УДК 343.321
DOI https://doi.org/10.32837/npnuola.v26i0.660

І. В. Діордіца

ПОНЯТТЯ ТА ЗМІСТ КІБЕРШПИГУНСТВА

Постановка проблеми. Кіберпростір докорінно трансформував глобальний світ, чітко поділивши не лише реальність і віртуальність, але й інформаційний простір від власне кібернетичного. Кіберпростір трансформував наш світогляд, водночас значною мірою забезпечуючи майже пів планети доступом до інформації, до комунікації, до нових економічних можливостей. Відкритість Інтернету зумовила виникнення нових загроз національній і міжнародній безпеці. Поряд із інцидентами природного походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Передумовою до виникнення таких понять, як «кібербезпека» та «кібершпигунство», є не лише збільшення випадків нелегального втручання в персональні системи, а також перехоплення інформації з боку кримінальних структур і терористичних організацій, а й системний, цілеспрямований вплив державних або квазідержавних структур на державні системи, критичну інфраструктуру, хід виборів або навіть конституційний лад.

Розвиток і вдосконалення заходів кримінально-правової охорони державної таємниці (секретної інформації) передбачає ґрунтовне дослідження та вдосконалення диспозиції відповідних норм Кримінального кодексу України, зокрема й шпигунства, та введення в нього такої нової правової категорії, як кібершпигунство. При цьому важливими аспектами є такі: врахування сучасних суспільно-політичних змін у законодавчому регулюванні обігу секретної інформації, максимальна конкретизація та уніфікація понятійно-категорійного апарату, що застосовується в диспозиції норми, а також дотримання усталених принципів законодавчої техніки та використання наявної зарубіжної практики, норм і доктрин. Ці та інші фактори і зумовлюють *актуальність теми*.

У межах обговорення та визначення концептуальних засад кібербезпекової політики країни наріжним каменем постає питання вдосконалення наявного категорійно-понятійного апарату з метою подальшої його операціоналізації. У літературі сформувалася певна низка напрямів тлумачення поняття «кібербезпека», яка відображає різноманітні аспекти інформаційної політики, військової політики, міжнародного права, критичних інфор-

маційних структур, інформаційно-комунікаційних технологій та комп'ютерних мереж. При цьому спостерігаються зміщення формулювань у різних нормативних документах, пропозиція нових, які почасти суперечать попереднім або просто їх дублюють.

Аналіз останніх досліджень і публікацій свідчить про те, що питання збирання секретної інформації як форми кібершпигунства не досліджувалося на достатньому рівні та розглядалося науковцями переважно у межах загальної кримінально-правової характеристики шпигунства, зокрема його об'єктивної сторони, або ж дослідження проблем кібербезпеки загалом. Тому в моїй статті використано наукові здобутки вчених із різних сфер. Окремо виділю роботи наукової школи В.А. Ліпкана [1–5]. Також зазначу окремі публікації таких авторів, як: Д.С. Мінін [6], М.М. Чеховська [7], В.М. Шлапаченко [8].

Метою статті є визначення поняття та змісту кібершпигунства.

Основними **завданнями,** розв'язанню яких присвячено статтю, є такі:

1) сформулювати авторське розуміння «кібершпигунства»;

2) визначити його об'єкт, об'єктивну сторону, суб'єкт, суб'єктивну сторону та його предмет;

3) надати певні пропозиції щодо підвищення ефективності правового регулювання цього системного явища.

Виклад основного матеріалу. Нині в Україні особливої гостроти набуває проблема інформаційної безпеки та комп'ютерної злочинності, тоді як розвиток правової бази і судова практика не відповідають вимогам реального життя. При цьому мають місце так звані комп'ютерні злочини – протиправні діяння, за яких інформаційно-обчислювальні системи стають предметом або знаряддям здійснення злочинних посягань. Практично всі відомі світовій практиці види цих злочинів (комп'ютерне шахрайство, комп'ютерний саботаж, комп'ютерний шпіонаж, крадіжки програм) реєструються вже і в Україні.

1 вересня 2001 р. набув чинності Кримінальний кодекс України, який містить розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж». Ним уперше закріплюються визначення та юридичні моделі наявних суспільно небезпечних діянь у цій сфері, хоча методичних рекомендацій з їхнього розслідування поки що немає, а судова практика незначна.

Однак слід зазначити, що ані закони самі по собі, ані лише організаційно-технічні заходи не здатні системно захистити інформаційні системи від злочинних посягань, тому державі в законодавчій і правозастосовній практиці слід адекватно не лише реагувати на існування суспільно небезпечних посягань у сфері інформатизації, як це вже зроблено у сфері програмно-апаратних заходів захисту, а й формувати адекватну реаліям і прогнозованим напрямам розвитку тих чи інших тенденцій у кібернетичній сфері напрями державної кібербезпекової політики.

Досліджуючи поняття та зміст кібершпигунства, перш за все зазначу, що до цієї категорії входять два окремі терміни – «кібер» («кібернетичне») та «шпигунство». Отже, для здійснення ґрунтовного дослідження вищезазначеної категорії, зупинюся на кожній окремо.

Використовуючи «Тлумачний словник української мови», зазначу, що «*шпигунство*» – злочинна діяльність, яка полягає в таємному збиранні відомостей або викраданні матеріалів, що становлять державну таємницю, з метою передачі їх іншій державі; вистежування, розшук [9, с. 526].

А «*кібернетичний*» стосується кібернетики; який створено, працює на основі принципів, методів кібернетики [9, с. 168].

У Кримінальному кодексі України «*шпигунство*» визначено як передача або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю, якщо ці дії вчинені іноземцем або особою без громадянства (ст. 114 КК України) [10].

Безпосереднім об'єктом шпигунства (кібершпигунства – *Д. І.*) є зовнішня безпека України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека.

Предметом цього злочину є відомості, що містять державну таємницю, вичерпний перелік яких міститься в Законі України «Про державну таємницю» від 21 січня 1994 р. Згідно з цим Законом *державна таємниця* (також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України (кібербезпеці – *Д. І.*) та які визнані в порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [11]. Ці відомості мають гриф секретності, який визначає її ступінь. Спеціальним уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Кібершпигунство, або комп'ютерний шпіонаж (вживається також термін «*кіберрозвідка*») – термін, що позначає, як правило, несанкціоноване отримання інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюване з використанням обходу (злому) систем комп'ютерної безпеки, зі застосуванням шкідливого програмного забезпечення, включно з «троянськими конями» і шпигунськими програмами. Кібершпигунство може здійснюватися як дистанційно, за допомогою Інтернету, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств звичайними шпигунами («кротами»), а також хакерами. Віднедавна кібершпигунство передбачає також аналіз провідними спецслужбами (ЦРУ, Моссад, ФСБ), зокрема, за спостереженням цифрового сліду поведінки користувачів соціальних мереж (повідомлення, друзі, фотографії, відео тощо), таких як Facebook, ВКонтакте, Twitter тощо, з метою виявлення екстремістської, терористичної чи антиурядової діяльності, закликів збору на мітинги проти влади.

Кібернетичне шпигунство (кібершпигунство) – передача або збирання з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей з обмеженим доступом, що здійснюється в кіберпросторі [10].

Отже, під *кібершпигунством* пропоную розуміти злочинну діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іно-

земній державі, іноземній організації або їхнім представникам, якщо ці дії вчинені іноземцем або особою без громадянства і з використанням кібернетичного простору.

Характеризуючи кібершпигунство, зауважу, що це злочинне діяння повинно бути закріплене на законодавчому рівні – не лише національному, але й міжнародному, з метою уніфікації та можливості приведення наявних норм в єдине ціле.

Як було зазначено вище, то одним із понять, які входять до категорії «кібершпигунства», є «шпигунство», тому визначати зміст першої категорії буду через аналіз останньої.

З об'єктивної сторони шпигунство може виявлятися у двох формах:

1) передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю;

2) збиранні таких же відомостей із метою передачі іноземній державі, її організаціям або їхнім представникам.

Ініціатива збирання чи передачі відповідних відомостей може належати як виконавцю, так і адресату шпигунства. Для кваліфікації злочину це значення не має.

Передача зазначених відомостей має місце у разі, коли особа володіє ними і повідомляє (вручає) їх іноземній державі або її представнику (агенту). Способи передачі можуть бути різними (усно, письмово, безпосереднє ознайомлення з будь-якими матеріалами, передача по радіо, телефону, з використанням тайників, кур'єрів та інше). Для відповідальності не має значення, чи передаються першоджерела (наприклад, оригінали документів, креслення, зразки), їхні копії або лише відомості про них (зліпки, макети, опис технічних систем, будь-яких об'єктів та інше). Тому будь-які дії, виявлені як у формі передачі в буквальному розумінні цього слова, так і у створенні умов для ознайомлення агента іншої держави з ними, підпадають під поняття передачі [12, с. 580], тобто віддавати в розпорядження кого-, чого-небудь; повідомляти кого-небудь про щось; розповідати кому-небудь про щось почуте, побачене і таку інше; повідомляти, інформувати про щось кого-небудь, звичайно за дорученням іншого [9, с. 354].

Збирання відомостей, що становлять державну таємницю, – це будь-які випадки здобуття (діставання, розшук, знаходження чого-небудь [9, с. 106]) таких відомостей (наприклад, викрадення, особисте спостереження, фотографування, підслуховування телефонних розмов та інше). У кібершпигунстві для отримання таких відомостей використовується найскладніша сучасна техніка.

Для відповідальності за ст. 114 КК важливо встановити, що відомості, які становлять державну таємницю, були передані чи збиралися для передачі саме іноземним державам, іноземним організаціям або їхнім представникам.

Закінченим шпигунство вважається з моменту початку збирання зазначених відомостей або з моменту їх передачі.

Аналізуючи *суб'єктивну сторону* злочинів, слід говорити про те, що шпигунство характеризується прямим умислом, за якого особа усвідомлює, що відомості збираються або передаються іноземній державі, орга-

нізації або їхнім представникам і що ці відомості є державною таємницею, яка не підлягає передачі. Мотиви злочину на кваліфікацію злочину не впливають [13].

Суб'єкт злочину спеціальний – іноземець або особа без громадянства, які досягли 16-річного віку. Шпигунство, вчинене громадянином України, кваліфікується за ст. 111 КК як державна зрада [10].

Визначальними ознаками шпигунської діяльності є такі: це складник розвідувальної діяльності, метою якої є отримання лише секретної інформації (державної таємниці), що спеціально охороняється; полягає у незаконному передаванні (збиранні протиправними способами з метою незаконного передавання) секретної інформації; здійснюється винятково в інтересах адресатів передавання – іноземних держав (організацій), які є організаторами цієї діяльності та споживачами здобутої інформації; заборонена законодавством держави – володільця секретної інформації; з огляду на кримінально-правову заборону та системну контррозвідувальну діяльність здійснюється таємно, конспіративно; спричиняє або створює загрозу спричинення шкоди життєво важливим інтересам держави (повноті та своєчасності їх реалізації) у тих сферах її діяльності, де відбувається обіг секретної інформації [8, с. 100].

Якщо шпигунство вчинене шляхом незаконного втручання в роботу автоматизованих електронно-обчислювальних машин, їхніх систем чи комп'ютерних мереж, це потребує додаткової кваліфікації за ст. 361 Кримінального кодексу України, а шляхом викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службової особи своїм службовим становищем – за ст. 362 КК.

Якщо особою викрадено з метою передачі іноземній державі, іноземній організації чи їхнім представникам предмети, відомості про які становлять державну таємницю (зразки військової зброї, спеціальної техніки, криптографічного чи іншого обладнання, радіоактивні матеріали тощо), або офіційні документи, що є в державних підприємствах і містять державну таємницю, ці дії, залежно від їхнього конкретного способу, а також від особливостей предмета і суб'єкта, слід додатково кваліфікувати за ст. ст. 185–191, 262, 357, 410 КК України.

Шпигунство, поєднане з незаконним використанням спеціальних технічних засобів негласного отримання інформації, повністю охоплюється ст. 114 КК і не потребує додаткової кваліфікації за ст. 359 КК [14].

Отже, провівши дослідження кібершпигунства, можу **висновувати** таке: як на міжнародному, так і на національному рівнях відсутня уніфікована дефініція поняття «кібершпигунство», і це формулює підстави для здійснення ґрунтовних досліджень цього явища. Під *кібершпигунством* запропоновано розуміти злочинну діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їхнім представникам, якщо ці дії вчинені іноземцем або особою без громадянства і з використанням методів кібернетики. Об'єктом кібершпигунства є зовнішня безпека України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна

чи інформаційна безпека та кібернетичний простір загалом. З об'єктивної сторони шпигунство виражається в передачі або збиранні з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю. Предметом цього злочину є відомості, що містять державну таємницю. Аналізуючи суб'єктивну сторону злочинів, слід говорити про те, що кібершпигунство характеризується прямим умислом. Суб'єкт злочину спеціальний – іноземець або особа без громадянства, які досягли 16-річного віку. Наголошую на тому, що це злочинне діяння повинно бути закріплене на законодавчому рівні – не лише національному, але й міжнародному, з метою уніфікації та можливості приведення наявних норм в єдине ціле.

Література

1. Інформаційна безпека України : глосарій / В.А. Ліпкан, Л.С. Харченко, О.В. Логінов. Київ : Текст, 2004. 136 с.

2. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : монографія / В.А. Ліпкан, В.Ю. Баскаков ; за заг. ред. В.А. Ліпкана. Київ : О.С. Ліпкан, 2013. 344 с.

3. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : 12.00.07 / Національний університет біоресурсів і природокористування України. Київ, 2015. 247 с.

4. Шепета О.В. Адміністративно-правові засади технічного захисту інформації : монографія. Київ : О.С. Ліпкан, 2012. 296 с.

5. Ліпкан В.А., Діордіца І.В. Національна безпека України: кримінально-правова охорона : навч. посібник. Київ : КНТ, 2007. 292 с.

6. Мінін Д.С. Підходи до визначення поняття «кібербезпека». URL: http://istfak.org.ua/tendentsii-rozvytku-suchasnoi-systemy-mizhnarodnykh-vidnosyn-ta-svitovoho-politychnoho-protsesu/185-heopolitychna-dumka-ta-heostratehichni-protsesy-v-khkhi-st/971-pidkhody-do-vyznachennya-ponyattya-kiberbezpeka.

7. Чеховська М.М. Кібершпіонаж як загроза національній безпеці. *Актуальні проблеми управління інформаційною безпекою держави*. Київ : Науково-видавничий відділ НА СБ України, 2012. С. 232–234.

8. Шлапаченко В.М. Шпигунство як діяльність зі здобування інформації. *Інформаційна безпека людини, суспільства, держави*. Київ, 2015. № 1 (17). С. 99–109.

9. Великий тлумачний словник сучасної української мови / укл. О. Єрошенко. Донецьк : ТОВ «Глорія Трейд», 2012. 864 с.

10. Кримінальний кодекс України від 5 квітня 2001 р. *Відомості Верховної Ради України*. 2001. № 25. Ст. 131.

11. Про державну таємницю : Закон України від 21 січня 1994 р. URL: http://zakon3.rada.gov.ua/laws/show/3855-12.

12. Кримінальний кодекс України : Науково-практичний коментар / Ю.В. Баулін, В.І. Борисов, С.Б. Гавриш та ін. ; за заг. ред. В.В. Сташиса, В.Я. Тація. Київ : Концерн «Видавничий Дім «Ін Юре», 2003. 1196 с.

13. Бутчана В.В. Відмінність складу злочину «Державна зрада» у формі шпигунства (ст. 111 КК України) від складу злочину «Шпигунство» (ст. 114 КК України): кримінально-правовий аспект кваліфікації. URL: http://www.rusnauka.com/46_PWMN_2015/Pravo/5_204351.doc.htm.

14. Коментар до статті 114. Шпигунство. URL: http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/112.php.

А н о т а ц і я

Діордіца І. В. **Поняття та зміст кібершпигунства.** – Стаття.

У статті автор здійснив дослідження поняття «кібершпигунство» на основі аналізу концепту «шпигунство» в його теоретичному сенсі, а також застосуванні сучасних шпигунських технологій у кіберпросторі. Актуальність дослідження зумовлена не лише значним збільшенням випадків нелегального втручання в персональні системи, а також перехоплення інформації з боку кримінальних структур і терористичних організацій, але й системним, цілеспрямованим впливом державних або квазідержавних структур на державні системи, критичну інфраструктуру, хід виборів або конституційний лад. При цьому важливими аспектами дослідження стали такі: врахування сучасних суспільно-політичних змін у законодавчому регулюванні обігу секретної інформації, максимальна конкретизація та уніфікація понятійно-категорійного апарату, що застосовується в диспозиції норми, а також дотримання усталених принципів законодавчої техніки та використання наявної зарубіжної практики, норм і доктрин. Запропоновано авторське розуміння кібершпигунства: це злочинна діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їхнім представникам, якщо ці дії вчинені іноземцем або особою без громадянства в кібернетичному просторі. Встановлено, що об'єктом кібершпигунства є зовнішня безпека України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека та кібернетичний простір загалом. З об'єктивної сторони шпигунство виражається в передачі або збиранні з метою передачі іноземній державі, іноземній організації або їхнім представникам відомостей, що становлять державну таємницю. Предметом цього злочину є відомості, що містять державну таємницю. Із суб'єктивної сторони кібершпигунство характеризується прямим умислом. Суб'єкт злочину спеціальний – іноземець або особа без громадянства, які досягли 16-річного віку. Наголошено на тому, що це злочинне діяння повинно бути закріплене на законодавчому рівні – не лише національному, але й міжнародному, з метою уніфікації та можливості приведення наявних норм в єдине ціле.

Ключові слова: кібернетичний, кіберпростір, кібербезпека, шпигунство, кібершпигунство, національна безпека.

S u m m a r y

Diorditsa I. V. **The concept and content of cyber espionage.** – Article.

It was noted that, there is no unified definition of "cyberespionage" both at the international and national levels and it formulates grounds for the future fundamental studies of the phenomenon. The relevance of the study is due to the significant increase in cases of illegal interference with personal systems, as well as the interception of information by criminal structures and terrorist organizations, as well as the systematic, targeted impact of state or quasi-state structures on state systems, critical infrastructure, the election process or the constitutional order. At the same time, important aspects of the study were: taking into account modern socio-political changes in the legislative regulation of the circulation of classified information, maximum specification and unification of the conceptual apparatus used in the disposition of the norm, as well as adherence to the established principles of legislative technology and the use of existing foreign, doctrine. It was offered to define the cyberespionage as a criminal activities carried out by secret stalking, investigation, collection, abduction and transfer of information which contains the state secrets to a foreign state, a foreign organization or their representatives, if these acts are committed by a foreigner or a stateless person and in the cyberspace. It was defined that external security of Ukraine, its sovereignty, territorial integrity and security, defense, government, economic or information security and cyber space in general is the object of the cyberespionage. The objective side of the espionage is expressed in the transmission or collection for the transfer to a foreign state, a foreign organization or their representatives of information which is the state secret. Information which contains the state secrets is the subject. Analyzing the mens rea it was said that the cyberespionage is characterized by direct intention. The special subject of crime was defined – a foreigner or a person without citizenship who have reached 16 years. It was stresses that this criminal act should be enshrined in law, not only nationally, but also internationally, to unify and to bring existing rules together.

Key words: cyber, cyberspace, cyber security, espionage, cyber espionage, national security.