criminal case, are hard to overestimate for our research, and they are decisive. However, on the assumption that the category of the witness's credibility to this or that degree was discussed in the works of processualists grounded not on the concepts of the materialistic dialectics, but the latter was the one which during the Soviet epoch of the development of the national testimony theory and till this day caused almost complete exclusion from the scholarly circulation of the credibility category in favor of the objective truth.

This, to our point of view, requires considering of the scholarly experience of the processualists, who chose other philosophical concepts as a methodological basis for studying the issues of the witness's credibility, in particular, the ones contained in the witnesses' testimony. Which means that being on the platform of the materialistic dialectics shows the restrained conservatism i.e. openness to the perception of the scholarly achievements of other methodological platforms of the testimony research in the criminal proceeding, in particular, during the studying of the issues of witness credibility and the methods of its clarification in the criminal proceeding.

Key words: *methodology; evidence; credibility; witness testimony; utilitarianism, humanism, skepticism, materialism, philanthropy, rigorism, empirism, rationalism, materialistic dialectics, relativism.*

Стаття надійшла 7 липня 2017 р.

УДК 343.3/7

О. Р. Пелещак

КІБЕРДИВЕРСІЯ ЯК ФОРМА СУЧАСНОЇ ДИВЕРСІЙНОЇ ДІЯЛЬНОСТІ

Досліджено питання, пов'язані з визначенням поняття «диверсія» та її поділом на окремі види. Запропоновано класифікацію нових форм диверсійних актів у сучасних умовах. Виокремлено кібердиверсію як форму сучасної диверсійної діяльності.

Обґрунтовано необхідність узгодження ст. 113 Кримінального кодексу України (диверсія) з іншими статтями (злочини у сфері використання комп'ютерів).

Ключові слова: *національна безпека, гібридна війна, диверсія, гібридна диверсія, кібердиверсія.*

Постановка проблеми. Глобалізація та розвиток інформаційних технологій суттєво вплинули на технологію ведення сучасних війн, невід'ємним елементом яких стали диверсії, скоєні за допомогою кіберпростору. Проте загальна кримінально-правова норма, що передбачає відповідальність за диверсію, хоч й відповідає положенням су-

часної науки кримінального права і вимогам демократичного суспільства та має на меті захист національної безпеки України, однак є надто обмеженою щодо вияву окремих форм (способів і засобів їх здійснення) об'єктивної сторони диверсійної діяльності. Так, науковцями, які досліджують поняття «диверсія», створена умовна класифікація, згідно з якою існують диверсії в різних сферах, проте форми сучасних диверсій є практично не дослідженими. Серед основних причин обмеженого підходу вчених до їх дослідження є такі: 1) практична складність доведення належними і допустимими доказами факту диверсійної діяльності, яка охоплюється диспозицією ст. 113 Кримінального кодексу України (далі – ККУ), наслідком чого є розслідування скоєних диверсій за іншими статтями чинного кримінального закону; 2) негативні прояви так званого «людського фактора», які полягають у практичній зацікавленості слідчих підрозділів у більш стислих строках досудового слідства та передачі обвинувального акта в судові інстанції. Звісно, до таких дій слідчих спонукають «показники», тому, щоб отримати хороші результати проведеного досудового слідства, працівники слідчих органів, обирають ту статтю кримінального закону, яку «простіше» застосувати до підозрюваної особи та довести це належними засобами доказування.

Отож захист інтересів держав і громадян у кіберпросторі стає життєво важливим завданням, яке перетворює безперешкодне використання комп'ютерних мереж на питання безпеки й оборони. З 2014 року очевидно, що диверсійна діяльність загалом і кібердиверсійна діяльність зокрема загрожують системам вітчизняного державного та військового управління, економіці й промисловості, життю і здоров'ю громадян України.

Якщо розглядати загалом технології ураження систем життєзабезпечення і критично важливої військово-економічної інфраструктури, то найефективнішими, безсумнівно, є кібердиверсії, що вчиняються в поточних операціях з контролю над ресурсами. І, як свідчить світовий досвід, це твердження давно перейшло з категорії гіпотез у категорію стійкої практики. Зрозуміло, що контроль і перехоплення управління або виведення з ладу промислового обладнання, автоматизованих систем управління, об'єктів військової інфраструктури – найважливіші завдання, які вирішуються в результаті вчинення кібердиверсій.

Незважаючи на доволі незначну частку серед суспільно небезпечних діянь, величезна потенційна небезпека кібердиверсії зумовлена тим, що навіть одиничний кібердиверсійний акт може завдати серйозних збитків економіці нашої держави, сповільнити темпи будівництва та введення в експлуатацію окремих підприємств, порушити рит-

мічність роботи тієї чи іншої галузі економіки, розпалювати національну та релігійну ворожнечу, не кажучи про оборонний комплекс нашої держави. Крім того, такі злочинні акції заподіюють злочинну морально-політичну шкоду.

Тому практичне існування новітніх форм диверсійної діяльності та їх можливий потужний негативний вплив на основи національної безпеки України потребують кримінально-правового наукового дослідження для впорядкування внутрішнього нормативно-правового поля.

Стан дослідження. Диверсія й основні форми її вчинення стали об'єктом наукових досліджень таких учених, як О. О. Климчук, О. Д. Довгань, В. Г. Хлань, В. С. Картавцев, О. О. Черноног, О. І. Манартович, О. А. Чуваков та ін. Аналіз напрацювань низки науковців дає змогу дійти висновку, що дослідження диверсійної діяльності з позиції кримінально-правової науки здебільшого зосереджені на загальній характеристиці елементів складу цього злочину й лише деякі з них, детальніше вивчають форми об'єктивної сторони злочину, передбаченого ст. 113 ККУ.

Огляд дисертацій та монографій за 2000–2016 рр., в яких досліджувалися проблеми кримінально-правової відповідальності за диверсійну діяльність, показав, що лише окремі аспекти злочину, передбаченого ст. 113 ККУ, ставали предметом наукових розробок. Наприклад, розглянуто окремі питання притягнення до кримінальної відповідальності за диверсії проти здоров'я громадян у дисертації Є. В. Фесенка [2]. Певною мірою відповідальність за диверсійну діяльність досліджується у працях В. С. Картавцева [3], О. Ф. Бантишева й О. В. Шамари [4], Ю. В. Луценка [5].

У дисертації О. О. Климчука розглянута проблематика притягнення до кримінальної відповідальності за диверсійну діяльність [6]. Зокрема науковцем проведено юридичний аналіз складу злочину, передбаченого ст. 113 ККУ, досліджено особливості притягнення та звільнення від кримінальної відповідальності за диверсійну діяльність, розмежовано поняття об'єктів, що мають важливе народногосподарське й оборонне значення.

Однак поза увагою науковців залишилися нові форми такої суспільно небезпечної поведінки, як диверсійна діяльність й нові підходи до оцінки рівня небезпечності тих її форм, що відомі. Проте ці новітні форми є значно небезпечнішими за своїми злочинними наслідками, адже загалом у сучасному світі сформувалася ситуація, коли, з одного боку, деякі країни мають кіберзброю (а країни-агресори, скажімо РФ, її активно використовують), а, з іншого – основні інформаційні

системи інших держав, серед яких, на жаль, й Україна, відкриті для нападу.

Якщо в стандартній війні застосовуються диверсії та кібердиверсії, то у гібридній війні простежуємо нові явища правової дійсності – гібридні диверсії та кібергібридні диверсії.

Тому необхідними є наукові дослідження, спрямовані на впорядкування і теоретичних положень, і законодавчих визначень щодо нових форм диверсійних проявів, а також на відмежування їх від суміжних кримінально-правових категорій, насамперед від таких, як бандитизм, тероризм.

Мета статті полягає у визначенні таких понять, як гібридна диверсія та кібердиверсія, а також здійсненні класифікації нових форм диверсійних актів у сучасних умовах. Для цього потрібно виконати такі *завдання*: проаналізувати сукупність ознак, характерних рис та істотних особливостей, що визначають сутність поняття «кібердиверсія»; провести умовну класифікацію диверсійних актів залежно від засобів й способів їх учинення в сучасних умовах.

Також практичним завданням цієї наукової публікації є показати зв'язок ст. 113 ККУ з іншими статтями ККУ, насамперед зі ст.ст. 361, 361-1, 361-2, 362, 363, 363-1, які передбачають покарання за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку.

Виклад основних положень. Перед тим, як безпосередньо розглянути сучасні форми диверсійної діяльності, проаналізуємо понятійний апарат диверсії як злочину проти основ національної безпеки.

Відповідно до Великого тлумачного словника сучасної української мови, диверсія (від лат. *diversio* – відхилення, відвернення) – 1) акт зруйнування або пошкодження об'єктів військового, державного значення агентами ворожих країн або народними месниками у тилу окупантів; 2) воєнна операція, здійснювана для відвернення уваги противника від місця, де готується головний удар [7].

Щодо наукових дефініцій аналізованого поняття, то можна стверджувати, що наука кримінального права сформувала порівняно узгоджену позицію стосовно визначення диверсії. Зокрема О. М. Литвак під диверсією розглядає сукупність ознак, характерних рис та істотних особливостей, які притаманні диверсії як воєнно-політичній та правовій категорії, котрі становлять її внутрішній зміст, що дає можливість розглядати диверсію, як злочин, який насамперед спрямований на ослаблення держави та спричинення великої шкоди її економічній системі [8]. Однак, попри цей, здавалося б, усталений підхід, кримінально-правова наука продовжує продукувати численні визначення поняття

диверсійної діяльності, які, на нашу думку, не містять фундаментальних розбіжностей, а основна полеміка науковців триває навколо численних ознак предметів складу диверсії, що характеризують диверсійну діяльність, адже сукупність таких ознак у їх взаємозв'язку та взаємообумовленості характеризує диверсію як злочин, що вчиняється. Наприклад, деякі дослідники вважають, що диверсія – це діяння, яке спрямоване проти держави й її громадян і вчиняється щоб підірвати устрій та порядок, власне, на території країни [9].

Щодо нормативного закріплення аналізованого поняття, то у ст. 113 ККУ під диверсією розглядається вчинення з метою ослаблення держави вибухів, підпалів або інших дій, спрямованих на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, на зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення, а також вчинення з тією самою метою дій, спрямованих на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій [1]. Зауважимо, що майже аналогічна дефініція диверсії містилася в Кримінальному кодексі УРСР. За сучасних умов таке трактування ускладнює правозастосування положень ст. 113 ККУ на практиці.

Серед наукового загалу також є критичні зауваження стосовно такого законодавчого трактування диверсійної діяльності. Наприклад, О. А. Чуваков уважає правильнішим визначення диверсії, яке використовує у своїх звітах Держдепартамент США, за яким під диверсією розуміють умисне, політично мотивоване насильство, що вчиняється проти сторони, яка не воює, наднаціональними групами або таємними агентами з метою впливу на громадськість. Своєю чергою, його структурний орган, Бюро по боротьбі з диверсіями, під диверсією розуміє «…погрозу застосування або застосування насильства в політичних цілях окремими особами або групами, які діють або в підтримку, або проти встановленої урядової влади, коли призначення таких дій полягає у тому, щоб приголомшити або залякати обрану групу, більш ширшу, ніж безпосередні жертви» [10].

Огляд наукових праць з окресленої проблематики свідчить, що розгляд цих предметів більшість науковців здійснює не систематизовано та сукупно з предметами, які опосередковано визначені в диспозиції зазначеної норми.

Так, В. С. Картавцев уважає, що об'єктом диверсії можуть бути життя та здоров'я людей, землі, моря, водоймища, річки, ліси, парки, гаї, важливі споруди і комунікації народногосподарського чи оборонного значення (фабрики, заводи, мости, греблі, вокзали, електростанції,

газопроводи, склади тощо), стада тварин, риби, молюски, рослини (посіви на кореню) [11]. Практично аналогічну позицію займають О. О. Дудоров та Є. О. Письменський [12].

Інші вчені (О. Ф. Бантишев та О. В. Шамара) об'єктом диверсії визначають об'єкти, що мають важливе народногосподарське чи оборонне значення, об'єкти тваринного і рослинного світу, довкілля (зауважимо, що зміст цих понять авторами не розкрито) [13].

Дещо розширене тлумачення предмета диверсії подає М. І. Хавронюк, який відносить до нього: земельні угіддя, водойми, ліси, стада та колекції тварин, риби, що водяться у ставках та інших водоймищах, великі пасіки, посіви сільськогосподарських чи інших культур, будівлі, споруди й інші об'єкти, які мають важливе народногосподарське чи оборонне значення, від діяльності яких залежить життєдіяльність певних регіонів чи інших великих територій, належне функціонування певних галузей економіки, структур державного управління, зокрема підприємства, зруйнування чи пошкодження яких саме собою є фактором небезпеки [14].

Отже, предметами, що безпосередньо визначені у ст. 113 ККУ, та у більшості наукових праць, є об'єкти, які мають важливе оборонне та народногосподарське значення. Однак чинне вітчизняне законодавство не містить нормативного визначення поняття «об'єкт народногосподарського значення». На наш погляд, це радянський рудимент, який абсолютно незаслужено «перекочував» із радянського кримінального кодексу в кримінальний закон незалежної України.

Зазначимо, що в умовах незалежності та розвитку суспільних відносин поняття народного господарства втратило юридичне підґрунтя (термін «народне господарство» відповідав суспільно-економічним відносинам радянської доби за часів існування виключної монополії держави на суспільне виробництво). З прийняттям Основного Закону України відбулося закріплення державної, комунальної та приватної власності і власності Українського народу (земля, її надра, атмосферне повітря, водні та інші природні ресурси, які знаходяться в межах території України, природні ресурси її континентального шельфу, виключної (морської) економічної зони) (ст.ст. 13, 41 Конституції України). Крім того, у ч. 1 ст. 325 та ч. 2 ст. 81 Цивільного кодексу України зазначено, що суб'єктами права приватної власності, крім фізичних осіб, є також юридичні особи, що поділяються залежно від порядку їх створення на юридичні особи приватного права (підприємницькі товариства тощо) і юридичні особи публічного права (державні підприємства, навчальні заклади тощо), які держава може створювати безпосередньо або брати участь в їх діяльності (чч. 2–3 ст. 167 ЦК України). Такі ж

права надані територіальним громадам. У першому випадку йдеться, зокрема, про комунальні підприємства, навчальні заклади тощо, у другому – про різні підприємницькі товариства тощо (чч. 2–3 ст. 169 ЦК України).

Як бачимо, з одного боку, існує чимала кількість об'єктів різних форм власності, які здійснюють той чи інший вид діяльності й можуть бути предметами, внаслідок зруйнування або пошкодження яких ослабиться держава. Проте не всі об'єкти можна визнавати такими, що мають важливе значення для держави в контексті ст. 113 ККУ: наприклад, об'єкти юридичних осіб, що здійснюють страхову діяльність, операції з нерухомим майном або задіяні у сфері мистецтва, спорту, розваг чи відпочинку тощо.

Отож застосування у диспозиції ст. 113 ККУ терміна «народногосподарське значення» не відповідає вимогам сьогодення й ускладнює кваліфікацію диверсії. Вважаємо за необхідне законодавцю внести зміни у диспозицію ст. 113 ККУ, вилучивши з неї слова «народногосподарське значення» та замінити їх на «важливе соціально-економічне та інше значення».

За такого підходу під соціально-економічним значенням для держави відповідних об'єктів пропонуємо розуміти саме їх соціальну (лікарні, санаторії ВНЗ, школи тощо) та економічну діяльність, головними характеристиками якої є витрати на виробництво, процес виробництва та випуск продукції, а сама вона полягає у процесі виробництва продукції (товарів і послуг), що здійснюється з використанням певних ресурсів: сировини, матеріалів, устаткування, робочої сили, технологічних процесів тощо.

Своєю чергою, під об'єктами, що мають інше важливе значення, треба розуміти, зокрема, засоби масової інформації й інші об'єкти матеріального світу, які залежно від конкретного прояву зазначеного злочину та умов його вчинення можуть мати важливе значення для держави (об'єкти юридичних осіб, що здійснюють діяльність у сфері телекомунікацій, будь-яка інформація, критичні об'єкти національної інформаційної інфраструктури тощо).

Поділ диверсійних актів на форми, як і будь-яка інша класифікація, мають певною мірою умовний характер. Але виокремлення конкретних ознак тих чи інших форм диверсії є необхідним для надання більшої цілеспрямованості та систематизації правотворчої діяльності у цій сфері.

Найбільшу небезпеку, на думку О. А. Чувакова, становлять такі форми диверсії [10]:

– фінансування диверсійно-терористичної діяльності;

– використання в диверсійних цілях вибухових пристроїв, зброї (зокрема біологічної, хімічної, радіаційної);

– використання інформації, яка містить державну таємницю; залучення у диверсійну діяльність громадян та організацій, так зване вербування агентів, створення агентурних мереж; використання комерційних, суспільних і релігійних організацій;

– провокація воєнних, релігійних, міжетнічних конфліктів;

– використання службового, суспільного становища або посадових повноважень;

– використання засобів масової інформації, зокрема мережі Інтернет, спеціальної літератури тощо.

Наведений список не є вичерпним. Окрім того, варто зазначити, що головною метою диверсійного акту за чинним законодавством є навмисне послаблення того чи іншого елементу безпеки чи обороноздатності держави. Однак мета диверсії, на переконання більшості науковців, не обмежується вказаними в законі об'єктами. Тому О. А. Чуваков пропонує класифікувати диверсію на:

– економічну;

– політичну;

– ідеологічну;

– диверсії, що спрямовані на розпалення національної та релігійної ворожнечі, на порушення територіальної цілісності держави;

– кібердиверсію (наприклад, хакерські атаки на сайти органів державної влади) та ін. [10].

В аспекті нашої статті вважаємо за необхідне серед інших видів диверсійних актів детальніше розглянути особливий вид диверсії, який стосується комп'ютерів та комп'ютерних мереж – кібердиверсії.

Водночас зауважимо, що явище кібердиверсії часто застосовується в умовах так званої «гібридної війни», яка нині триває між Росією та Україною. Визначень поняття «гібридна війна» є чимало, однак ми розуміємо гібридну війну як поєднання принципово різних можливостей ведення і законного, і незаконного способу війни, яка перемішується то малою, то великою війною із застосуванням кібервійни.

У гібридній війні Росія приховує пряме вторгнення в Україну, а також застосовує гібридні диверсії щодо України, перекладає свою безпосередню участь у гібридній війні на інших, різними способами приховує свою диверсійну діяльність проти України, тому дії РФ можна класифікувати як гібридну диверсію.

Гібридна диверсія – акт диверсії, під час проведення якої застосовуються некласичні прийоми ведення війни із спеціально підготовленими військовослужбовцями зі складу штатного підрозділу

військ спеціального призначення, та нерегулярних збройних формувань, найманців, повстанців, терористів, завербованих громадян тощо, які маскуються під мирне населення та вчиняють такі види диверсії: класичну диверсію, інформаційно-ідеологічну та кібердиверсію, під час класифікації якого відбувається схрещування принципово різних статей Особливої частини ККУ, при якому неможливо вивести склад злочину за диспозицією ст. 113 ККУ.

Щодо кібердиверсії, то цілком слушною є позиція О. О. Черноногa, який зазначає, що сьогодні провідні держави світу та суспільство загалом щораз більше покладаються і, відповідно, залежать від безперешкодного функціонування п'ятого простору – кіберпростору, під яким пропонується розглядати сукупність взаємопов'язаних інформаційних ресурсів, програмного забезпечення, баз та банків даних, що обробляються в комп'ютерних мережах і пов'язаній із ними інфраструктурі, разом з об'єктами, що підпадають під їх контроль та управління [15].

Вважаємо, що кібердиверсію можна застосовувати в екологічному, економічному, політичному й інформаційному аспекті. Зазначимо, що кібердиверсія – це прагнення ліквідувати суспільний і державний лад певної країни чи країн за допомогою використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та використати їх так, щоб їх послабити, а також, щоб вони виявилися нездатними протистояти офіційно озброєній агресії країни-агресора. Аналізуючи такі форми диверсійної діяльності, О. Д. Довгань, своєю чергою, зазначає, що кібердиверсія – це суспільно небезпечні діяння у кіберпросторі, наслідки яких можуть призвести до масового знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження стратегічних об'єктів шляхом втручання у роботу інформаційних систем [16].

За допомогою використання проводових і безпроводових технологій у мережі Інтернет розміщується величезна кількість інформаційних ресурсів і послуг, які використовуються користувачами локальних, академічних, приватних, корпоративних та урядових мереж. Поширеність мережі Інтернет у всьому світі дало низку можливостей диверсантам через кіберпростір застосовувати диверсії в економічних, політичних, інформаційних, екологічних сферах.

Вважаємо, що кібердиверсія може і приховувати, і не приховувати своєї приналежності до диверсії через комп'ютерні мережі.

Отже, кібердиверсія – це вчинений надзвичайно небезпечний акт з поєднанням принципово різних типів скоєння диверсії за ст. 113 ККУ, який здійснюється шляхом втручання у роботу ІТС за допомогою

використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку та управління людьми цими системами, приховування або не приховування причетності їх організаторів, а також способу та методів застосування, наслідки яких можуть призвести до масового знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження важливих соціально-економічних, оборонних чи інших об'єктів, які для країни мають важливе стратегічне значення.

За формою діяльності кібердиверсії можуть поділятися на явні й таємні.

Також варто виокремити ознаки, які вирізняють кібердиверсію з-поміж інших форм диверсій.

По-перше, йдеться про дистанційний вплив на супротивника.

По-друге, джерело та зрештою й суб'єкт кібердиверсії під час використання сучасних комп'ютерних технологій незавжди підлягає ідентифікації. Тобто ідентифікація максимально ускладнена і вимагає часу й організаційно-технічних зусиль.

По-третє, кібердиверсії дають змогу помітно диверсифікувати об'єкти руйнування.

Враховуючи наведене, розглянемо склад злочину, передбачений ст. 113 ККУ «Диверсія», через деякі злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за допомогою ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 ККУ [1]. В диспозиціях ч. 2 ст. 361, ч. 2 ст. 361-1, ч. 2 ст. 361-2, ч. 3 ст. 362, ст. 363 та ч. 2 ст. 363-1 ККУ трапляються вислови: «...або якщо вони заподіяли значну шкоду», проте до вислову «під значною шкодою» в ККУ є примітка. Значною шкодою у ст.ст. 361 та 363-1, якщо вона полягає у заподіянні матеріальних збитків, вважається така шкода, яка в сто і більше разів перевищує неоподатковуваний мінімум доходів громадян [1].

Визначаючи межу в кримінальному провадженні в терміні «значна шкода», з якої настає кримінальна відповідальність за незаконні дії особи, було зазначено нижню межу кримінальної відповідальності, але не зазначено верхньої межі, тому що не було потреби, у зв'язку зі застосуванням терміна в різних статтях ККУ. Шкода, яка перевищує значну, називається великою, а та шкода, що перевищує велику, – особливо великою.

У статтях ККУ злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку не зазначено «велика та особливо велика шко-

да». Тому, розглядаючи значну шкоду, вчинену з метою ослаблення держави, треба визначити межу значної шкоди. В цьому разі вона визначатиметься зі стану загального матеріального становища фізичної особи, юридичної особи, держави Україна та інших суб'єктів публічного права.

Як зазначає з цього приводу науковець Л. В. Дорош, значна шкода щодо держави – це наслідок будь-яких дій або вчинків, що охоплюють втрати, збитки, іноді людські жертви, неприємності, шкоду здоров'ю, руйнування або пошкодження об'єктів, які мають важливе значення для держави, а також дії, спрямовані на радіоактивне забруднення, масове отруєння, поширення епідемій, епізоотій чи епіфітотій, тобто знищення благ із метою ослаблення держави [17].

З огляду на фактичні обставини справи значна шкода може бути заподіяна не лише майну, а й, наприклад, інтересам, здоров'ю людини, праву і свободі людини. Всі ці об'єкти в нашому повсякденному житті використовують електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі та мережі електрозв'язку. Тобто диверсії можуть вчинятися через злочини, для вчинення яких використовують електронно-обчислювальні машини (комп'ютери), автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку, а також, застосовуючи шкідливі програми та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ, АС, комп'ютерні мережі чи мережі електрозв'язку і передбачену ч. 3 ст. 362 комп'ютерну інформації, що не призначена для відкритого доступу та вільного користування.

Характеризуючи злочини, пов'язані із диверсійною діяльністю, Б. В. Кузьменко справедливо зазначає, що основним безпосереднім об'єктом диверсії є національна безпека у зовнішньополітичній сфері, сфері державної безпеки, воєнній сфері та сфері безпеки державного кордону України, внутрішньополітичній сфері, економічній сфері, соціальній та гуманітарній сферах, науково-технологічній сфері, екологічній сфері та в інформаційній сфері, а також додатковим об'єктом злочину є життя та здоров'я, власність, довкілля [18].

Вважаємо, що об'єктом диверсії і предметом суспільно небезпечного діяння в кіберпросторі – кібердиверсії можуть бути всі наведені об'єкти, які мають важливе соціально-економічне й інше державне чи оборонне значення, а також – електростанції, водо-, нафто-, газопродуктопроводи, мости, дамби, греблі, системи інформаційних комунікацій, вокзали, аеропорти, морські чи річкові порти, лабораторії, банки, метрополітени, підприємства тощо, які обслуговуються електронно-обчислювальними машинами (комп'ютерами), автоматизованими сис-

темами, комп'ютерними мережами, мережами електрозв'язку. Тому все може бути об'єктом диверсійної діяльності (кібердиверсії) через втручання у комп'ютерні мережі, а тому має кваліфікуватися за ст. 113 ККУ.

Об'єктивна сторона такої диверсії, як форми суспільно небезпечного діяння в кіберпросторі виявляється у вчиненні суспільно небезпечних дій через втручання у комп'ютерні мережі (зокрема, вибухів і підпалів та інших загальнонебезпечних дій), що спрямовані на:

1) масове заподіяння тілесних ушкоджень, а також знищення людей, шляхом спричинення шкоди їхньому здоров'ю;

2) повне або часткове руйнування об'єктів, які мають важливе соціально-економічне, інше державне значення, оборонне значення;

3) знищення об'єктів життєзабезпечення населення;

4) радіоактивне забруднення;

5) масове отруєння;

6) поширення: епідемій; епізоотій; епіфітотій;

7) провокацію воєнних, релігійних, міжетнічних конфліктів;

8) завдання шкоди технічному та програмному забезпеченню, що унеможливлює або порушує функціонування найвищих державних органів та інших державних установ) тощо.

Однак, як свідчить перебіг триваючого російсько-українського військового протистояння, найбільшу небезпеку становлять кіберзлочини, пов'язані з військовою діяльністю держав, підготовкою збройних сил, а також участю у військових конфліктах і локальних війнах нового типу. Отож диверсія й така її форма суспільно небезпечного діяння в кіберпросторі, як кібердиверсія є закінченою з моменту вчинення вибуху, підпалу, затоплення, обвалу чи інших дій відповідної спрямованості, що стались через втручання у комп'ютерні мережі, незалежно від того, чи фактично настали ті або інші наслідки (наприклад, у результаті втручання в комп'ютерну мережу щоби спровокувати вибух, у зв'язку з недостатньою міцністю може взагалі не настати будь-яких помітних наслідків, через дощ може не загорітися підпалене сховище або отрута чи патоген виявляться неефективними).

Варто зазначити, що суб'єктом такого злочину є осудна особа, якій виповнилось 14 років [1].

Суб'єктивна сторона диверсії, як і її форми суспільно небезпечного діяння в кіберпросторі – кібердиверсії, характеризується виною у виді дій, що мають прямий умисел і спеціальну мету.

Характерною ознакою диверсії, кібердиверсії, кібергібридної диверсії є те, що вчинення диверсійних дій не є самоціллю, а вико-

ристовується винним як засіб досягнення його головної мети – ослаблення держави. На думку деяких учених, відмежування диверсії й її форми у кіберпросторі – кібердиверсії від інших суспільно небезпечних діянь, пов'язаних з атаками на національну безпеку, варто проводити саме за суб'єктивними ознаками – за метою вказаних злочинів. У цьому аспекті В. П. Ємельянов виокремлює такі характерні ознаки диверсії:

– при скоєнні диверсій дії винних спрямовані саме на спричинення тієї чи іншої шкоди (руйнування чи пошкодження підприємств, будівель, споруд, об'єктів життєзабезпечення та ін.);

– метою диверсійних актів є ослаблення держави, підрив її економічної безпеки й обороноздатності, дестабілізація діяльності державних органів або суспільно-політичної обстановки;

– диверсанти переважно діють таємно і не афішують свою діяльність [19].

Розглянемо приклад складу злочину, передбаченого ст. 113 ККУ, через кібердиверсію. На основі цього прикладу встановимо, чи це явна, чи замаскована диверсія, чи буде це кібердиверсія, якщо була скоєна в кіберпросторі. Для прикладу розглянемо випадок, що відбувся 5 серпня 2008 року на нафтопроводі Баку-Тбілісі-Джейхан. За три дні до російського вторгнення в Грузію на турецькій ділянці нафтопроводу Баку-Тбілісі-Джейхан стався вибух, який призвів до зупинки роботи цього нафтопроводу на 2 місяці, розливу 30 000 барелів нафти, і збитку близько на 1 млрд доларів. За повідомленням журналістів, нафтопровід оснащений надійною системою безпеки, навколо нього скрізь встановлені камери і тому заява курдських сепаратистів про те, що це вони підірвали трубу, є дуже сумнівною. Далі, після російсько-грузинської війни, світової кризи, російсько-українського збройного конфлікту, міжнародних санкцій і політичної ізоляції режиму Путіна розпочалися розмови про зближення Росії і Туреччини, з'явилася низка публікацій, зокрема і в BLOOMBERG [20]. Стверджувалося, що 5 серпня 2008 року вибух нафтопроводу на території Туреччини був учинений за допомогою комп'ютерного вірусу і що до цієї атаки причетні російські спецслужби. Комп'ютерний вірус змінив тиск у трубі та приховав це від центру управління.

На основі цього прикладу можна класифікувати цю кібердиверсію екологічним та економічним напрямом, а також стверджувати, що це активна форма фізичного руйнування або знищення. Також відомо, що при зупинці роботи цього нафтопроводу на 2 місяці, розливу 30 000 барелів нафти постраждала екосистема, і були завдані збитку близько

на 1 млрд доларів. Спосіб, яким був скоєний злочин, – це поширення технічними носіями інформації, які містять шкідливі програми для ЕОМ, за допомогою безпосереднього доступу до комп'ютерної мережі або віддаленого доступу до комп'ютерної мережі. Отже, цей випадок можна розглядати як диверсію [1].

Однак, якщо пошкодження об'єктів магістральних нафто-, газо- та нафтопродуктопроводів умисно вчиняється з метою ослаблення держави і спрямоване на масове знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, то вчинене, за наявності підстав, повинно кваліфікуватися за ст. 113 ККУ [17, с. 292].

У цьому разі безпосередній об'єкт диверсії – це безпека держави в економічній, екологічній сфері. Під час скоєння конкретного акту диверсії є обов'язковий додатковий об'єкт – навколишнє середовище, від функціонування якого залежить діяльність певних регіонів, а також території, на якій функціонує певна галузь економіки.

Об'єктивна сторона диверсії проявляється у зруйнуванні та пошкодженні нафтопроводу Баку-Тбілісі-Джейхан, що має важливе економічне значення. Диверсія є закінченою з моменту введення комп'ютерного вірусу.

Як зазначалося, нині в різних кримінальних провадженнях є складнощі в розмежуванні диверсії від інших складів злочину. Щоб виявити диверсію, треба порівняти ознаки за ст. 113 з іншими статтями Особливої частини ККУ. Вважаємо, головною ознакою диверсії є мета ослабити державу, що і відрізняє її від інших складів злочинів.

Наведемо ще один приклад диверсії, здійсненої за допомогою злочину в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Співробітники СБУ разом з українським інтернет-товариством знайшли вірус, призначений для знищення бази даних Центральної виборчої комісії (ЦВК). Про це повідомив тодішній голова СБУ В. Наливайченко.

Цей склад злочину проти основ національної безпеки України (ст. 113 ККУ) скоюється через злочин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електроз'язку (ст. 361 ККУ), а також злочинами за іншими статтями ККУ [1]. Ця політична диверсія належить до активних форм дії фізичного руйнування або знищення за допомогою «інфікованої» програми, яка була цілеспрямовано спрямована на ЦВК. Це давало змогу знищувати результати виборів та керувати ними, обираючи

своїх людей. Водночас відбувалось знищення країни з середини так званою «п'ятою колоною».

Основний безпосередній об'єкт диверсії – безпека держави в політичній сфері. Предметом диверсії може бути державний суверенітет України. Коли програма була запропонована ЦВК, з того моменту диверсія вважається закінченою.

Об'єктивна сторона диверсії виявляється в пошкодженні сервера ЦВК, який має важливе суспільно-державне й оборонне значення.

Зауважимо, що з 2015 року значно активізувалися й зовнішні кібердиверсії проти України.

Щодо зовнішньої диверсії, то огляд подій останніх років, інформації ЗМІ, спеціалізованої літератури та судової практики дав змогу узагальнити деякі аспекти цієї проблематики, а саме:

1. Реальні події недавніх років свідчать про вже сформовані загрози кібердиверсій щодо систем управління промислових підприємств і об'єктів критично важливої інфраструктури нашої країни. Основними об'єктами є нафто- і газовидобувні виробництва, об'єкти енергетики, зокрема атомної промисловості, об'єкти транспорту. Кібердиверсії вчиняються в межах поточних операцій з контролю над ресурсами нашої держави й її окремих регіонів.

2. Технологічні можливості кібердиверсій, анонімність джерела, а також їх результативність принципово змінюють уявлення про зміст бойових дій, зокрема локального характеру, а також про зміст того, що у слідчій практиці зазвичай кваліфікують як кібертероризм.

3. Кібердиверсії стали частиною масштабної економічної конкуренції, негласного політичного протистояння і широко застосовуються в поточних операціях з контролю над ресурсами.

4. За механізмом скоєння кібердиверсії максимально схоже на кібершпіонаж. Відмінність полягає, на нашу думку, в знищенні / пошкодженні (або загрозі таких наслідків) реального матеріального об'єкта.

Висновки. Здійснений аналіз нормативного закріплення поняття «диверсія» дає змогу стверджувати, що застосування у диспозиції ст. 113 ККУ терміна «народногосподарське значення» не відповідає сучасності й ускладнює кваліфікацію диверсії. Тому надважливо внести зміни у диспозицію ст. 113 ККУ шляхом вилучення з неї слів «народногосподарського значення» та замінити його на «важливе соціально-економічне та інше значення».

Саме за ознакою спеціальної мети та суб'єктивної сторони, яка характеризується виною у виді прямого умислу, відмежовується диверсія від інших статей Особливої частини ККУ. Нині диверсія як злочин часто трапляється у судовій практиці. Однак різновиди і

небезпечність диверсій в умовах сьогодення посідають важливе місце серед небезпечних злочинів проти нашої держави.

Актуальним також є таке політико-правове явище, як «гібридна війна». Під час такої війни суб'єкт злочину приховує пряме вторгнення в іншу державу, а також застосовує різні форми диверсій, відповідальність за які намагається перекласти на інших, або приховати взагалі. Вважаємо, що такі дії можна класифікувати як *гібридну диверсію*. У гібридній війні суб'єкт злочину приховує пряме вторгнення в Україну, диверсія за ст. 113 ККУ, яку називаємо гібридною, також приховується або маскується диспозицією статті, більш віддалено, ніж інша стаття ККУ, тому ми назвали це гібридними диверсіями щодо України. Є спроби приховання диверсій взагалі за допомогою інших статей Особливої частини ККУ, тому такий вид диверсії можна класифікувати як гібридну диверсію. В стандартній війні застосовуються просто диверсії, а новизна полягає в тому, що в гібридній війні застосовують не тільки стандартні диверсії, а й гібридні диверсії.

Узагальнюючи зазначені наукові підходи та приклади, враховуючи положення кримінального законодавства, які встановлюють кримінальну відповідальність за вчинення диверсійної діяльності, пропонуємо ввести визначення нового правового явища, яке називаємо *«гібридна диверсія»*.

Гібридна диверсія – це унікальна диверсія із поєднанням різних статей ККУ, які тільки відмежовуються ст. 113 ККУ. Вони виводять спосіб скоєння диверсії, який спрямований на досягнення остаточного результату.

Запропоновано визначення поняття «кібердиверсія» як учинений надзвичайно небезпечний акт із поєднанням принципово різних типів скоєння диверсії за ст. 113 ККУ, що здійснюється шляхом втручання у роботу ІТС за допомогою використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та управління людьми цими системами, приховування або неприховування причетності їх організаторів, а також способу та методів застосування, наслідки яких можуть призвести до масового знищення людей, заподіяння тілесних ушкоджень чи іншої шкоди їхньому здоров'ю, зруйнування або пошкодження важливих соціально-економічних, оборонних чи інших об'єктів, які для країни мають важливе стратегічне значення.

Проблема притягнення до кримінальної відповідальності за кібердиверсії – багатоаспектна й є не лише у законодавчій сфері. Проте зміна та розробка нової нормативно-правової бази, яка б регулювала відношення у кіберпросторі (профілактику кіберзлочинів, протидію та

боротьбу з правопорушеннями в інформаційній сфері), – є першочерговим стратегічним напрямом. Така база може мати форму окремого кодексу або щонайменше окремих розділів у чинних кодексах і законах, зокрема кримінальному законі, «Кримінальному процесуальному кодексі України», Законі України «Про оперативно-розшукову діяльність» тощо.

Перспективи використання результатів дослідження дають змогу вчасно виявляти та запобігати диверсійній діяльності і країни-агресора, і окремих ОЗГ, дії яких спрямовані на підрив і ослаблення держави Україна, а також передбачати ті чи інші види диверсій, які можуть бути скоєні на території України, правильно класифікувати диверсію та відмежовувати її від інших статей ККУ.

Отож кримінально-правова норма, що передбачає відповідальність за диверсію, лише частково відповідає положенням сучасної науки кримінального права, хоча й має на меті охорону інтересів національної безпеки України.

1. Кримінальний кодекс України від 05.04.2001 № 2341-III (зі змінами і доповненнями в редакції станом на 01.05.2016 р.) [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2341-14

2. Фесенко Є. В. Злочини проти здоров'я населення та системи заходів з його охорони: монографія / Є. В. Фесенко. – К.: Атіка, 2004. – 280 с.

3. Картавцев В. С. Кримінальна відповідальність за злочини проти основ національної безпеки України (наукові засади кваліфікації): навч. посібник / В. С. Картавцев. – К.: Вид-во Національної академії СБ України, 2004. – 57 с.

4. Бантишев О. Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації): монографія / О. Ф. Бантишев, О. В. Шамара. – 2-е вид., перероб. та доп. – К.: Наук.-вид. відділ НА СБ України, 2010. – 168 с.

5. Луценко Ю. В. Звільнення від кримінальної відповідальності за злочини проти основ національної безпеки України: монографія / Ю. В. Луценко. – Х.: Право, 2015. – 200 с.

6. Климчук О. О. Кримінальна відповідальність за диверсію по законодавству України: дис ... канд. юрид. наук: 12.00.08 / О. О. Климчук; НА СБ України. – К., 2003. – 269 с.

7. Великий тлумачний словник сучасної української мови (з дод. і допов.) / уклад. і голов. ред. В. Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2005. – С. 293.

8. Литвак О. М. Держава і злочинність / О. М. Литвак. – К.: Атіка, 2004. – 302 с. – С. 147.

9. Лихова С. Я. Кримінальна відповідальність за диверсію (ст. 113 КК України) / С. Я. Лихова, М. В. Садовський // Юридична наука і практика: виклики часу: матеріали V Міжнародної науково-практичної конференції (м. Київ, 12 березня 2015 р.). – К.: НАУ, 2015. – Т. ІІ. – С. 72.

10. Чуваков О. А. Деякі види диверсійних актів у сучасних умовах / О. А. Чуваков // Актуальні проблеми держави і права. – Одеса: Юрид. літ., 2010. – № 55. – С. 221.

11. Картавцев В. С. Кримінальна відповідальність за злочини проти основ національної безпеки України (наукові засади кваліфікації): навч. посібник / В. С. Картавцев. – К.: Вид-во Національної академії СБ України, 2004. – 57 с. – С. 39.

12. Кримінальне право (Особлива частина): підручник / за ред. О. О. Дудорова, Є. О. Письменського. – Луганськ: Елтон-2, 2012. – Т. 1. – 780 с. – С. 60.

13. Бантишев О. Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації): монографія / О. Ф. Бантишев, О. В. Шамара. – 2-е вид., перероб. та доп. – К.: Наук.-вид. відділ НА СБ України, 2010. – 168 с. – С. 142.

14. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. – 9-те вид., перероб. та допов. – К.: Юридична думка, 2012. – 1316 с. – С. 276.

15. Черноног О. О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління / О. О. Черноног // Междисциплинарные исследования в науке и образовании. – 2015 [Електронний ресурс]. – Режим доступу: mino.esrae.ru/178-1484

16. Довгань О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О. Д. Довгань, В. Г. Хлань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 49–53.

17. Кримінальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. – 5-те вид., допов. – Х.: Право, 2013. – Т. 2: Особлива частина / Ю. В. Баулін, В. І. Борисов, В. І. Тютюгін та ін. – 2013. – С. 749.

18. Кузьменко Б. В. Інформаційна диверсія та інформаційний саботаж – інструменти кібертероризму / Б. В. Кузьменко // Роль правоохоронних органів у формуванні правової держави в умовах євроінтеграції України: матеріали Всеукр. підсумк. наук.-практ. конф. (м. Київ, 12 березня 2015 р.). – К.: Нац. акад. внутр. справ, 2015. – Ч. 1. – С. 20.

19. Емельянов В. П. Терроризм и преступления с признаками терроризирования: уголовно-правовое исследование / В. П. Емельянов. – СПб.: Юридический центр Пресс, 2002. – 291 с. – С. 278.

20. Взрыв нефтепровода БТД на территории Турции 5 августа 2008 г. – результат кибердиверсии России [Электронный ресурс]. – Режим доступа: http://cyxymu.livejournal.com/1619335.html, публикация в BLOOMBERG; http://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Пелещак О. Р. Кибердиверсия как форма современной диверсионной деятельности

Исследованы вопросы, связанные с определением понятия «диверсия» и ее разграничением на отдельные виды. Предложена классификация новых форм диверсионных актов в современных условиях. Идентифицирована кибердиверсия как форма современной диверсионной деятельности.

Обоснована необходимость согласования ст. 113 Уголовного кодекса Украины (диверсия) с другими статьями (преступления в сфере использования компьютеров).

Ключевые слова: *национальная безопасность, гибридная война, диверсия, гибридная диверсия, кибердиверсия*

Peleshchak O. R. Cyber sabotage as a form of the modern sabotage activity

In the conditions of undeclared hybrid war, by Russian Federation is conducted on territory of east part of Ukraine, concept of diversion, in its different forms acquires a new value for Ukraine, in fact this crime, responsibility for which the foreseen item 113 the Criminal code of Ukraine, and it infringes on the foundations of Ukraine's national security, that is, on the security of the people of Ukraine as a bearer of sovereignty and the only source of power in Ukraine.

Unfortunately, detailed analysis of positions of item 113 the Criminal code of Ukraine, especially objective side of this crime, suggests the author of the article an idea that a criminal law in force does not answer the calls of time in part of establishment of responsibility for the modern forms of diversionary activity. In particular, if to take into account the criminal norm of disposition of item 113 the Criminal code of Ukraine, it is possible to establish, that criminal acts which are engulfed concepts «diversion» toward realization of criminally punishable acts in a cyberspace do not have not a single attitude.

However, conducted by us research of forms of modern diversionary activity is led to by the fallaciousness of such approach, in fact self interference over with komputer networks can result in consequences, to foreseen disposition of item 113 the Criminal code of Ukraine.

Because of said, this scientific article is devoted research of new forms of diversionary acts in the conditions of modern. The article examines the issues related to the definition of sabotage and its division into separate species. It attempts classification of new forms of subversive acts in the modern world. In particular, the author tries to identify cyber diversion as a separate form of modern subversive activities.

Key words: *national safety, hybrid war, sabotage, hybrid sabotage, cyber diversion.*

Стаття надійшла 23 серпня 2017 р.