Bohatyrov I.G. Confiscation of property – for and against

The article raised issues of confiscation of property as a form of punishment, which to some extent dependent on the degree of scientific elaboration, the adequacy of legal regulation and the effectiveness of its practical application. Follows the legal technique, we can attest, that confiscation of property, as a form of criminal punishment, meets chapter 2, Art. 50 of the Criminal Code, which provides for purpose of punishment under it is a punitive effect on the convicted person has a significant impact on corrections and prevents convicted of new crimes as prisoners as others. However, we believe, that the confiscation of property, as an additional form of punishment, compared with the principal, is a complementary means of coercive influence on the convict, and not always used, and only then when there is a need lightweight aggregate punishment achieve the goals. The author states: First, the crime rate in Ukraine determines the need for use of court confiscation of property as a form of punishment; Secondly, based on critical analysis of current legislative provisions and the views of scientists criminologists proposed the following doctrinal definition confiscation of property – a measure of compulsion applied for the State by a court to a person convicted of a criminal offense and is prescribed by law limiting its ownership of the removal of all or part of the property; Thirdly, comparing the degree law qualifications and confiscation of rights in property consider it rather harsh form of punishment. This constant is the fact that nowadays the importance of property rights for individuals is higher compared with the right of free choice of the type of employment; In-fourth, there is a need for separating confiscation as criminal penalties as administrative punishment and as a form of enforcement of civil – legal obligations.

Key words: *confiscation of property, punishment, scientific development, the legal framework, practical application, right of property.*

УДК 342.951

О.І. Богучарова,
С.А. Комісаров

БЕЗПЕКА КІБЕРНЕТИЧНОГО ПРОСТОРУ ЯК ЕКОЛОГІЧНОГО СЕРЕДОВИЩА ТА ОСЕРЕДКУ ВЧИНЕННЯ ЗЛОЧИНІВ

Проаналізовано проблему утвердження сучасного кібернетичного (інформаційного) простору як предмета теорії та практики оперативно-розшукової діяльності. Зроблено огляд підходів до його визначення через урахування особливостей «кіберпростору» при виборі дієвих стратегій оперативно-розшуковіх заходів. Запропоновано розуміння кіберзлочинності як екологічного злочину, а кіберпростору – як специфічного «інформаційного екологічного середовища» (environment), на яке певні особи можуть усвідомлено й зловмисно впливати (взаємодіяти) аж до його руйнування, знищення, спричинення йому та його об'єктам/суб'єктам суттєвої шкоди, небезпечної для їх функціонування або здоров'я. Також зазначено необхідність визначення цифрового суверенітету країни в правовій площині та безпекових заходів із його посилення.

Ключові слова: *екологічне середовище, екологічне право, кіберпростір, комп'ютерна злочинність, контент, оперативно-розшукова діяльність.*

Постанова проблеми. Поняття «простору» завжди вважалося поняттям суто географічним. Звісно, географічні «простори», або території розглядалися також і як предмет політики й політичних відносин та фігурували в більшості міжнародних конфліктів. Але все змінилося в ХХ сторіччі з появою радіо, телебачення, а згодом й Інтернету. Саме в цей час ідею «простору» було перетворено на ключове поняття та своєрідний мейнстрім наукової думки, зокрема й у сфері правоохоронних і правознавчих наук. Сталося це за умов виникнення нової «просторової реальності» – інформаційного простору й кіберпростору, які хоч й не в змозі замінити географічний простір, однак здатні стати середовищем й цілком реальним місцем вчинення злочинів, наприклад, несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), пропагандистського «промивання мізків» й навіть кібератак на державні установи, зокрема й сайти Міністерства внутрішніх справ (МВС), Генеральної прокуратури тощо.

До речі, оцінюючи сучасний стан злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж в Україні, необхідно зазначити її негативну динаміку, тобто поступове й неухильне зростання цього виду злочинів. Притому, як слушно зазначають учені, офіційна статистика відображає не стільки стан злочинності, скільки стан її реєстрації в державі. Тож можна припустити, що реальний стан злочинності у сфері використання електронно-обчислювальних машин (комп'ютерів) набагато вищий.

Зрозуміло, що зовсім невипадково дедалі активніше порушується проблема посилення цифрового суверенітету країни. Оскільки, окрім вищезазначеного, останнім часом, зважаючи на складну ситуацію на Сході України, де наявні порушення основного права людини – права на життя, особливу увагу в правоохоронних органів при формуванні оперативно-розшукових заходів, пов'язаних із віртуальним простором, викликає контроль за так званим контентом у соціальних мережах та блогах, який усе частіше демонструє людиноненависницьку ідеологію, відкриті обговорення та заклики щодо вбивства окремих осіб, професійних груп фахівців і цілих поселень або народів. Звідти, аналізуючи ті повноваження, що надаються ЗМІ у ХХІ сторіччі, зокрема й Інтернет-виданням, науковці засвідчують, що їх роль у сучасному суспільстві має полягати в їх правомірному управлінні аудиторією, позбавленої шкідливого впливу на суспільні відносини.

Отже, з одного боку, комп'ютерна злочинність та комп'ютерний тероризм, поширення невластивих українській культурі традицій і цінностей, культу насильства й жорстокості, порнографії, пропагування наркотично узалежненого способу життя як єдине «правильного» для молодої людини, зневажливого ставлення до людської та національної гідності,

попри зростаючу кібернетичну небезпеку, ще не мають належного висвітлення в правознавчій літературі. З іншого боку, термінологічна невизначеність, слабка нормативно-правова оснащеність, методологічна «неприписаність» злочинних дій з інформацією в чинному КП і КПК України, труднощі кваліфікації, що виникають при проведенні оперативно-розшукових заходів, потребують розширення досліджень у галузі антикримінального інформаційного простору й кіберпростору.

Аналіз останніх досліджень і публікацій. Незважаючи на значний науковий й суспільний інтерес проблематика інформаційного простору та кіберпростору, як і кіберзлочинності в правовій площині, а також оперативно-розшуковій діяльності є маловивченою. Термінологічні дослідження інформаційного простору й кіберпростору знайшли належне відображення у працях західних учених Л. Вентц, Д.Ф. Крамер, Д. Куел, Дж. Ліпман, М. Лібіцкі, М. Мацубара. У сфері правових та інших наук цій тематиці присвятили свої праці й вітчизняні вчені В. Бик, А. Климчук, Д. Дубов, А. Марченко, О. Манжай, М. Ожеван, В. Панченко, В. Петров, В. Пилипчук, М. Погорецький, О. Порфимович, Ю. Федорова, В. Шеломенцев та ін.[1; 4; 5; 6; 8; 12]. Причому в працях В.Бебика, Н. Власенко, О. Гриценко, В. Іванова, Т. Костецької, О. Литвиненко, І. Слісаренко, О. Сосніна, Д. Швеця, Т. Шульги, Д. Яковлева та інших сучасних дослідників піддані глибокому аналізу зміни, що відбуваються у співвідношенні різних гілок влади, зокрема й інформаційної, виявлені її місце і роль у демократичному суспільстві [7]. Проте деякі із зроблених висновків втратили актуальність і потребують перегляду. Тим більше, що питома вага цих праць опублікована для висвітлення політичного впливу інформаційної влади й насамперед її головних носіїв – засобів масової інформації (ЗМІ) – на всі сфери суспільного життя, їх сприянню розвиткові процесів глобальної демократизації тощо. Водночас правоохоронний аспект залишається поза увагою науковців. Варто при цьому зважити на такі факти: перехід до реальної розбудови інформаційного суспільства в Україні, оновлення основних засад українського інформаційного законодавства, урахування темпів значного приросту українських Інтернет-користувачів (2011–2012 рр. рекордне збільшення – 34%; 2012–2013 рр. – 16%) [2].

Через це доречно вказати на остаточне формування національної моделі українських ЗМІ (четвертої влади – інформаційної), яке відбулося завдяки викладенню у новій редакції Закону України «Про інформацію», прийняттю Законів України «Про захист персональних даних» та «Про доступ до публічної інформації», відповідно до яких фактично знято питання ототожнення «інформаційної влади» та ЗМІ. Разом із тим негативні інформаційні впливи, а також поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України та її громадянам і високопо-

садовцям, поки що залишаються поза увагою як провідних українських ЗМІ, так і науковців.

Ураховуючи вищезазначене, підкреслимо, що на сьогодні залишаються невирішеними нагальні правові питання, що унеможливлює формалізацію антикримінальної, або карної кіберполітики: досі відсутні системні нормативно-правові документи, у яких було б надано чітке визначення основних термінів у сфері кібербезпеки, зокрема й міжнародні; не визначено правовий статус кіберпростору; відсутній консенсус щодо правил поведінки в кіберпросторі; відсутня загальноприйнята методологія оцінки наслідків кіберзлочинів.

Формування цілей. Однією з вихідних проблем запропонованого дослідження є утвердження сучасного кібернетичного (інформаційного) простору як предмета теорії та практики оперативно-розшукової діяльності та виявлення підходів щодо врахування цього «простору» при побудові дієвих стратегій оперативно-розшукових заходів.

Мета публікації полягає в тому, щоб на підставі літературного огляду розглянути визначення кіберпростору як особливого інформаційного екологічного середовища, яке водночас може бути осередком підготовки та вчинення злочинів. Останні завдають шкоди кіберпростору як екологічному середовищу, а також можуть наносити непоправну шкоду як його нематеріальним «об'єктам», порушуючи їх функціонування аж до знищення й руйнування, так і його «реальним суб'єктам» – провайдерам, користувачам, людським організаціям й установам, завдаючи їм фінансових, матеріальних збитків або шкоди здоров'ю. І саме тому ці кримінальні дії й вчинки потребують правової кваліфікації та дієвого правоохоронного реагування.

Виклад основного матеріалу. На сьогодні відбулися зміни в правовому полі, також й у чинних КП і КПК України щодо розуміння принципів роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. На думку вчених, загальні зміни в законодавстві, й особливо ті, що стосується сфери боротьби з комп'ютерними злочинами, стали наслідком не стільки технічного прогресу або розвитку технологій, скільки фундаментальних перетворень правових концепцій. Адже до середини XX століття правові системи в більшості випадків захищали право власності на «матеріальні» об'єкти. Однак поява інформаційного суспільства призвела до зростання важливості захисту саме «нематеріальних об'єктів» та особливого правового «об'єкта» – інформації. Ці нові «об'єкти» зрештою потребували прийняття нових правових норм, оскільки не могли бути захищені за аналогією з динамікою злочинних дій у сфері матеріальних об'єктів. На жаль, на заваді цьому захисту сьогодні в першу чергу стає термінологічна невизначеність щодо понять «кіберпростір», «кіберзлочинність», «кібербезпека».

Притому, як констатують науковці, оцінюючи стан «кіберзлочинності» в Україні та розробляючи засади з методології оцінки наслідків кіберзлочинів, а також дієві оперативно-розшукової заходи з протидії їй, необхідно враховувати як потужну динаміку, так і високу латентність цього виду злочинів. Наведемо лише декілька цифр. Так, якщо у 2013 році злочинів щодо несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України) було зафіксовано 408, то лише за січень-квітень 2014 року обліковано 140 таких кримінальних правопорушень. Водночас, наприклад, у 2009 році було зареєстровано 96 таких випадків, 2010 році – 87, 2011 році – 67, 2012 році – 83 кримінальних злочини. Теж саме й щодо несанкціонованих дій з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях подібної інформації, що вчинено особою, яка має право доступу до неї (ст. 62 КК України). У 2013 р. – 152 злочини, тоді як лише за січень-квітень 2014 р. обліковано 23 таких кримінальних правопорушень [9; 10].

Отже, створенню ефективних правових механізмів протидії кіберзлочинних дій і кіберзлочинам, кіберзагрозі різних рівнів складності заважають як термінологічна, так і нормативно-правова недосконалість у сфері кіберпростору, а також їх висока латентність.

Однак, попри значну термінологічну невизначенність, наявні нормативно-правові суперечності, однією з ключових проблем у формуванні тезаурусу сфери антикримінальної кібербезпеки є все ж таки визначення поняття «кіберпростору» з акцентом на розумінні першої його частини, а саме – «кібер». Зараз активно обговорюється це поняття в мілітарній площині, особливо західними, російськими та китайськими фахівцями [11]. США як країна з найбільшим рівнем інтернет-проникнення в усі сфери життя суспільства чи не найбільше опікується проблемами інформаційного простору й кіберпростору. У доповіді, підготовленій для Б. Обами під керівництвом А.Дж. Льюїса, доводиться, що «кіберпростір – це більше, ніж просто мережа Інтернет, і включає всі мережеві форми та цифрову діяльність» [3, с. 11]. Автори дослідження «Кібермогутність і національна безпека», одним із яких є відомий фахівець у цій галузі Д. Куел, звертають увагу на те, що зміст поняття кіберпростір може бути визначений по-різному. Теж саме й щодо поняття «кібербезпека». Щоправда, останнім часом у змісті цього поняття пропонується розглядати не лише технічні чинники, а й людський фактор як провідний – ворожі інсайдерські дії, людські помилки, владні відносини [4].

Вітчизняні науковці, досліджуючи це поняття в юридично-правовохоронній площині, зазначають дещо інше. Так, О. Манжай подає

його визначення таким чином: «Це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем та управління людьми цими технічними (комп'ютерних) системами» [6, с. 145]. Напротивагу такому визначенню кіберпростору А. Погорецький та В.Шеломенцев вважають, що це «штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворено в результаті функціонування кібернетичних комп'ютерних систем управління й оброблення інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання електронних послуг, ведення електронної комерції тощо)» [8, с. 80].

Отже, як в мілітарній, так і юридично-правовій та правоохоронній площині єдиного концептуального розуміння поняття кіберпростору, тим більше антикримінального, і досі так й не сформовано.

Зважаючи на зазначене, пропонуємо розглянути іншу, другу частину цього поняття, а саме – поняття «простір», що може роз'яснити засадові ідеї поняття «кіберпростір».

Це поняття переважно розробляється в термінологічних працях зарубіжних учених. У вітчизняних роботах щодо інформаційних електронних (комп'ютерних) систем простір розуміється як загальне поняття, що «схоплює» певні соціальні, психологічні, правові ознаки буття людини. Водночас у зарубіжних працях існує принаймні три його тлумачення: domain, realm, environment [3; 11].

Як констатують американські й європейські вчені, перше поняття – переважно постає в його просторово-географічних характеристиках. Відтак саме завдяки поняттю domain описуються земля, вода, повітря, космос як окремі простори. Частіше всього його застосовують в мілітарній проблематиці як «поле» вірогідного протистояння та кіберборотьби, а також в політичний – як кіберполітику щодо нової цифрової реальності.

У свою чергу, поняття realm поширене в навколонауковій і публіцистічній літературі, а також загальних працях із постмодерністської тематики. Тобто його зміст досить далекий від юридико-правових теорій.

Environment як поняття надає певних характеристик «простору» «навколишнього середовища», яке можна «відчути» на собі, та на яке можна впливати аж до його знищення, як й руйнування певних його частин. Притому впливати (взаємодіяти) усвідомлено й зловмисно, спричинюючи йому та його «об'єктам/суб'єктам» суттєвої шкоди. Припускаємо, що саме цей вимір найбільш вписується в нормативно-правове поле ан-

тикримінальної політики й кіберзагроз різних рівнів складності.

Енвайронментальний правовий підхід, на нашу думку, дозволяє створити ефективну методологію оцінки протиправних дій і кіберзлочинів, до того ж указує на можливий ефективний правовий механізм протидії кіберзлочинності, оскільки дозволяє за аналогією з базовими засадами екологічного права подолати термінологічну та нормативно-правову недосконалість у сфері кіберпростору.

Оскільки завдяки цьому тлумаченню кіберпростору як environment, або інформаційне «навколишнє середовища», на яке певні особи можуть впливати аж до його знищення, застосовуючи ці дії як щодо його об'єктів, так і суб'єктів, то стає можливим інкримінувати будь-якій особі такі дії. Звідти дії щодо завдання шкоди інфраструктурі, пошкодження або знищення зв'язків усередині неї чи зовні, матеріальні збитки, спричинені внаслідок цих дій, а також специфічний контент (заклики до повалення влади, пропозиції щодо прекурсорів, порнографія, військовий контент) можуть розглядатися як кримінальні, що порушують внутрішню або зовнішню екологію кіберпростору. Тим самим вони підпадають під правовий розгляд в суді або в кримінальному провадженні щодо наслідків цих дій для самого середовища як системи та осіб чи особи (суб'єкти, зокрема, користувачі, провайдери, організації), яким завдається екологічна шкода такою інформаційною кібернетичною кампанією, діями, вчинками тощо.

Через призму такого підходу по-новому постають й завдання ОВС і взагалі співробітників правоохоронної діяльності з боротьби у сфері злочинних дій щодо інформаційної безпеки країни.

Зокрема, науковці визначили не тільки базові поняття «об'єктів» інформаційного простору й кіберпростору, а також і чинники, що негативно впливають на забезпечення кібернетичної безпеки країни, серед яких:

– прискорені темпи розробки й використання засобів несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем;

– постійні спроби неправомірного використання та блокування інформаційних ресурсів як своєї, так й іноземних держав;

– протиправні посягання на критичну інфраструктуру інформаційного простору й кіберпростору;

– дії, спрямовані на домінування в інформаційному просторі, ведення кібератак, здійснення тиску та інформаційних війн.

Саме ці чинники мають опинитися в полі діяльності сучасних правоохоронців. У зв'язку із цим слід послатися на термінологічні праці та роботи щодо інформаційної влади західних науковців (Д. Куел), які зазначають, що кіберпростір має три виміри: під'єднаність (інфрастуктурний); контент (дії з інформацією); когнітивну спрямованість (маніпулятивного психологічного впливу). Останній вимір кіберпростору є начебто

найбільш привабливий для вільних користувачів, оскільки вміщує освітній, пізнавальний аспект. Адже завдяки його можливостям можна впливати на прийняття рішень людини, що, зокрема, можна побачити при застосуванні технологій «обробки» свідомості вільних користувачів за допомогою маніпулятивних інформаційних психотехнологій, таких як нейролінгвістичне програмування (НЛП, скор.) [1; 3; 4].

Притому, як констатує один із відомих зарубіжних науковців, М. Кавеллі, украй потрібно визначення кіберконфлікту за ступенем загрози, яку він має справляти в системі внутрішньої кібербезпеки. Так, учений пропонує розглядати такі їх види: *кібервандалізм, Інтернет-злочини, кібершпигунство, кібертероризм, кібервійна*. Для нас тут важливим є перші два види кіберконфліктів, що стосуються функціонування інформаційних електронних (комп'ютерних) систем у правоохоронній площині [4].

Кібервандалізм є найпоширенішою формою кіберконфлікту, що отримує суспільний резонанс. Зазвичай він включає зміни чи знищення змісту веб-сайту, відключення чи перезавантаження серверу, як це відбулося при закритті, наприклад, відомого українського файло-обмінника, коли «впали» урядові сайти, зокрема й МВС. Однак, незважаючи на свій шкідливий характер, наслідки таких інцидентів обмежені в часі та відносно незначні. Зовсім інший характер мають *Інтернет-злочини*, що спрямовують діяльність певних осіб переважно для отримання безпосереднього фінансового зиску. Це стосується «обнуління» чи пограбування рахунків банківських установ, налагодження зв'язків наркотрафіку або продаж курсорів і прекурсорів, торгівлі людьми, винайму комбатантів, розповсюдження дитячої порнографії тощо. Повний перелік Інтернет-злочинів ще мають скласти правники, тому не варто сподіватися, що лише ці злочини повинні опинитися в провадженнях правоохоронців, оскільки часто зовсім невідомі наслідки інших, начебто «простих» Інтернет-правопорушень.

Звісно, кіберпростір працює з усіма трьома вищевказаними вимірами – під'єднаність (інфраструктурний), контент (дії з інформацією), когнітивна спрямованість (маніпулятивного психологічного впливу), але в українському законодавстві щонайбільше чітко представлений тільки інфраструктурний аспект, який забезпечує «роботу», тобто функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Однак, скажімо, щодо контенту та впливовості на свідомість (психотехнології, як наприклад, НЛП), то в чинному КП України кваліфікацій явно бракує.

«Фільтром» у таких випадках можуть слугувати заходи з викриття злочинних дій щодо *контенту* або *маніпулятивного психологічного впливу* на аудиторію, інакше – у вільних користувачів Інтернету сформуються не лише неправильні установки та погляди на цінності, а й можливо, кіберз-

лочинні установки. Енвайронментальний правовий підхід, на нашу думку, саме у цих випадках дозволяє створити методологію оцінки Інтернет-злочинів. У суспільстві кіберпростір «працює» із різним змістом інформації, формою її подання, унаслідок чого виникає низка проблем, таких як: достовірність та надійність інформації, її вплив на свідомість користувача. Перевірити надану інформацію мережею Інтернет майже неможливо, адже не завжди є дані про авторів, що займаються розробкою та розповсюдженням інформації, на відміну від друкованих джерел інформації.

На противагу традиційним підходам якраз у понятті «контенту» можна встановити екологічний зміст, що може бути шкідливим або навпаки корисним для молодого покоління, особи. Невипадково в західній психологічній літературі операціоналізоване поняття «екологічна майстерність» як психотехнічно компетентне вміння встановлювати позитивні контакти з навколишнім оточенням, що може бути використано й у юридично-правовій площині. Зокрема, застосування полярної категорії – «інформаційно-екологічна зловмисна майстерність» як психотехнологічно компетентне, майстерне і злочинне вміння руйнувати зв'язки й позитивні контакти в інформаційному екологічному оточенні, наносити шкоди, зловмисно впливати на нього, його об'єкти / суб'єкти та налагоджувати зловмисні контакти та зв'язки в ньому для фінансового чи іміджевого зиску.

Особливі дії з приводу контенту отримали після скандалу зі Е. Сноуденом, що привернуло увагу до безпеки даних, передусім, персональних. Звісно європейські інституції відразу кваліфікують «фільтрування» як поширення «китайського підходу». Але навіть більшість громадян (Європи та США) не заперечують використання урядом технологій моніторингу та фільтрування мережевого трафіку, а також можливість певних служб мати доступ до їхніх особистих поштових серверів. І це незважаючи на суворе дотримання європейцями права вільного обміну думками, інформацією тощо.

«Фільтрування» контенту та встановлення контролю за Інтернет-трафіком у таких випадках може слугувати «конституційність» заходів із викриття злочинних дій. Оскільки вбачається, що в умовах інформаційного суспільства відносини владної субординації, засновані на принципі «влада-підкорення», поступово мають зникати, натомість суттєвого поширення мають зазнати відносини інформаційної субординації як втілення принципів «допуску до інформації», «доступу до джерела інформації», «розпорядження інформацією», «цільового користувача інформації» тощо.

Висновки. Отже, у запровадженні ефективної системи оперативно-розшукової діяльності в кіберпросторі досить відчутною стає відсутність належної законодавчої бази та координації діяльності відповідних відомств. Підкреслимо те, що на сьогодні залишаються невирішеними нагальні

правові питання, що унеможливлює формалізацію антикримінальної карної кіберполітики. У запровадженні ефективної системи оперативно-розшукової діяльності, крім того, заважає відсутність навіть визначення уповноваженого органу в правовій площині. До цього додається потреба підготовки досвідчених фахівців-правоохоронців із питань захисту інформації та протидії кіберзлочинності; на жаль, низький рівень фінансування оперативно-розшукової діяльності в цій правовій площині не сприяє їх становленню. У сфері фіксації кіберзлочинів наявна також висока залежність України від програмних і технічних продуктів іноземного виробництва, що не може не позначатися на якості практичних оперативно-розшукових заходів, над усуненням чого потрібно працювати невідкладно як у теорії, так і в практиці оперативно-розшукової діяльності.

Зважаючи на вищевказане, енвайронментальний правовий підхід, на нашу думку, де кіберпростір розглядається як один із вимірів «environment» – тлумачення, що є поширеним у зарубіжних працях -, дозволяє створити ефективну методологію оцінки протиправних дій і кіберзлочинів, до того ж указує на можливий ефективний правовий механізм протидії кіберзлочинності, оскільки дозволяє за аналогією з базовими засадами екологічного права подолати термінологічну та нормативно-правову недосконалість у сфері кіберпростору.

Використані джерела:

1. Бутузов В. М. Протидія комп'ютерній злочинності: деякі аспекти міжнародного досвіду (на прикладі діяльності правоохоронних органів США та Німеччини) / В. М. Бутузов // Інформаційна безпека: людина, суспільство, держава. – 2009. – №1. – С.30–38.

2. У 2013 році кількість Інтернет-користувачів в Україні склала половину населення [Електронний ресурс]. – Режим доступу : http://www.unian.ua/society/846299-v-2013-/rotsi-kilkist-internet-koristuvachiv-v-ukrajini-sklala-polovinu-naselennya.html. – Назва з екрана. – Дата звернення : 20.04.15.

3. Доклад правительственных экспертов по достижениям в сфере информатизаций и телекоммуникаций в контексте международной безопасности [Электронный ресурс] / Организация Объединенных Наций ,Нью-Йорк. – 2012. – 57с. – Режим доступа : http://www.un.org/disarmament/HomePage/DAPublications/DisarmamentStudySeries/PDF/DSS_33_Russian.pdf.

4. Дубов Д. В. Підходи до формування тезаурусу у сфері кібербезпеки / Д. В. Дубов // Політичний менеджмент. – 2010. – №5. – С. 19– 30.

5. Евтихевич Н. С. Концепция «безопасности личности и общества» : канадский подход [Електорнний ресурс] / Н. С. Евтихевич, Е. В. Исраелян. – Режим доступу : http://www.imemo.ru/files/File/magazines/puty_miru/2013/13008_02.pdf.

6. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай // Право і безпека. – 2009. – №4. – С. 42–149.

7. Комісаров О. Г. Роль та місце інформаційної влади в сучасному держа-

вному управлінні / О. Г. Комісаров// Науковий вісник Дніпропетровського держуніверситету внутрішніх справ. – 2012. – № 1. – С. 308–317.

8. Погорецький М. Поняття кіберпростору як середовища вчинення злочинів / М. Погорецький, В. Шеломенцев // Інформаційна безпека людини, суспільства, держави. – 2009. – № 2 – С. 77–81.

9. Статистична звітність форми № 1 (річна) «Єдиний звіт про злочинність» // Офіційний веб-сайт Міністерства внутрішніх справ України [Електронний ресурс]. – Режим доступу : http://www.mvs.gov.ua/mvs/control. – Назва з екрана. – Дата звернення : 23.04.15.

10. Моніторинговий кримінологічний аналіз злочинності в Україні (2009–2013 роки) : [моногр.] / [Є. М. Блажівський, І. М. Козьяков, О. О. Книженко та ін.]. – К. : Національна академія прокуратури України, 2014. – 484 с.

11. Понимание киберпреступности : руководство для развивающихся стран [Електронний ресурс]. – Режим доступу : http://www.itu.int/dms_pub/itu.-d/oth/01/0B/D0/D010B0000073301/ PDFR.pdf.

12. Порфірович О. Віртуальний криміналітет: від хакера до терориста (портрет явища) / О. Порфірович // Актуальні питання масової комунікації. – Вип. 9. – 2008. – С.25–34.

Богучарова Е.И., Комисаров С.А. Безопасность кибернетического пространства как экологической среды и центра совершения преступлений.

Проанализирована проблема становления современного кибернетического (информационного) пространства как предмета теории и практики оперативно-розыскной деятельности. Осуществлен обзор подходов к его определению в связи с учетом особенностей «киберпространства» при выборе действенных стратегий оперативно-розыскных мероприятий. Предлагается понимание киберпреступности как экологического преступления, а киберпространства – как специфической «информационной экологической среды» (environment), на которую определенные лица могут осознанно и умышленно воздействовать (взаимодействовать) вплоть до ее разрушения, уничтожения, причинения ей и ее объектам/субъектам существенного вреда, опасного для их функционирования либо здоровья. Также отмечена необходимость определения цифрового сувернитета страны в правовой плоскости и мероприятий в сфере безопасности по ее усилению.

Ключевые слова: *киберпространство, компьютерная преступность, контент, оперативно-розыскная деятельность, экологическая среда, экологическое право.*

Bogucharova O. I., Komisarov S.A. safety of cybernetic space as ecological environment and place of committing a crime

Background. In spite of considerable scientific and public interest Ukranian's Cybercrime problems, in particular in operatively-search activity and also in the frame of Ukranian's legitimate institute system as whole are insufficiently studied. Up today many urgent questions are unresolved, that does impossible formalization the principles of ukranian's anticriminal (criminal) internal affairs ministry' cyberpolitik law. There

aren't normatively legal law documents, including international, in which basic juridical terms on securing our nation's cyber infrastructure, its content, information-psyological actions in cyberspace, its legal status and consensus as to its conduct' law rules would be given. The generally accepted legislative-juridical law estimation cybercrime' methodology is not determinated too. Toward the single secure European cyberspace and in order to biuld Ukrainian legitimate institute of operatively-search activity for juridical scientists are necessary to examine the principles to combat high-tech crimes. *Objective.* The main purpose of the current study is aimed to theoretical-analytical research principles to combat high-tech crimes which are under the operatively-search activity investigation' rules. Also the legislative-juridical conceptual approach on the base of ukrainian ecological law is aimed to preposed. *Method.* Legislative-juridical conceptual approach and theoretical-analytical observation for applied questions from operatively-search activity' point of view are choosen. *Results.* Toward the single secure European cyberspace and Ukrainian legitimate institute of operatively-search activity there are some negative/positive factors for the creation of possible effective legal counteraction mechanism. It is passing to the real alteration of informative society in Ukraine, update of basic principles of the Ukrainian informative legislation, considerable growth rates of Ukrainian Internetusers. Terms «domain», «realm», «environment» are investigated. Also some aspects of the legislative-juridical estimation cybercrime' methodology and main principles to combat high-tech crimes as one of «environment's» measurings are investigated too. That's its environmental interpretation is widespread in foreign but not national legislative, juridical and military analytical literature. That analytical research and literature observation allow formalization the principles of internal cyberpolitik's law, creates effective legal counteraction mechanism as to antilaw actions and cyberattacs. Besides specifies a cybercrimes by analogy with the ecolaw's base principles and overcomes legal-normative terminology imperfection in the cyberspace. *Conclusion.* Conceptual environmental legal-juridical approach is described in this paper. The principles to combat high-tech crimes as environmental aspect crime are proposed.

Key words: *ecological law, environmental legislative-juridical approach, cybercrimes, cyberspase, iternet-crimes, high-tech crimes, operatively-search activity.*

УДК 343.37+343.45

В.М. Бровко

ПРОБЛЕМИ СПІВВІДНОШЕННЯ ЗЛОЧИНІВ, ПЕРЕДБАЧЕНИХ ст. 209-1 КК УКРАЇНИ, З ОКРЕМИМИ ЗЛОЧИНАМИ У СФЕРІ СЛУЖБОВОЇ ДІЯЛЬНОСТІ

Статтю присвячено дослідженню специфіки співвідношення злочинів, передбачених у ст. 209-1 Кримінального кодексу України, з урахуванням змін, що відбулися в конструкції складів цих злочинів, з окремими злочинами у сфері службової діяльності, ознаки яких мають подібний конкретний зміст, та визначенню типів співвідношення цих злочинів.

Ключові слова: *запобігання легалізації, службова недбалість, зловживання повноваженнями.*