діяльність ведеться провайдером: хто, скільки і куди підключився, яка саме інформація і звідки передана. Моніторинг дій, вчинених у системі, необхідний як у профілактичній діяльності для знаходження вразливостей Інтернет-системи, так і для розслідування вже вчинених кіберзлочинів. Представляється, що реалізація технічних заходів можлива лише при відповідній кваліфікації фахівців, пов'язаних з комп'ютерною безпекою. Не можна не погодитись з думкою тих авторів, які вважають, що кваліфікація фахівців з комп'ютерної та Інтернет безпеки принаймні не повинна поступатися кваліфікації зловмисників [6, с. 11].

Економічні заходи. Розглядаючи проблему профілактики кіберзлочинів, не можна не враховувати того факту, що поки залишається великий попит на незаконні послуги кіберзлочинців, серйозних зрушень у боротьбі з мережевою злочинністю не передбачається. Орієнтованість економіки на видобувну сферу і відсталість інформаційно-технічного сектору створюють проблему браку робочих місць для комп'ютерних фахівців.

Розвиток галузі програмного і технічного комп'ютерного забезпечення дозволив би Україні не тільки позбутися залежності від цін на нафту, але й вийти в лідери світової економіки. Нашому потенціалу комп'ютерних фахівців могла б позаздрити будь-яка розвинена країна. Тут можуть зіграти роль державні заходи підтримки бізнесу Інформаційних технологій в Україні, в тому

числі інвестиції в створення нових технологій. Світовий досвід вказує на те, що оптимальному розвитку даної сфери допомогло б надання різних податкових пільг підприємствам і інвесторам, що працюють у цьому секторі, пільгового кредитування за рахунок коштів, закладених в державних та регіональних програмах підтримки підприємництва.

Також негативно впливає на зростання кіберзлочинності висока ціна на програмне забезпечення зарубіжного виробництва і, як наслідок, на зростання так званого піратства, тобто незаконного копіювання і продажу програмного забезпечення в обхід правовласників (ст. 176 КК України). Якби програмне забезпечення продавалося за цінами, що влаштовує максимально широкі верстви населення, то піратства як такого не було б.

Ідеологічні заходи профілактики кіберзлочинності охоплюють цілий комплекс методів і засобів, спрямованих на усунення в певних групах і у певних індивідів антигромадської поведінки, а також на вироблення негативного суспільного ставлення до кіберзлочинців і діянням, вчиненим хакерами. Ідеологічна робота повинна бути спрямована на певну аудиторію. Це можуть бути як і широкі суспільні верстви, так і представники злочинної сфери в мережі Інтернет, а також комп'ютерні фахівці, які володіють технічними навичками та професійними якостями для вчинення кіберзлочинів.

Існує висока імовірність того, що серед комп'ютерних фахівців, що навчаються у вищих навчальних закладах, певна їх частина може стати висококваліфікованими злочинцями, а тому і з ким, як не з ними необхідно проводити профілактичну роботу. На жаль, у більшості вищих навчальних закладів, що готують технічних фахівців, мало уваги приділяється формуванню правової свідомості. Так, всі правові дисципліни в них обмежуються одним семестровим курсом Правознавство, в якому розглядаються питання загального характеру, далекі від кіберзлочинів. Необхідно виробити єдину ідеологічну лінію, обґрунтовану науково, на противагу ідеології, створеної в соціокультурному середовищі хакерів. Тобто пояснення про неприпустимість вчинення кіберзлочинів не повинні обмежуватися тим, що це заборонено законом, а мати під собою ще і серйозну філософсько-моральну базу.

Крім пропагандистських заходів, орієнтованих на комп'ютерних фахівців, слід вживати заходи, які спрямовуються на широку громадськість. Так, наприклад, викликає занепокоєння той факт, що широким верствам населення властиво ідеалізувати кіберзлочинця. Ідеалізація в суспільній свідомості протиправної діяльності хакерів заважає боротьбі з кіберзлочинністю та створює додат-

кові стимули для ведення злочинного способу життя в Глобальній мережі. Так, насамперед необхідно обмежити потік інформації, що популяризує субкультуру хакерів і створює необхідні умови для вчинення кіберзлочинів. Це дозволило б суспільству контролювати формування і розвиток певних груп населення, особливо серед підлітків та молоді, схильних до злочинної поведінки; призвело б до зниження в їх середовищі антигромадських настроїв, поглядів, традицій. Така профілактика служить інструментом попередження конкретних проявів кіберзлочинності шляхом заохочення і стимулювання законного способу життя.

Правові заходи. Також важливим є вирішення проблеми профілактики та боротьби з кіберзлочинністю у правовому полі. Деякі автори вважають, що правові заходи попередження полягають у розробці та прийнятті норм для нейтралізації умов, які сприяють вчиненню конкретних злочинів, стимулюючих до дій, що перешкоджають або припиняють вчинення злочину, а також регламентують процес попередження злочинів [2, с. 184].

На думку Г. М. Міньковського, правові заходи профілактики містять: а) вдосконалення кримінального, адміністративного, трудового, цивільного, сімейного та інших галузей законодавства; б) введення і вдосконалення правових заборон і обмежень, що сприяють попередженню і припиненню виникнення умов для злочинів; в) введення і вдосконалення адміністративно-правових норм, спрямованих на те, щоб заходами стягнення за правопорушення присікти формування звичок і стереотипів поведінки, які в певній ситуації можуть призвести до злочину; г) введення і вдосконалення кримінально-правових норм, так званої подвійної превенції, спрямованих на те, щоб не допустити тяжких та особливо тяжких злочинів шляхом притягнення до відповідальності осіб, які створили сприятливу обстановку для їх вчинення; ґ) введення і вдосконалення норм, що заохочують припинення дій злочинців і самозахист від них; д) заохочення добровільної відмови від виконання підготовлюваного злочину; е) заохочення повного розкриття і виявлення злочинів; є) правову регламентацію діяльності суб'єктів профілактики; ж) виховання правосвідомості з тим, щоб досягти рівня дотримання правових норм за особистим переконанням; з) виховання профілактичної активності громадян та їх готовності допомагати в боротьбі зі злочинністю; и) нормативне закріплення стандартів безпеки від злочинів [12, с. 194–195]. Ми згодні з тим, що дана класифікація найбільш повно розкриває основні напрямки попередження в сфері кіберзлочинів, а активному використанню цивільно-правових, адміністративно-правових заборон, форм попередження перетворення правопо-

рушень в злочини, також має бути відведено відповідне місце в системі заходів профілактики.

Метод впливу на злочинність за допомогою адміністративних санкцій допоміг би попередженню і припиненню умов виникнення кіберзлочинів. Наприклад, було б дієвим заходом введення адміністративної відповідальності за поширення інформації, що сприяє вчиненню кіберзлочинів, а також коштів для їх здійснення, за винятком спеціалізованих порталів та друкованих видань, розрахованих на фахівців з комп'ютерної безпеки. За допомогою адміністративного впливу можна було б також обмежити поширення інформації, що закликає до вчинення комп'ютерних злочинів.

До цих пір не піднято питання про кримінальну відповідальність за рекламу виготовлення, переробки або перевезення наркотичних речовин. Приклади в КК України є – так, за незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів передбачена кримінальна відповідальність за ст. 307 КК України. Високу суспільну небезпеку представляють спеціалізовані Інтернет-сайти, створені для споживачів і наркоторговців.

Введення норм КК і КУпАП, спрямованих на боротьбу з Інтернет-сайтами, які пропагують асоціальний і злочинний спосіб життя, сприяло б вирішенню такого завдання правової профілактики, як формування законослухняної правосвідомості [13, с. 18]. Представляється, що зменшення кількості прозлочинної інформації в мережі знизило б число людей, психологічно готових до вчинення злочинів.

У більшості випадків при використанні Інтернету для вчинення злочинів їх суспільна небезпека зростає. По-перше, злочини можуть охоплювати невизначене велике коло потерпілих. По-друге, використання Інтернету створює відчуття безкарності в силу віддаленості вчиненого діяння від злочинця та складнощів у його розшуку і припиненні злочинної поведінки. А отже, вчинення злочину за допомогою мережі Інтернет обтяжує як суб'єктивну, так і об'єктивну складові суспільно небезпечного діяння забороненого кримінальним кодексом. Тому, на наш погляд, є всі передумови для введення в КК України нової обтяжуючої обставини – вчинення злочину за допомогою комп'ютерної мережі, з додаванням відповідних кваліфікуючих ознак, тяжкість яких збільшується при використанні мережі Інтернет, інших комп'ютерних мереж чи мереж електрозв'язку.

Висновок. З урахуванням викладеного пропонується додати до Кримінального кодексу в порядку de lege ferenda такі зміни, а

саме доповнити Розділ 16 Кримінального кодексу України статтею 363-2:

Ст. 363-2. Рекламування наркотичних засобів, психотропних речовин або їх аналогів

1. Незаконні рекламування чи пропаганда наркотичних засобів, психотропних речовин або їх аналогів, – караються ...

2. Ті самі діяння, вчинені за допомогою публікації матеріалів у комп'ютерній мережі або засобах масової інформації, – караються ...

Підсумовуючи, зауважимо, що існуючі заходи боротьби зі кіберзлочинністю є неефективними, про це свідчить швидке зростання даної категорії правопорушень. Пов'язано це не тільки з неефективністю окремих заходів, але перш за все і з відсутністю цілісної системи адміністративних, кримінально-правових, кримінологічних заходів, спрямованих на протидію кіберзлочинності. Саме тому, лише комплексний підхід з нейтралізації причин та умов кіберзлочинності, а також ефективна державна кримінальна політика в цій сфері здатні зупинити швидкий розвиток цього негативного явища.

Список використаних джерел:

1. Криминология: учебник для студентов вузов / под науч. ред. Н.Ф Кузнецовой, В. В. Лунева. – 2-е изд., перераб. и доп. – М. : Волтерс Клувер, 2005. – 640 с.

2. Криминология : учебник для вузов./ Под ред. д.ю. н. В. Н. Бурлакова, д.ю. н. Н. П. Кропачева. – СПб. : Санкт-Петербургский государственный университет, Питер, 2004. – 427 с.

3. Криминология : учебник / под ред. В. Н. Кудрявцева, В. Е. Эминова. – 2-е изд., перераб. и доп. – М. : Юристъ, 1999. – 512 с.

4. Терещенко Б. Л. Предупреждение преступлений, посягающих на интеллектуальную собственность : дис. … канд. юрид. наук: 12.00.08 / Терещенко Б. Л. – М., 2005. – 217 с.

5. Безпека комп'ютерних систем: злочинність у сфері комп'ютерної інформації та її попередження / Вертузаєв М.С., Голубєв В.О., Котляревський О. І., Юрченко О. М. / під заг. ред. О. П. Снігерьова. – Запорізький юридичний інститут МВС України, Національна академія внутрішніх справ України. – Запоріжжя : ПВКФ «Павел», 1998. – 315 с.

6. Снігерьов О. П. Деякі правові проблеми злочинності в сфері комп'ютерної інформації / Снігерьов О. П., Сергач О. І. // Інформаційні технології та захист інформації. Збірник наукових праць. – Міністерство внутрішніх справ України. Запорізький юридичний інститут. – Випуск № 1. – 1998. – С. 59–64.

7. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС [Електронний ресурс] : наказ МВС України від 31 травня 2012 року № 494. – Режим доступу: http://document.ua/pro-organizaciyu-dijalnosti-upravlinnja-borotbi-z-kiberzloch-doc103883.html. – Назва з титул. екрану.

8. Бытко С. Ю. Некоторые проблемы уголовной ответственности за

преступления, совершаемые с использованием компьютерных технологий : дис. … канд. юрид. наук: 12.00.08 / С. Ю. Бытко. – Саратов, 2002. – 204 с.

9. Жмыхов А. А. Компьютерная преступность за рубежом и ее предупреждение : дис. … канд. юрид. наук: 12.00.08 / А. А. Жмыхов. – М., 2003. – 178 с.

10. Голубєв В. О. Інформаційна безпека: проблеми боротьби із злочинністю у сфері використання комп'ютерних технологій / за заг. ред. д.ю. н. професора Р. А. Калюжного / Голубєв В. О., Говловський В. Д., Цимбалюк В. С. – Запоріжжя : Просвіта, 2001. – 257 с.

11. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Изд-во «Наука и техника», 2004. – 384 с.

12. Криминология : учебник / под ред. проф. Н. Ф. Кузнецовой, проф. Г. М. Миньковского. – М. : Изд-во БЕК, 1998. – 566 с.

13. Лукашевич В.Г. Реформування чинного законодавства з питань кримінальної відповідальності за злочини в сфері комп'ютерної інформації / Лукашевич В.Г., Голубєв В. О. // Інформаційні технології та захист інформації : зб. наук. праць ; Міністерство Внутрішніх Справ України, Запорізький юридичний інститут. – Випуск № 1.– 1998. – С. 14–28.

Надійшла до редакції 04.11.2012